CARLOS HENRIQUE DOS SANTOS SILVA PATROCÍNIO

ANÁLISE QUANTITATIVA DE SOLUÇÕES DE ARQUITETURA SASE

Ouro Preto, MG
2023

CARLOS HENRIQUE DOS SANTOS SILVA PATROCÍNIO

ANÁLISE QUANTITATIVA DE SOLUÇÕES DE ARQUITETURA SASE

Trabalho de conclusão de curso apresentado ao Instituto Tecnológico Vale, como parte dos requisitos para obtenção do título de especialista em Automação para Processos de Mineração.

Área de concentração: Cibersegurança

Orientador: Prof. Ralf Luís Moura, D.Sc.

,

Ouro Preto, MG
2023

Título: Análise quantitativa de soluções de arquitetura SASE
Classificação: **( ) Confidencial ( ) Restrita ( ) Uso Interno (X) Pública**

Informações Confidenciais - Informações estratégicas para o Instituto e sua Mantenedora. Seu manuseio é restrito a usuários previamente autorizados pelo Gestor da Informação.

Informações Restritas - Informação cujo conhecimento, manuseio e controle de acesso devem estar limitados a um grupo restrito de empregados que necessitam utilizá-la para exercer suas atividades profissionais.

Informações de Uso Interno - São informações destinadas à utilização interna por empregados e prestadores de serviço.

Informações Públicas - Informações que podem ser distribuídas ao público externo, o que, usualmente, é feito através dos canais corporativos apropriados.

Dados Internacionais de Catalogação na Publicação (CIP)

P342a

Patrocínio, Carlos Henrique dos Santos Silva
Análise quantitativa de soluções de arquitetura SASE. Carlos Henrique dos Santos Silva Patrocínio... [et al.] - Ouro Preto, MG: ITV, 2023.

51 f.: il.

Monografia (Especialização latu sensu) - Instituto Tecnológico Vale, 2023.
Orientadora: Ralf Luis Moura

1. Segurança em Nuvem. 2. Confiança-Zero. I. Moura, Ralf Luis. II. Título.

CDD.23. ed. 629.892

Carlos Henrique dos Santos Silva Patrocínio

ANÁLISE QUANTITATIVA DE SOLUÇÕES DE ARQUITETURA SASE

Trabalho de conclusão de curso apresentado ao Instituto Tecnológico Vale, como parte dos requisitos para obtenção do título de especialista *lato sensu* em [Automação para Processos de Mineração].

Orientador: Prof. D.Sc. Ralf Luis de Moura

Trabalho de conclusão de curso defendido e aprovado em 15 de dezembro de 2023 pela banca examinadora constituída pelos professores:

_____

Prof. D.Sc. Ralf Luis de Moura
Orientador – Vale

_____

Prof. D.Sc. Pedro Henrique Gomes da Silva
Membro externo – Ericsson Telecomunicações

_____

D.Sc. Antonio Lemos Maia Neto
Membro externo – Amazon Web Service (AWS)

Os Signatários declaram e concordam que a assinatura será efetuada em formato eletrônico. Os Signatários reconhecem a veracidade, autenticidade, integridade, validade e eficácia deste Documento e seus termos, nos termos do art. 219 do Código Civil, em formato eletrônico e/ou assinado pelas Partes por meio de certificados eletrônicos, ainda que sejam certificados eletrônicos não emitidos pela ICP-Brasil, nos termos do art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001 ("MP nº 2.200-2").

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal de Assinaturas Vale. Para verificar as assinaturas clique no link: https://vale.portaldeassinaturas.com.br/Verificar/27D3-FC80-B309-923A ou vá até o site https://vale.portaldeassinaturas.com.br:443 e utilize o código abaixo para verificar se este documento é válido. The above document was proposed for digital signature on the platform Portal de Assinaturas Vale . To check the signatures click on the link: https://vale.portaldeassinaturas.com.br/Verificar/27D3-FC80-B309-923A or go to the Websitehttps://vale.portaldeassinaturas.com.br:443 and use the code below to verify that this document is valid.

Código para verificação: 27D3-FC80-B309-923A

Hash do Documento

8F0D3E7A8C0881E4D3021A5166D20EE2DE1C6C25244BD611546FDFACDD524E90

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 09/02/2024 é(são) :

☑ Pedro Henrique Gomes da Silva (Signatário) - em 21/12/2023 17:32 UTC-03:00
Tipo: Assinatura Eletrônica
Identificaçao: Por email: pedrohenriquegomes@gmail.com; Código de acesso: 1

Evidências

Client Timestamp Thu Dec 21 2023 17:32:52 GMT-0300 (Brasilia Standard Time)
Geolocation Latitude: -23.488088 Longitude: -46.731585 Accuracy: 133
IP 177.9.156.22
Hash Evidências:
48E4BE5C10CCF15D124175A7BBB112817DB072D1946C3801CEC1EF2B18981723

☑ Antonio Lemos Maia Neto (Signatário) - 078.114.446-90 em 21/12/2023 16:13 UTC-03:00
Tipo: Assinatura Eletrônica
Identificaçao: Por email: lemosmaia@gmail.com; Código de acesso: 1

Evidências

Client Timestamp Thu Dec 21 2023 16:12:55 GMT-0300 (Brasilia Standard Time)
Geolocation Location not shared by user.
IP 179.183.137.121
Hash Evidências:
B3CCA9918F3571F803CDF1D07014AB55F02158218240BF964A1CCD3C1E6B4026

☑ Ralf Luis de Moura (Signatário) - em 21/12/2023 14:42 UTC-03:00

Tipo: Assinatura Eletrônica
Identificaçao: Por email: ralf.moura@vale.com; Código de acesso: 1

Evidências

Client Timestamp Thu Dec 21 2023 14:42:02 GMT-0300 (Horário Padrão de Brasília)
Geolocation Latitude: -20.1457664 Longitude: -40.2587648 Accuracy: 999.5686049679772
IP 189.24.162.174
Hash Evidências:
B3E8D4832F73FDE8A9315ADE89C28A1AC5DC339B037981EA0A31A1048D7E8580

À minha família, amigos e colegas de profissão.

AGRADECIMENTOS

À minha família, que foi meu alicerce para chegar até aqui. Ao meu orientador, Ralf Moura, meu guia durante o processo. À Rinaldo Oliveira e Vânia Neves, que permitiram que eu cursasse a Especialização. Ao ITV e Vale por criarem a oportunidade de evoluir e ampliar conhecimentos.

O conhecimento se adquire com o estudo, mas a sabedoria apenas com a reflexão e a experiência.

RESUMO

O trabalho híbrido, impulsionado pela pandemia, tornou-se a norma, com 62% dos empregadores planejando manter funcionários em regime remoto ou híbrido pós-COVID-19. A migração para data centers em nuvem, necessária para acessibilidade remota, eleva preocupações sobre segurança de dados. Soluções tradicionais como redes virtuais privadas (VPNs) tornam-se ineficientes, demandando revisão nas políticas de acesso remoto. Surge, então, o Serviço de Acesso Seguro de Borda (SASE), uma arquitetura em nuvem que combina funções para oferecer acesso seguro. Assim, a Vale busca avaliar tecnicamente fornecedores de SASE visando à seleção futura, considerando custos operacionais e complexidade tecnológica. O SASE, termo cunhado pelo Gartner em 2019, é uma arquitetura baseada em nuvem que combina recursos de rede e segurança para prover acesso seguro a aplicações e serviços, independentemente de onde os usuários estejam. Este estudo foca nas funcionalidades de segurança do SASE, em especial o Acesso de Confiança Zero à Rede (ZTNA). O uso de uma metodologia estruturada, a definição clara de critérios e a análise detalhada de requisitos funcionais e não-funcionais foram aplicados em uma abordagem abrangente e criteriosa na escolha de uma solução baseada em SASE para atender às necessidades específicas da Vale. A pesquisa avaliou diferentes fornecedores de soluções SASE para a Vale. A análise revelou disparidades significativas entre os fornecedores, com destaque para três deles. Verificou-se a aderência de um único fornecedor a todos os critérios da Vale, o que torna a solução deste a mais adequada para adoção na Vale.

Palavras-chave: Segurança em nuvem. Confiança-zero.

Fase da Cadeia: Cadeia de valor.

ABSTRACT

Hybrid work, driven by the pandemic, has become the new normal, with 62% of employers planning to maintain remote or hybrid work post-COVID-19. The migration to cloud data centers, essential for remote accessibility, raises concerns about data security. Traditional solutions like Virtual Private Networks (VPNs) become inefficient, requiring a review of remote access policies. Enter Secure Access Service Edge (SASE), a cloud architecture that combines functions to provide secure access. Thus, Vale seeks to technically assess SASE providers for future selection, considering operational costs and technological complexity. Coined by Gartner in 2019, SASE is a cloud-based architecture that combines network and security features to provide secure access to applications and services, regardless of user location. This study focuses on SASE's security functionalities, particularly Zero Trust Network Access (ZTNA). Using a structured methodology, clear criteria definition, and detailed analysis of functional and non-functional requirements, a comprehensive and meticulous approach was applied in choosing a SASE-based solution to meet Vale's specific needs. The research evaluated different SASE solution providers for Vale, revealing significant disparities among them, with three standing out. The adherence of a single provider to all Vale's criteria makes their solution the most suitable for adoption at Vale.

Keywords: Cloud security. Zero-trust.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

AWS	–	*Amazon Web Services*
CASB	–	*Cloud Access Security Broker*
CNPq	–	Conselho Nacional de Desenvolvimento Científico e Tecnológico
DDoS	–	*Distributed Denial-of-Service*
DIA	–	*Direct Internet Access*
DLP	–	*Data Loss Prevention*
DNF	–	*Domain Name Filtering*
DNS	–	*Domain Name System*
DNSSEC	–	*Domain Name System Security Extensions*
DPC	–	*Device Posture Check*
DPF	–	*DNS Protocol Filtering*
GCP	–	*Google Cloud Platform*
IaaS	–	*Infrastructure-as-a-Service*
IDP	–	*Identity Provider*
IPS	–	*Intrusion Prevention System*
IPv4	–	*Internet Protocol version 4*
IPv6	–	*Internet Protocol version 6*
ITOM	–	*Information Technology Operations Management*
ITSM	–	*Information Technology Service Management*
ITV	–	Instituto Tecnológico Vale
MDM	–	*Mobile Device Manager*
MI	–	Mineração
OTP	–	*One Time Password*
OVA	–	*Open Virtualization Format*
RBAC	–	*Role Based Access Control*
RBI	–	*Remote Browser Isolation*
SaaS	–	*Software-as-a-Service*
SASE	–	*Secure Access Service Edge*
SD-WAN	–	*Software-Defined Wide Area Network*
SIEM	–	*Security Information and Event Management*
SSL	–	*Secure Sockets Layer*
SWG	–	*Secure Web Gateway*
TCO	–	*Total Cost Ownership*
TLS	–	*Transport Layer Security*
UFOP	–	Universidade Federal de Ouro Preto
URL	–	*Uniform Resource Locator*
WAN	–	*Wide Area Network*
ZTNA	–	*Zero-Trust Network Access*

SUMÁRIO

1 INTRODUÇÃO

O trabalho híbrido se tornou o novo normal e um requisito para muitas organizações como resultado da pandemia. Pesquisas indicam que empregadores esperam que 62% de seus funcionários trabalhem remotamente ou de forma híbrida, mesmo após o fim das restrições relacionadas à COVID-19 (GRADY; LALIBERTE, 2021). Como resultado, várias empresas planejam suportar um modelo no qual a maioria dos empregados possa trabalhar de forma fluida nos escritórios, sites remotos, em casa ou em trânsito.

A necessidade de tornar serviços e sistemas, antes restritos às redes internas das empresas, acessíveis a partir de qualquer localidade e dispositivo, acelerou a migração para data centers em nuvem. Essa mudança traz preocupações em relação à segurança de dados, uma vez que as aplicações estão agora expostas para a Internet e portanto suscetíveis a ataques cibernéticos. O uso de redes e dispositivos não gerenciados pelas organizações torna-se um risco, visto que as políticas de segurança não são aplicáveis a estes. Ainda, o uso de tecnologias tradicionais, como redes privadas virtuais (VPNs), são ineficientes em oferecer um controle de acesso granular, e geralmente permitem acesso à toda rede uma vez que o usuário esteja conectado. Desta forma, faz-se necessário rever políticas e ferramentas de acesso remoto, assim como soluções de proteção de dados.

Com o propósito de endereçar essa nova demanda, surge o Serviço de Acesso Seguro de Borda (SASE), um modelo de arquitetura que unifica rede e segurança como um serviço em nuvem para prover acesso seguro de ponta-a-ponta. O SASE combina diferentes funções e recursos como *Software-Defined WAN* (WAN definida por software), *Zero Trust Network Access* (Acesso de confiança zero à rede), *Secure Web Gateway* (*Gateway* Web Seguro) e *Cloud Access Security Broker* (Agente de Segurança de Acesso à Nuvem) para criar um modelo único de serviço. De acordo com um relatório do Gartner, estima-se que até 2025, ao menos 60% das empresas terão estratégias explícitas para adoção de SASE, um aumento expressivo em comparação a 10% em 2020 (MACDONALD et al., 2021).

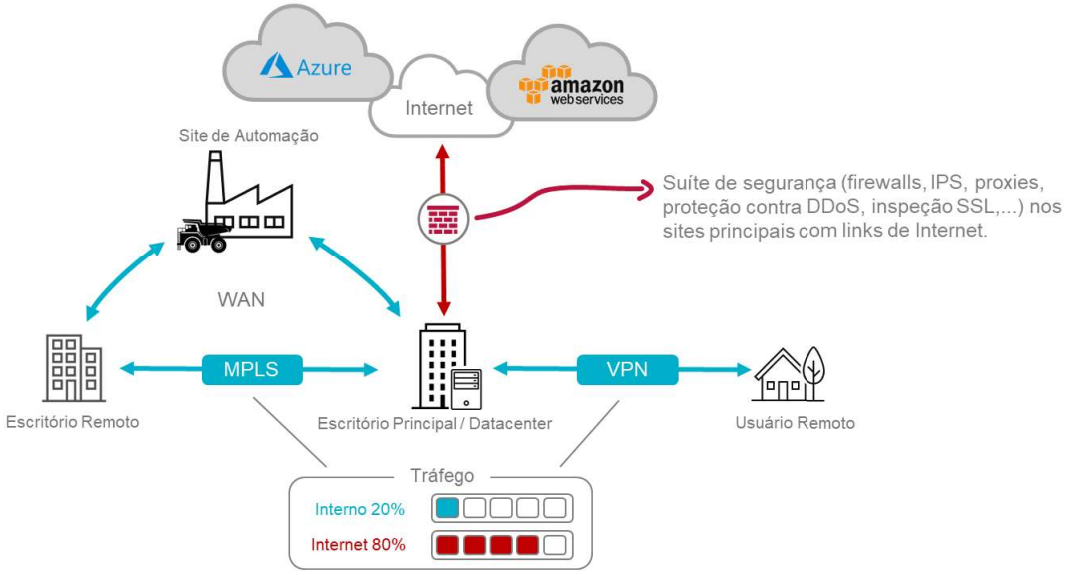
Este estudo tem por finalidade avaliar tecnicamente fornecedores e soluções de SASE disponíveis no mercado para auxiliar na tomada de decisão por um ou mais a serem adotados na VALE. Aqueles mais bem avaliados serão selecionados para uma prova de conceito, condição para futura implementação no ambiente tecnológico da Vale.

1.1 Justificativa

A transformação digital, assim como a pandemia de COVID-19, acelerou a migração de aplicações e serviços para a nuvem. O modelo de trabalho híbrido requer que a informação esteja disponível ao usuário onde quer que ele esteja, seja no escritório da empresa, filial ou mesmo em casa.

No modelo tradicional, o tráfego dos usuários remotos é redirecionado através de VPN para um infraestrutura corporativa centralizada, onde são aplicados controles de segurança, como filtro de conteúdo, inspeção de tráfego e *firewalls*, como ilustrado na Figura 1. Esta arquitetura cria gargalos de rede que comprometem a experiência do usuário, e frequentemente oferecem um acesso mais permissivo que o necessário. Uma vez que usuário se desconecta da VPN, as políticas de segurança não são mais aplicadas, o que oferece riscos. Uma outra abordagem é o acesso direto da Internet (DIA) às aplicações, expondo estas a ataques maliciosos e vazamento de dados sensíveis (Figura 2).

Figura 1 – Modelo tradicional de acesso remoto via VPN



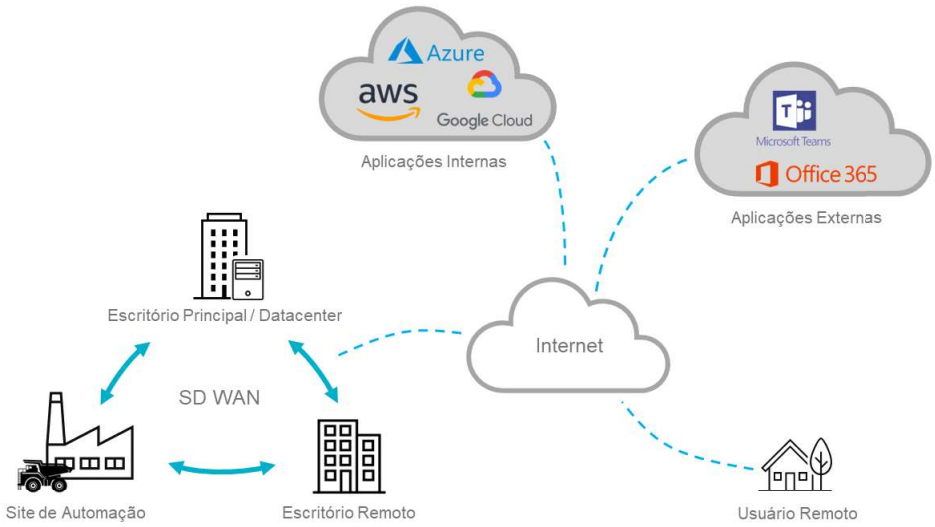
O tráfego é redirecionado para o site principal onde os controles de segurança são aplicados

Fonte: Elaboração própria.

Neste contexto, o SASE surge como resposta, em um *framework* que une recursos de rede e segurança para prover acesso seguro aos sistemas corporativos. Uma arquitetura de acesso remoto baseada em SASE remove a necessidade de expor as aplicações diretamente para a Internet, reduzindo assim a superfície de ataque. O controle de acesso é granular, disponibilizando-se ao usuário somente os recursos estritamente necessários. O modelo permite ainda a consolidação das políticas de segurança, simplificando o gerenciamento, provendo maior visibilidade e mitigação de riscos de segurança cibernética.

Devido ao alto custo operacional de uma plataforma baseada em SASE, à grande quantidade de fornecedores disponíveis, e à complexidade do ambiente tecnológico da Vale, é preciso uma análise criteriosa das soluções, considerando necessidades atuais e futuras, a fim de reduzir o custo total de operação (TCO).

Figura 2 – Acesso direto da Internet



Aplicações acessíveis pela Internet se tornam expostas a ataques

Fonte: Elaboração própria.

1.2 Objetivo

Este trabalho tem como objetivo a elaboração de uma análise quantitativa das soluções de SASE disponíveis no mercado, o que permitirá a tomada de decisão por um ou mais fornecedores que melhor atendem às necessidades da Vale. Os objetivos específicos incluem identificar fornecedores e produtos, definir critérios de avaliação e respectivos impactos e, por fim, avaliar as soluções de acordo com a metodologia adotada.

Ao final deste estudo, espera-se ter um compilado de informações de diferentes fornecedores quantificadas em um conjunto de critérios alinhados aos requisitos da Vale.

2 REFERENCIAL TEÓRICO

O termo SASE foi cunhado pelo Gartner em 2019 (MACDONALD; ORANS; SKORUPA, 2019) e pode ser definido como um modelo de arquitetura baseado em nuvem que combina recursos de rede e segurança para prover acesso seguro, conectando usuários e aplicações, independente de onde estes estejam.

2.1 Arquitetura SASE

O *framework* de arquitetura SASE engloba diferentes serviços, divididos em duas categorias: *Secure Services Edge* (SSE) e *WAN Edge Services*. Enquanto o primeiro concentra funcionalidades de segurança, o segundo aborda funções da rede de dados. As capacidades são oferecidas em um modelo "como serviço", disponíveis em uma infraestrutura em nuvem.

A Figura 3 ilustra o *framework* SASE e suas capacidades de rede - como Rede de Longa Distância Definida por Software (SD-WAN) - e funções de segurança - como *Gateway* de Web Seguro (SWG), *Broker* de Segurança de Acesso à Nuvem (CASB) e Acesso de Confiança Zero à Rede (ZTNA), para citar alguns - combinados para habilitar de forma segura a conectividade de entidades, à esquerda, com os recursos e serviços à direita.

Figura 3 – *Framework* SASE

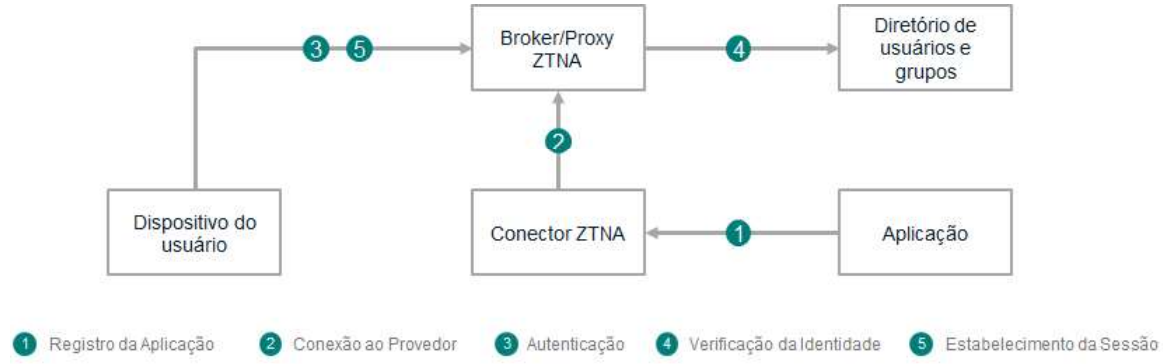
Visão detalhada do *framework* SASE

Fonte: Adaptado de MacDonald et al. (2021, p. 4).

Dentro do modelo SASE, o Gartner define duas abordagens de arquitetura para ZTNA: iniciado por serviço e iniciado por dispositivo (ORANS; RILEY, 2020). No primeiro, conectores - *gateways* na forma de máquinas virtuais ou hardware dedicados - instalados próximos às aplicações iniciam conexões em direção a uma infraestrutura do provedor. As aplicações são publicadas nos conectores, indicando que uma determinada aplicação é

acessível via um conjunto específico de conectores. As conexões iniciadas pelos usuários remotos são direcionadas à infraestrutura do provedor, habilitando-se assim um túnel criptografado entre usuários e aplicações de destino. A Figura 4 representa o modelo conceitual de ZTNA iniciado por serviço.

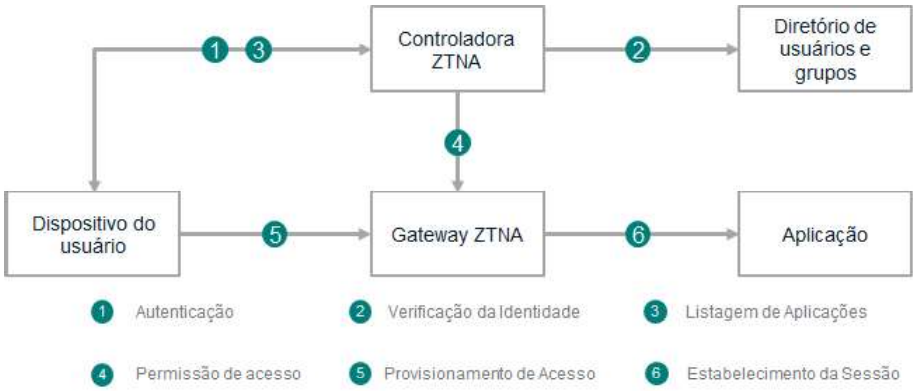
Figura 4 – Modelo Conceitual de ZTNA Iniciado por Serviço



Modelo Conceitual da Arquitetura de ZTNA Iniciado por Serviço
Fonte: Adaptado de Orans e Riley (2020, p. 6)

No ZTNA iniciado por dispositivo, uma controladora exerce a função de autenticador e autorizador, provisionando acesso através de um *gateway* localizado entre os usuários e as aplicações. Importante salientar que este modo requer o uso de um software cliente na máquina do usuário. A Figura 5 ilustra o conceito de ZTNA iniciado por dispositivo.

Figura 5 – Modelo Conceitual de ZTNA Iniciado por Dispositivo



Modelo Conceitual da Arquitetura de ZTNA Iniciado por Dispositivo
Fonte: Adaptado de Orans e Riley (2020, p. 5)

Algumas soluções de mercado dispõem de um *broker* - na forma de uma máquina virtual ou hardware dedicado - provisionado em uma rede interna local, cuja função é estender os controles de acesso da infraestrutura CASB. Este tem como principal função intermediar o tráfego entre usuários e aplicações localizados em redes internas, ainda que

segregados em zonas de segurança e instalações físicas distintas. O *broker* se integra com a plataforma em nuvem do fornecedor e sincroniza as configurações necessárias.

2.2 Capacidades SASE

Este estudo se concentra nas funcionalidades de segurança do modelo SASE, mais especificamente no ZTNA, visto que tem como foco endereçar questões de cibersegurança e aprimorar a experiência do usuário no acesso remoto ao ambiente tecnológico da Vale. As funções de rede, em especial SD-WAN, são abordadas em outras iniciativas internas na Vale. Importante dizer, no entanto, que deve haver sinergia entre os estudos, de modo que haja compatibilidade entre diferentes soluções adotadas.

As principais capacidades do modelo SASE - de acordo com o Gartner (MACDONALD et al., 2021)) - relacionadas a SSE são: SWG, CASB, ZTNA, *Firewall* como Serviço (FWaaS) e inspeção de tráfego de dados. Adicionalmente, são recomendados o Isolamento Remoto do Navegador (RBI) e Proteção de Sistemas de Nome de Domínio (DNS).

SWG é um recurso de segurança que executa filtros de conteúdo do tráfego web baseado em políticas de segurança, e efetua bloqueios de tráfego quando uma ameaça em potencial ou acesso não autorizado são identificados. O SWG implementa as seguintes tecnologias e recursos:

- Filtro de URL
- Detecção e bloqueio antimalware
- Controle de aplicativos
- Prevenção de perda de dados (DLP)

ZTNA consiste em um modelo de acesso adaptativo, baseado em identidade e contexto, no qual a confiança nunca é implícita, sendo necessário validar critérios de segurança antes de habilitar o acesso ao recurso solicitado. Uma ferramenta ZTNA pode incluir diferentes modos de acesso, utilizando-se um software cliente no dispositivo do usuário - também conhecido como agente - ou sem cliente.

CASB é um conjunto de serviços hospedados em nuvem ou localmente que intermedeia o tráfego entre usuários e provedores de nuvem, consolidando políticas de segurança e governança entre diferentes serviços de nuvem. De acordo com Lawson e Riley (2020), as principais funções do CASB são prover visibilidade, segurança de dados, conformidade e proteção contra ameaças.

RBI é uma tecnologia que aloca a sessão do navegador web do usuário em um servidor remoto, de forma a prevenir que a máquina do usuário execute código malicioso.

Proteção DNS refere-se a mecanismos de defesa contra a ataques baseados em DNS, tais como: DNSSEC (extensões de segurança do protocolo DNS, mitigação de Ataques de Negação de Serviço Distribuído (DDoS), filtro de conteúdo e outros. Dois importantes serviços de segurança compõem a base deste recurso: Filtro de Protocolo DNS (DPF) e Filtro de Nomes de Domínio (DNF)(MEF, 2022).

FWaaS é um serviço de *firewall* em nuvem, com recursos avançados de segurança, como: filtro de conteúdo e URL, prevenção de ameaças, sistemas de prevenção de intrusos (IPS), segurança de DNS e inspeção de tráfego criptografado.

2.3 Gestão de Identidades

O processo de autenticação consiste na identificação de uma entidade - usuários ou dispositivos -, enquanto a autorização define quais recursos a entidade é capaz de acessar, baseado em um conjunto de critérios e políticas (MEF, 2022). Visto que a identificação do usuário é parte fundamental em uma arquitetura de confiança-zero, é essencial que uma solução baseada em SASE inclua mecanismos necessários aos processos de autenticação e autorização de usuários e grupos. Dentro do contexto de uma ferramenta de ZTNA, diferentes métodos de autenticação são aplicáveis, como:

- Autenticação Manual - O usuário insere manualmente suas credenciais de acesso na ferramenta para efetuar *login* na plataforma.
- Autenticação via SSO - A ferramenta utiliza um serviço de SSO para autenticação do usuário, de modo que os usuários executem *login* em todos os serviços vinculados ao mesmo provedor SSO uma única vez.
- Autenticação via Certificado Digital de Usuário - A ferramenta utiliza um certificado digital de usuário, localizado em um diretório na máquina, para autenticação. O usuário é identificado através de um atributo do certificado, tais como:
  - *CN – Common Name*
  - *SAN – Subject Alternative Name*
  - *UPN – User Principal Name*

A fim de facilitar a gestão de identidades e controles de acesso, faz-se necessário a integração com sistemas provedores de identidade (IdPs), cuja função é armazenar e verificar identidades digitais, as quais identificam usuários ou dispositivos (ENTRUST, 2023). IdPs são normalmente disponibilizados como um serviço em nuvem, como o *Azure AD* e *Google Identity*. O IdP utiliza um ou mais fatores de autenticação para identificar o usuário, tais como:

- Usuário e senha
- Certificado digital de usuário ou máquina
- *Token* físico ou digital
- Biometria

O uso de múltiplos fatores para verificar a identidade do usuário é conhecido como autenticação multifator (MFA).

Um Serviço de Logon Único (SSO), é um local unificado para os usuários fazerem login em todos serviços de uma única vez, o que proporciona mais agilidade e segurança ao processo de login. Um serviço SSO usualmente verifica a identidade do usuário junto ao

IdP e implementa métodos de autenticação moderna, como o *Secure Assertion Markup Language* (SAML) e OAuth (CLOUDFLARE, 2023).

2.4 Infraestrutura

Uma vez que a solução de ZTNA se torna um recurso crítico, no sentido de ser indispensável à operação do negócio, é imprescindível que a infraestrutura de toda a plataforma e seus componentes, internos e externos, seja redundante e de alta disponibilidade (HA), de modo que, em caso de falha de um dos nós da solução, a conectividade às aplicações não seja comprometida e não haja impacto para o usuário final.

A disponibilidade em infraestrutura é um métrica que mensura o tempo que aplicações, serviços ou dispositivos estão operacionais, expressa na forma de porcentagem. Uma disponibilidade de 99,99% implica em um tempo indisponível de 52,56 minutos no período de um ano ou 4,42 minutos em um mês (TELECO, 2023).

O uso de tecnologias como SD-WAN - arquitetura de WAN virtual que permite uma combinação de serviços de transporte de dados, como serviços de Internet banda larga e rede celular, para conectar usuários a aplicativos (ARUBA, 2023) - contribui para um gerenciamento mais eficiente da infraestrutura de rede, sendo assim um componente importante na manutenção da disponibilidade dos serviços.

2.5 Sistemas Auxiliares de Gerenciamento

É importante que qualquer plataforma se integre a serviços de gestão de segurança e processos relacionados ao uso de sistemas corporativos.

O gerenciador de informações e eventos de segurança (SIEM) é uma ferramenta de monitoramento e controle de eventos relacionados à segurança da informação, que permite a análise de registros de eventos e o controle automatizado do que acontece na infraestrutura virtual de uma empresa (IBM, 2023). Para tal, o SIEM implementa ou utiliza serviços que implementam o Syslog, protocolo de transmissão de mensagens de *log* em redes IP.

Um sistema de gerenciamento de serviços de tecnologia da informação (ITSM) permite a gestão de processos e serviços que têm interface com os usuários, como gerenciamento de incidentes, processos de mudança e solicitações de acesso a um determinado recurso (SERVICENOW, 2023).

O gerenciamento de operações de tecnologia da informação (ITOM) é o processo de gerenciar o provisionamento, capacidade, custo, desempenho, segurança e disponibilidade da infraestrutura e serviços (BMC, 2023).

2.6 Modos de Acesso Remoto

Há dois modos de acesso remoto em uma arquitetura SASE: com o uso de um agente e sem o uso de um agente. Usualmente, o modo está associado ao modelo ZTNA adotado - o modelo iniciado por dispositivo requer o uso de um agente, enquanto o iniciado por serviço, não - o Gartner aponta que existe a possibilidade de uso do agente em ambos os modelos atualmente (ORANS; RILEY, 2020).

Entende-se por modo com agente o uso de um software cliente, instalado nas máquinas dos usuários e servidores, para autenticação das identidades de usuários e dispositivos. Utilizando o agente e, estando devidamente autenticado e autorizado, o usuário é capaz de se conectar às aplicações remotas de forma transparente, isto é, como se estivesse acessando uma aplicação na rede local. O agente permite a comunicação de dados entre o dispositivo cliente e as aplicações de destino via protocolos TCP e UDP. Uma funcionalidade desejável para o uso do agente é a possibilidade de habilitar ou desabilitar recursos de acordo com o perfil associado ao usuário, como por exemplo executar *logoff* no agente ou mesmo alterar as configurações do agente.

Alternativamente, no modo de acesso remoto sem agente, não há a necessidade de instalação ou execução de um software cliente dedicado na máquina do usuário. A solução conta com um portal web (doravante denominado portal ZTNA) disponibilizado na modalidade Software como Serviço (SaaS), no qual o usuário, utilizando-se apenas de um navegador de Internet, tem acesso às aplicações. A plataforma implementa controles de acesso baseado em função (RBAC), de forma que o usuário visualize somente as aplicações às quais tem permissão de acesso. O acesso via portal ZTNA pode oferecer suporte a diferentes tipos de aplicações e protocolos, tais como:

- *Remote Desktop Protocol* (RDP)
- Clientes Web (HTTPS)
- *Secure Socket Shell* (SSH)
- *Virtual Network Computing* (VNC)
- Cliente-servidor (TCP/UDP)

2.6.1 Acesso Remoto Sob Demanda

O acesso remoto sob demanda consiste em um mecanismo, disponibilizado no portal de administração da ferramenta, no qual é possível habilitar acesso temporário através do portal ZTNA para um usuário remoto não registrado no IdP da organização. As etapas do processo são:

1. Um administrador configura o acesso temporário a uma determinada aplicação, registrando o endereço de e-mail do usuário remoto;
2. Uma senha temporária (OTP) é gerada no sistema;

3. O usuário remoto recebe um e-mail com a as instruções de acesso ao portal e a senha temporária;
4. O usuário acessa o portal ZTNA e utiliza seu e-mail e a senha temporária recebida para efetuar login na plataforma;
5. O usuário remoto realiza o acesso ao sistema cujo acesso foi provisionado.

O período de acesso, assim como a validade da senha, é especificado no momento do provisionamento. O usuário remoto visualiza e acessa somente os sistemas aos quais foi autorizado.

2.7 Segurança Cibernética

Em um contexto de acesso remoto seguro de confiança zero, é relevante validar não somente o usuário, como também as condições do dispositivo utilizado para acesso. Uma Verificação de Postura do Dispositivo (DPC), consiste na avaliação do risco que este oferece baseado em um conjunto de critérios de segurança, tais como (POINT, 2023):

- Versão do sistema operacional
- *Patches* de segurança instalados
- Disponibilidade e status de software antivírus
- Rede sem fio

É recomendável uma avaliação da postura do dispositivo como requisito de acesso a um sistema ou aplicação. Outras ferramentas e recursos de segurança são intrínsecos ao *framework* SASE, como DLP, proteção contra DDoS e inspeção de tráfego criptografado, já citados anteriormente.

2.8 Licenciamento

Em um modelo de licenciamento por subscrição, é pago somente o que for de fato consumido ou utilizado de acordo com a volumetria durante o período de medição estipulado, podendo aumentar ou diminuir ao longo da vigência do contrato (THALES, 2023). Diferentes métricas são aplicáveis, como número de usuários, ativos gerenciados, volume de dados trafegados ou uma combinação destes.

3 METODOLOGIA

A pesquisa consistiu inicialmente na coleta de informações de soluções e fornecedores de arquitetura SASE disponíveis no mercado. Como ponto de partida para a seleção dos fornecedores, foram utilizados como referência o Quadrante Mágico do Gartner para SSE (WATTS et al., 2022) e o Forrester New Wave: Zero Trust Network Access (HOLMES et al., 2021). Definidos os fornecedores, um questionário (RFI) foi enviado a estes para que pudessem detalhar as características e funcionalidades de suas respectivas soluções. A RFI encontra-se disponível no Apêndice A. De 14 fornecedores contactados, 11 reponderam à RFI e 3 optaram por não participar do processo. Reuniões técnicas foram conduzidas com representantes de cada fornecedor, a fim de dirimir dúvidas.

Considerando-se as respostas dos fornecedores, a pontuação para cada critério foi definida da seguinte forma: para os casos em que a resposta não é numérica, foi atribuído um valor indicando a aderência da solução no referido quesito - 0 (não atende), 0,5 (atende parcialmente) ou 1 (atende completamente); para os demais, considerou-se o valor numérico (nominal) da resposta.

A fim de comparar as soluções de forma quantitativa, foi adotado uma metodologia de decisão com múltiplos critérios (SHIMIZU, 2010). O processo consiste primeiramente na conversão dos valores nominais de cada critério em unidades de utilidade (U), expressa como um número de 0 a 1. Importante salientar que esta etapa permite a avaliação de critérios que contribuem de forma positiva - quanto maior o valor, melhor o resultado - ou negativa - um valor maior contribui para um pior resultado - para o cálculo da pontuação. Em seguida, os pesos são também normalizados, isto é, convertidos em valores de 0 a 1. A soma de todos os pesos normalizados deve ser igual a 1. Por fim, a pontuação total de um fornecedor é dada pela utilidade conjunta, que resulta do somatório da multiplicação entre peso normalizado e utilidade de cada critério.

Os seguintes conjuntos, parâmetros e variáveis foram definidos para a análise:

- F: Conjunto de fornecedores
- C: Conjunto de requisitos
- W: Peso
- Wn: Peso normalizado
- V: Valor nominal
- U: Utilidade
- $Vmax$: Valor nominal máximo
- $Vmin$: Valor nominal mínimo
- S: Pontuação
- Ucj: Utilidade conjunta

A normalização dos valores em cada critério é efetuada da seguinte forma: para

critérios positivos, ao menor valor é atribuído 0 e ao maior valor 1. Valores intermediários são calculados utilizando-se a Fórmula 1. Para critérios negativos, ao menor valor é atribuído 1 e ao maior valor 0. Valores intermediários são calculados através da Fórmula 2. O peso normalizado de cada critério consiste no valor nominal do peso divido pelo somatório dos pesos de todos os requisitos, conforme Fórmula 3.

$$U = \frac{V - Vmin}{Vmax - Vmin} \tag{1}$$

$$U = \frac{Vmax - V}{Vmax - Vmin} \tag{2}$$

$$Wn = \frac{W_i}{\sum_{i \in C} W_i} \tag{3}$$

Seguindo a metologia, a pontuação (S) para cada critério resulta da multiplicação do peso normalizado e a utilidade (Fórmula 4).

$$S = Wn * U \tag{4}$$

Para cada fornecedor, foi calculada a utilidade conjunta, cujo valor é o somatório da pontuação do conjunto de critérios considerados, conforme Fórmula 5.

$$Ucj = \sum_{i \in C} S_i \tag{5}$$

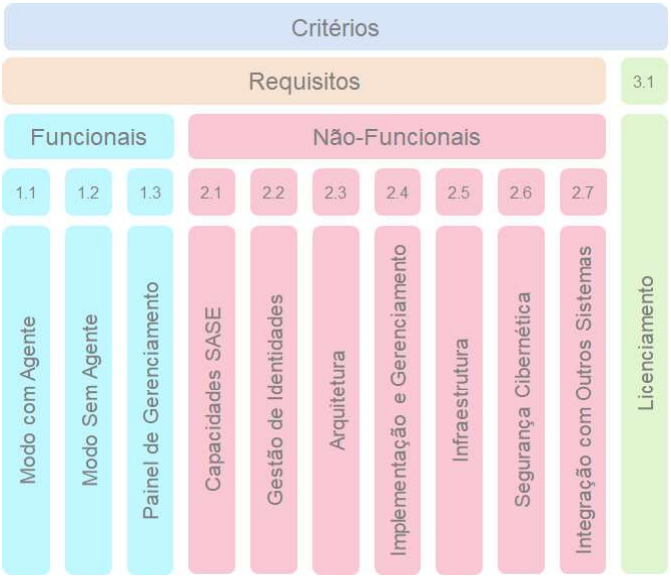
Todos os valores foram organizados em uma tabela. Foi utilizado o *software Microsoft Excel* para inserção das fórmulas e cálculos necessários. Uma vez obtidas as pontuações, foi gerado um gráfico de análise de correspondência - ferramenta estatística multivariada que representa geometricamente as correspondências (similaridades) existentes numa tabela de frequência ou contingência por meio de um gráfico que plota os dados, mostrando visualmente o resultado de dois ou mais pontos de dados (TIBCO, 2024) - utilizando-se o software *IBM SPSS Statistics*.

Após análise das respostas dos fabricantes e, considerando-se as necessidades e restrições do ambiente tecnológico da Vale, como diferentes zonas e regras de cibersegurança, segregação entre ambientes corporativo e industrial, além da grande distribuição geográfica das operações globalmente, foram definidos 61 critérios de avaliação, e destes 55 requisitos. Estes foram categorizados em duas classes principais - requisitos funcionais e não-funcionais - e subdivididos em 10 subcategorias. A categorização permitiu uma organização clara e sistemática dos critérios de avaliação, representada no *framework* da Figura 6. Importante mencionar que outros critérios inicialmente considerados foram excluídos desta avaliação devido à falta de assertividade nas respostas dos fornecedores.

Os requisitos também foram classificados em mandatórios (M) - atendem necessidades específicas de integração com sistemas, arquitetura, segurança, e operação da

Vale - ou desejáveis (D). Adicionalmente, a todos os requisitos, foi atribuído um valor inteiro de 1 a 3, que representa o peso (impacto) para o negócio. Requisitos mandatórios foram automaticamente classificados com peso 3 (alto impacto), enquanto aos demais foi atribuído o peso de 1 ou 2 (baixo e médio impacto, respectivamente). Os critérios, suas definições e classificações são apresentados a seguir.

Figura 6 – *Framework* de Critérios de Avaliação



Fonte: Elaboração própria.

3.1 Requisitos Funcionais

Requisitos funcionais tem relação com a experiência e ação do usuário. 15 requisitos foram atribuídos a esta classe e agrupados em 3 subcategorias.

3.1.1 Modo com Agente

A solução deve possuir um agente, a ser instalado em estações de trabalho, *laptops*, *tablets*, *smartphones* e servidores, para autenticação das credenciais de usuários e dispositivos. O agente deve ser compatível com os principais sistemas operacionais e suas versões. Deve-se considerar as versões de cada sistema operacional com suporte ativo do fabricante. O agente deve possuir as mesmas funcionalidades em todos os sistemas operacionais suportados. Os requisitos relacionados às funcionalidades do agente são (Tabela 1):

- Suporte ao *Windows OS* - O agente deve ser compatível com *Microsoft Windows OS*
- Suporte ao *Mac OS* - O agente deve ser compatível com *Mac OS*
- Suporte ao Linux - O agente deve ser compatível com Sistemas Operacionais Linux
- Suporte ao *Android OS* - O agente deve ser compatível com *Google Android OS*

- Suporte ao *iOS* - O agente deve ser compatível com *Apple iOS*
- Cliente Único - O agente deve ser único e consolidar todas as funções SASE da solução proposta.
- Suporte a Múltiplos Usuários - O agente deve permitir a autenticação de diferentes usuários em uma mesma máquina, incluindo usuários de diferentes organizações, domínios e IDPs. A transição de um usuário para outro deve ocorrer de forma facilitada, sem a necessidade de um novo registro do usuário na plataforma a cada *logon/logoff*.
- Múltiplos Perfis de Usuário - O agente deve oferecer suporte à diferentes perfis de usuário, que habilitam ou desabilitam recursos de acordo com o perfil associado ao usuário.

Tabela 1 – Tabela de Critérios - Modo com Agente

ID_CR	Critério/Requisito	M/D	W	Wn
1.1.1	Suporte à Windows OS	M	3	0,0188
1.1.2	Suporte à Linux OS	M	3	0,0188
1.1.3	Suporte à Mac OS	M	3	0,0188
1.1.4	Suporte à Android OS	M	3	0,0188
1.1.5	Suporte à iOS	M	3	0,0188
1.1.6	Cliente Único	M	3	0,0188
1.1.7	Suporte a Múltiplos Usuários	M	3	0,0188
1.1.8	Múltiplos Perfis de Usuário	D	1	0,0063

Fonte: Elaboração própria.

3.1.2 Modo sem Agente

A solução deve contar com um modo de acesso remoto sem uso de um agente, via portal ZTNA. As funcionalidades foram mapeadas nos seguintes requisitos (Tabela 2):

- Acesso Sem Agente - A solução deve oferecer um modo de acesso remoto sem a necessidade de instalação ou execução de um agente na máquina do usuário
- Acesso Remoto RDP Sem Agente - A solução deve oferecer suporte à clientes RDP para acesso remoto sem o uso de agente na máquina do usuário
- Acesso Remoto Sob Demanda - A solução deve prover um mecanismo, em seu portal de administração, no qual seja possível habilitar acesso temporário através do portal ZTNA para um usuário remoto que não esteja registrado no IdP da Vale.

Tabela 2 – Tabela de Critérios - Modo sem Agente

ID_CR	Critério/Requisito	M/D	W	Wn
1.2.1	Acesso Remoto RDP Sem Cliente	M	3	0,0188
1.2.2	Modo Sem Cliente	M	3	0,0188
1.2.3	Acesso Remoto Sob Demanda	D	2	0,0125

Fonte: Elaboração própria.

3.1.3 Painel de Gerenciamento

As características funcionais do painel de gerenciamento foram consolidadas em um único requisito (Tabela 3):

- Painel Único de Gerenciamento - A solução deve prover um painel único de gerenciamento, que centraliza todas as configurações da solução de SASE. A plataforma deve ser oferecida na forma de SaaS. Deve haver integração com o IdP da Vale para autenticação e autorização de todos os usuários à plataforma.

Tabela 3 – Tabela de Critérios - Painel de Gerenciamento

ID_CR	Critério/Requisito	M/D	W	Wn
1.3.1	Painel Único de Gerenciamento	M	3	0,0188

Fonte: Elaboração própria.

3.2 Requisitos Não Funcionais

Requisitos não-funcionais são aqueles que não tem relação direta com o usuário, mas representam recursos relevantes, como integração com outros sistemas e cibersegurança. Nesta classe foram categorizados 40 requisitos, agrupados em 7 subcategorias.

3.2.1 Arquitetura

Devido à especificações de cibersegurança da Vale, somente o ZTNA iniciado por serviço possui uma arquitetura aplicável para acesso remoto tanto ao ambiente corporativo quanto industrial. Este requisito determina outros critérios e componentes da solução, como suporte a proxy para os conectores e a disponibilidade de conectores em nuvem e *on-premise*. A dispersão geográfica das operações da Vale, muitas vezes em locais remotos, requer um *broker* interno para manter o tráfego de dados localmente em uma mesma região. Assim, requisitos muito específicos foram considerados nesta subcategoria (Tabela 4):

- ZTNA Iniciado por serviço - O modelo ZTNA deve ser iniciado por serviço
- Conectores em Nuvem - A solução deve permitir o provisionamento de conectores nos principais provedores de nuvem (Azure, GCP e AWS)
- Conectores *On-premise* - A solução deve oferecer conectores para instalação em redes locais internas, disponibilizados como sistemas fechados embarcados em máquinas virtuais.
- *Broker On-premise* - A solução deve dispor de um *broker* provisionado em rede interna que estenda os controles de acesso da infraestrutura CASB, disponibilizado como um sistema fechado embarcado em máquinas virtuais.
- Suporte à Proxy para o Conector - Os conectores devem possuir suporte à configuração de *proxy* de terceiros ou proprietário para intermediar a conexão com a infraestrutura CASB do provedor na nuvem.

Tabela 4 – Tabela de Critérios - Arquitetura

ID_CR	Critério/Requisito	M/D	W	Wn
2.3.1	ZTNA Iniciado por serviço	M	3	0,0188
2.3.2	Conectores em Nuvem	M	3	0,0188
2.3.3	Conectores On-premise	M	3	0,0188
2.3.4	Broker On-premise	D	2	0,0125
2.3.5	Suporte à Proxy para o Conector	M	3	0,0188

Fonte: Elaboração própria.

3.2.2 Capacidades SASE

Dentre as capacidades analisadas, ZTNA e CASB foram as principais, uma vez que uma solução de acesso remoto baseado em confiança zero e recursos de segurança em nuvem são necessidades primárias para a Vale. No entanto, é fundamental considerar demais capacidades do framework SASE, como SWG, RBI e FWaaS, visando-se uma futura arquitetura unificada. Segundo o Gartner, é recomendável selecionar fornecedores que consolidem o máximo de capacidades da arquitetura SASE em uma plataforma unificada ou que possuam um *roadmap* para disponibilização dos serviços (ORANS; RILEY, 2020). A solução deve contemplar as seguintes capacidades SSE do *framework* SASE, considerando-se uma arquitetura-alvo integrada (Tabela 5):

- SWG - A solução deve oferecer uma ferramenta de SWG
- ZTNA - A solução deve oferecer uma ferramenta de ZTNA
- CASB - A solução deve oferecer uma plataforma CASB
- RBI - A solução deve oferecer a funcionalidade de RBI
- Segurança DNS - A solução deve oferecer ferramentas de segurança de DNS
- FWaaS - A solução deve oferecer FWaaS

Tabela 5 – Tabela de Critérios - Capacidades SASE

ID_CR	Critério/Requisito	M/D	W	Wn
2.1.1	Gateway de Web Seguro (SWG)	M	3	0,0188
2.1.2	Acesso de Confiança Zero à Rede (ZTNA)	M	3	0,0188
2.1.3	Intermediador de Segurança de Acesso à Nuvem (CASB)	M	3	0,0188
2.1.4	Isolamento Remoto do Navegador (RBI)	M	3	0,0188
2.1.5	Segurança de DNS	M	3	0,0188
2.1.6	Firewall como Serviço (FWaaS)	D	1	0,0063

Fonte: Elaboração própria.

3.2.3 Gestão de Identidades

A solução deve oferecer suporte a diferentes métodos de autenticação, seja através do agente ou via portal ZTNA. Esta subcategoria inclui mecanismos e integrações necessários aos processos de autenticação e autorização dos usuários, cujos requisitos definidos foram (Tabela 6):

- Autenticação via Certificado Digital - A ferramenta deve ser capaz de autenticar o usuário utilizando um certificado digital
- Autenticação via SSO - A ferramenta deve ser compatível com serviços de SSO
- Autenticação Manual - A ferramenta deve permitir autenticação manual
- Suporte à MFA - A plataforma deve suportar autenticação multifator.
- Expiração de Sessão e Reautenticação Forçada - A solução deve prover mecanismos para forçar a reautenticação dos usuários após um período específico e de encerrar a sessão do usuário após um período de inatividade determinado.
- Suporte à Autenticação Moderna - A plataforma deve suportar métodos modernos de autenticação, como SAML 2.0 e OAuth 2.0.
- IdP Local - A solução deve incluir um IdP interno que permita o cadastro de usuários, grupos e credenciais temporárias.
- Suporte a Diferentes IdPs Simultaneamente - A ferramenta deve permitir que diferentes IdPs sejam utilizados, concomitantemente, como base de autenticação de usuários e grupos.

Tabela 6 – Tabela de Critérios - Gestão de Identidades

ID_CR	Critério/Requisito	M/D	W	Wn
2.2.1	Autenticação via Certificado Digital de Usuário	M	3	0,0188
2.2.2	Autenticação via Single-Sign-On	M	3	0,0188
2.2.3	Autenticação Manual	M	3	0,0188
2.2.4	Suporte à Autenticação Multifator (MFA)	M	3	0,0188
2.2.5	Expiração de Sessão e Reautenticação Forçada	M	3	0,0188
2.2.6	Suporte à Autenticação Moderna	M	3	0,0188
2.2.7	IDP Local	D	1	0,0063
2.2.8	Suporte a Diferentes IDPs Simultaneamente	D	2	0,0125

Fonte: Elaboração própria.

3.2.4 Implementação e Gerenciamento

A solução deve contar com funcionalidades que facilitem a implantação da ferramenta no ambiente e permitam o gerenciamento e monitoramento de forma centralizada. Os requisitos mapeados foram (Tabela 7):

- *Marketplace Azure* - A solução deve disponibilizar conectores via *marketplace* da *Azure*
- *Marketplace Amazon Web Services* (AWS) - A solução deve disponibilizar conectores via *marketplace* da AWS
- *Marketplace Google Cloud Platform* (GCP) - A solução deve disponibilizar conectores via *marketplace* da GCP
- *Marketplace Oracle Cloud* - A solução deve disponibilizar conectores via *marketplace* da *Oracle Cloud*

- *Marketplace SAP Cloud Platform* (SCP) - A solução deve disponibilizar conectores via *marketplace* da SCP
- Download através da Internet - Os pacotes de instalação de todos os softwares necessários à implantação e uso da ferramenta devem estar disponíveis para download através da Internet, incluindo o agente, OVAs, atualizações e *patches* eventualmente disponibilizados.
- Instalação e Atualizações Manuais - Deve ser possível a instalação manual, isto é, executada diretamente pelo usuário, e não através de uma ferramenta de distribuição automatizada, do agente nas máquinas de usuário e servidores.
- Instalação e Atualizações Gerenciadas - A solução deve oferecer uma ferramenta proprietária para gerenciar a instalação do agente nas máquinas e permitir o monitoramento das instalações. Alternativamente, pode ser utilizada uma plataforma de Gerenciamento de Dispositivos Móveis (MDM), como *Microsof Endpoint Manager*, *Microsoft Intune* ou *WMware Workspace ONE* para instalação, configuração e atualização, desde que haja compatibilidade com o pacote de instalação do agente.

Tabela 7 – Tabela de Critérios - Implementação e Gerenciamento

ID_CR	Critério/Requisito	M/D	W	Wn
2.4.1	Marketplace (Azure)	D	1	0,0063
2.4.2	Marketplace (AWS)	D	1	0,0063
2.4.3	Marketplace (GCP)	D	1	0,0063
2.4.4	Marketplace (Oracle)	D	1	0,0063
2.4.5	Marketplace (SAP)	D	1	0,0063
2.4.6	Download através da Internet	M	3	0,0188
2.4.7	Instalação e Atualizações Manuais	M	3	0,0188
2.4.8	Instalação e Atualizações Gerenciadas	M	3	0,0188

Fonte: Elaboração própria.

3.2.5 Infraestrutura

A solução deve possuir uma infraestrutura redundante e de alta disponibilidade, intra e inter *datacenters*, considerando-se os componentes proprietários provisionados entre o usuário e a aplicação de destino. Tendo em vista a dispersão geográfica das operações da Vale, os seguintes critérios foram considerados (Tabela 8):

- *Datacenters* no Brasil - Número de *datacenters* no Brasil deve ser igual ou superior a 2
- *Datacenters* no Canadá - Número de *datacenters* no Canadá igual ou superior a 2
- Disponibilidade - A disponibilidade da plataforma deve ser igual ou superior a 99,99%
- Suporte a IPv4 e IPv6 - A infraestrutura da plataforma ZTNA deve oferecer suporte à configuração de endereçamento de redes IPv4 e IPv6.
- Infraestrutura Redundante Intra *Datacenters* - A infraestrutura em um mesmo *datacenter* deve ter componentes em redundância

- Infraestrutura Redundante Inter *Datacenters* - A infraestrutura deve ter componentes redundantes em diferentes *datacenters*

Tabela 8 – Tabela de Critérios - Infraestrutura

ID_CR	Critério/Requisito	M/D	W	Wn
2.5.1	Datacenters no Brasil	M	3	0,0188
2.5.2	Datacenters no Canada	M	3	0,0188
2.5.3	Disponibilidade	M	3	0,0188
2.5.4	Suporte à IPv4 e IPv6	D	2	0,0125
2.5.5	Infraestrutura Redundante Intra Datacenters	M	3	0,0188
2.5.6	Infraestrutura Redundante Inter Datacenters	M	3	0,0188

Fonte: Elaboração própria.

3.2.6 Integração com Outros Sistemas

A utilização de um IdP centralizado é uma condição imprescindível ao controle de acesso a recursos e sistemas. A integração facilitada com sistemas de gestão de TI e Segurança da Informação traz agilidade na gestão de incidentes e mitigação de ameaças de cibersegurança. Assim, a integração com os seguinte sistemas e serviços é requerida (Tabela 9):

- Integração com IdP Externo para Autenticação - A solução deve ser capaz de se integrar ao *Microsoft Azure AD* e a outros IdPs para fins de autenticação de usuários e grupos.
- Integração SIEM - A solução deve oferecer integração com SIEM
- Integração Syslog - A solução deve oferecer suporte ao protocolo Syslog
- Integração ITSM/ITOM - A solução deve oferecer suporte a sistemas ITSM/ITOM
- Integração com Infraestrutura de Redes - A ferramenta deve ser compatível com hardware e tecnologias de redes de dados de outros fabricantes, como *switches*, roteadores, *proxies*, *firewalls*, SD-WAN, otimizadores e balanceadores de carga.

Tabela 9 – Tabela de Critérios - Integração com Outros Sistemas

ID_CR	Critério/Requisito	M/D	W	Wn
2.7.1	Integração com IDP Externo para Autenticação	M	3	0,0188
2.7.2	Integração SIEM	M	3	0,0188
2.7.3	Integração Syslog	M	3	0,0188
2.7.4	Integração ITSM/ITOM	D	2	0,0125
2.7.5	Integração com infraestrutura de redes	M	3	0,0188

Fonte: Elaboração própria.

3.2.7 Segurança Cibernética

A solução deve ter controles e mecanismos de defesa contra a ataques cibernéticos e vazamento de dados. Os requisitos especificados foram (Tabela 10):

- Verificação de Postura de Segurança - O agente deve ser capaz de validar as condições da máquina do usuário em relação a um conjunto de critérios de segurança antes de permitir acesso a um sistema ou aplicação.
- Prevenção de Perda de Dados - A solução deve oferecer ferramentas de DLP.
- Inspeção de tráfego SSL/TLS - A solução deve ser ter recursos de inspeção de tráfego criptografado.
- Proteção Contra DDoS - A plataforma deve oferecer mecanismos de proteção contra a ataques de DDoS.
- Descoberta de Aplicações - A solução deve ser capaz de identificar tentativas de acesso a aplicações não registradas na ferramenta.

Tabela 10 – Tabela de Critérios - Segurança Cibernética

ID_CR	Critério/Requisito	M/D	W	Wn
2.7.1	Verificação de Postura de Segurança	M	3	0,0188
2.7.2	Prevenção de Perda de Dados (DLP)	M	3	0,0188
2.7.3	Inspeção SSL/TLS	M	3	0,0188
2.7.4	Proteção Contra DDoS	M	3	0,0188
2.7.5	Descoberta de Aplicações	D	1	0,0063

Fonte: Elaboração própria.

3.3 Licenciamento

Foram avaliados 7 critérios em relação ao licenciamento. O modelo de licenciamento não foi computado no cálculo da pontuação, servindo apenas como uma forma de avaliar o comportamento adotado pelo mercado neste quesito. Considerando-se o número de usuários ativos na Vale, foram avaliados diferentes combinações de volume de usuários e período contratual para análise dos custos de licenciamento. Importante salientar que foram considerados somente os custos relacionados a implantação de uma ferramenta de ZTNA, excluindo-se assim custos com outras capacidades do SASE. Os critérios de custos de licenciamento avaliados se resumem em (Tabela 11):

- Modelo de licenciamento - Por número de usuários, número de sistemas gerenciados, volume de tráfego ou uma combinação destas métricas
- Custo 3000 usuários/1 ano - Custo de licenciamento para 3000 usuários no período de 1 ano
- Custo 3000 usuários/3 anos - Custo de licenciamento para 3000 usuários no período de 3 anos

- Custo 30000 usuários/1 ano - Custo de licenciamento para 30000 usuários no período de 1 ano
- Custo 30000 usuários/3 anos - Custo de licenciamento para 30000 usuários no período de 3 anos
- Custo 60000 usuários/1 ano - Custo de licenciamento para 60000 usuários no período de 1 ano
- Custo 60000 usuários/3 anos - Custo de licenciamento para 60000 usuários no período de 3 anos

Tabela 11 – Tabela de Critérios - Licenciamento

ID_CR	Critério/Requisito	M/D	W	Wn
3.1.1	Cost - 3000 users/1 year	n/a	3	0,0188
3.1.2	Cost - 3000 users/3 years	n/a	3	0,0188
3.1.3	Cost - 30000 users/1 year	n/a	3	0,0188
3.1.4	Cost - 30000 users/3 years	n/a	3	0,0188
3.1.5	Cost - 60000 users/1 year	n/a	3	0,0188
3.1.6	Cost - 60000 users/3 years	n/a	3	0,0188

Fonte: Elaboração própria.

4 RESULTADOS E DISCUSSÕES

Considerando-se a confidencialidade das informações fornecidas pelos fornecedores e, visto que algumas respostas apresentadas permitiriam a identificação destes, os valores nominais foram omitidos das tabelas e representações gráficas, apresentando-se assim somente os valores normalizados. Da mesma forma, os nomes dos fornecedores são aqui representados por letras de A a K.

A Figura 7 apresenta um gráfico de proporção do modelo ZTNA adotado pelos fornecedores. Observa-se que a maior parte - 64% - opta pelo modelo iniciado por serviço, em acordo com o requisito de arquitetura-alvo definido para a Vale. Este resultado está em linha com o que foi avaliado durante as entrevistas com representantes dos fornecedores, com alguns inclusive apresentando *roadmaps* indicando uma transição para este modelo. Esta tendência é justificada possivelmente em função da maior diversidade de opções de acesso remoto proporcionado por este modelo, com suporte a modos com e sem uso de um agente e compatibilidade com diferentes protocolos.

Figura 7 – Gráfico Percentual do Modelo ZTNA Adotado

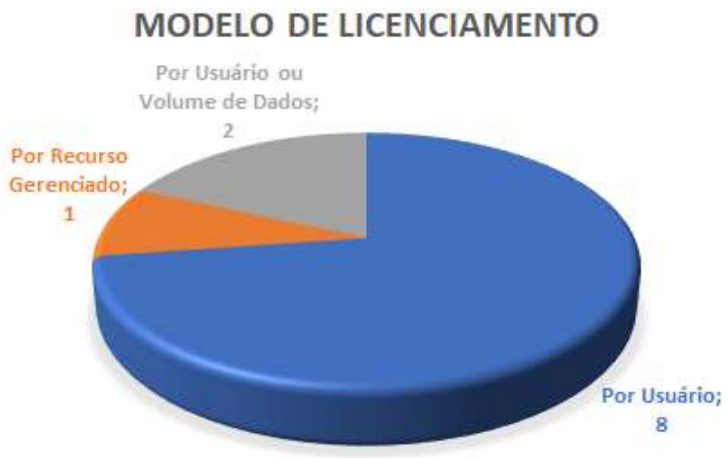
Fonte: Elaboração própria.

A Figura 8 apresenta um gráfico de proporção do tipo de licenciamento aplicado pelos fornecedores. Nota-se a preferência pelo modelo baseado em volume de usuários, com aproximadamente 73% dos fornecedores adotando unicamente este modelo e cerca de 91% oferecendo-o como uma das opções. Apenas 1 fornecedor oferece exclusivamente um modelo baseado em número de ativos gerenciados[1]. Deve-se considerar, portanto, a escalabilidade ao longo do tempo do número de usuários - e consequentemente dos custos -

[1]Neste caso, utilizou-se um número fixo de servidores para o cálculo dos custos de licenciamento.

ao adotar uma plataforma SASE, visto que há restrições na oferta por outros modelos de licenciamento que podem ser mais vantajosos.

Figura 8 – Gráfico Percentual do Modelo de Licenciamento Adotado



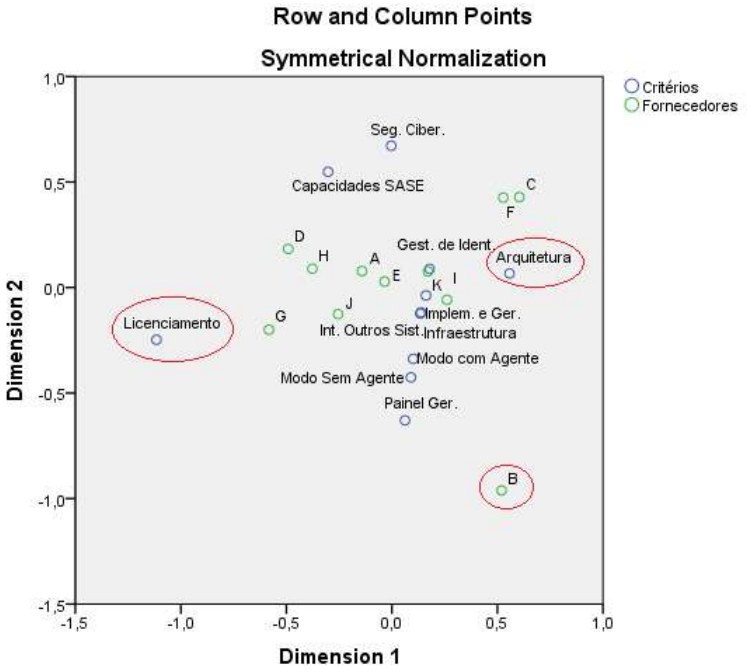
Fonte: Elaboração própria.

A Tabela 12 apresenta os valores de Utilidade obtidos para os critérios de custo associados ao licenciamento de uma ferramenta de ZTNA. Observa-se uma disparidade grande de valores entre os fornecedores, evidenciado pela análise do gráfico de correspondência da Figura 9, o qual ilustra os fornecedores afastados do critério de licenciamento. Observa-se que alguns fornecedores oferecem apenas um modelo de licenciamento que inclui todas as capacidades SASE em um único pacote, dificultando não só a comparação, mas também uma adoção faseada de funcionalidades.

Ainda sobre os custos de licenciamento, é possível notar que alguns fornecedores se sobressaem em propostas com baixo número de usuários, enquanto outros tem propostas melhores para um volume maior de licenças. Observa-se também que o tempo de contrato não exerce influência relevante, ainda que todos os fornecedores ofereçam algum tipo de desconto para contratos mais longos. A comparação entre a Figura 10, Figura 11 e Figura 12 permite uma percepção melhor da troca de posição no ranking de fornecedores de acordo com o número de licenças e tempo de contrato.

A Tabela 13 traz os valores de Pontuação agrupados em categorias, utilizados para gerar o gráfico de análise de correspondência da Figura 9. A análise de ambas nos permite inferir sobre pontos fortes e fracos dos fornecedores. Observa-se, por exemplo, uma baixa aderência do fornecedor B aos critérios de Segurança Cibernética e Capacidades SASE, em contraste com os demais, o que resulta em uma baixa pontuação total deste. Critérios de Arquitetura também foram determinantes na avaliação, com uma baixa aderência dos fornecedores D, G, I e J, uma vez que estes optam por uma arquitetura mais tradicional

Figura 9 – Gráfico de Análise de Correspondência entre Fornecedores e Critérios Avaliados



O gráfico ilustra a correspondência entre fornecedores e critérios distribuídos em categorias.

Fonte: Gerado com software *IBM SPSS Statistics*.

Tabela 12 – Tabela de Utilidade dos Custos de Licenciamento

		A	B	C	D	E	F	G	H	I	J	K
Critério/Requisito	M/D	U	U	U	U	U	U	U	U	U	U	U
Custo - 3000 usuários/1 ano	n/a	0,79	0,12	0,08	0,94	0,66	0,00	1,00	0,95	0,89	0,89	0,51
Custo - 3000 usuários/3 anos	n/a	0,82	0,05	0,00	0,95	0,63	0,26	1,00	0,97	0,03	0,88	0,62
Custo - 30000 usuários/1 ano	n/a	0,78	0,56	0,00	0,82	0,63	0,02	0,97	1,00	0,20	0,71	0,49
Custo - 30000 usuários/3 anos	n/a	0,81	0,56	0,00	0,83	0,62	0,28	0,96	1,00	0,56	0,70	0,61
Custo - 60000 usuários/1 ano	n/a	0,88	0,65	0,46	0,85	0,86	0,34	0,97	1,00	0,00	0,76	0,63
Custo - 60000 usuários/3 anos	n/a	0,84	0,41	0,09	0,76	0,75	0,22	0,93	1,00	0,00	0,59	0,53

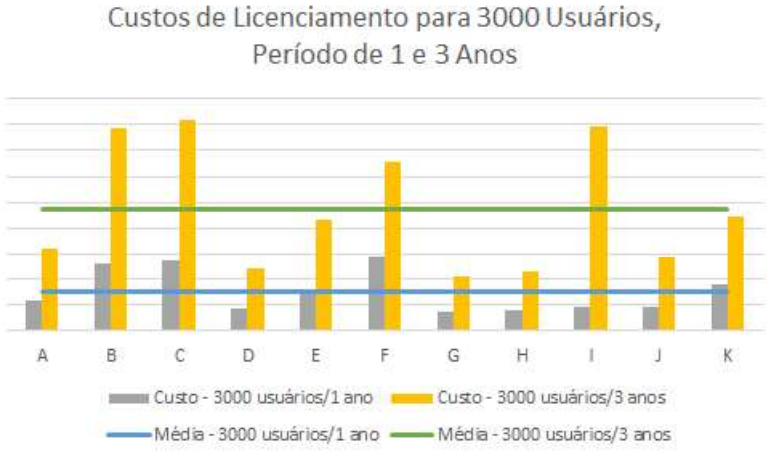
Fonte: Elaboração própria.

baseada em hardware e túneis VPN com conexões bidirecionais, em contraponto à tendência de mercado por um modelo mais escalável baseado em software e conexões em um único sentido. Entre os fornecedores com maior Pontuação - E, H e K - o baixo suporte ao Modo Sem Agente do fornecedor H o prejudica em relação aos demais, o que sugere uma menor maturidade da solução deste.

A Tabela 14 apresenta os valores de Utilidade para todos os critérios avaliados. Considerando-se somente os três melhores resultados, tem-se, do maior para o menor, os fornecedores K, H e E. Observa-se que os valores totais destes se destacam positivamente em relação aos demais, com proeminência do primeiro colocado. Importante ratificar, no entanto, que o cálculo da Utilidade não leva em consideração o peso de cada critério.

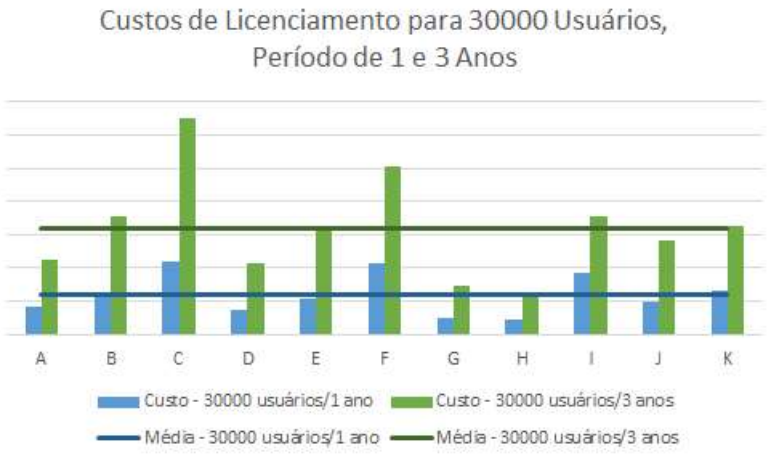
A Tabela 15 traz a Pontuação dos fornecedores em cada critério. Considerando-se as três melhores pontuações, temos os fornecedores K, E e H, em ordem do maior para o

Figura 10 – Gráfico de Estatística de Custos de Licenciamento para 3000 Usuários



Comparação entre os custos de licenciamento para 3000 usuários por períodos de 1 e 3 anos de contrato.
Fonte: Elaboração própria.

Figura 11 – Gráfico de Estatística de Custos de Licenciamento para 30000 Usuários

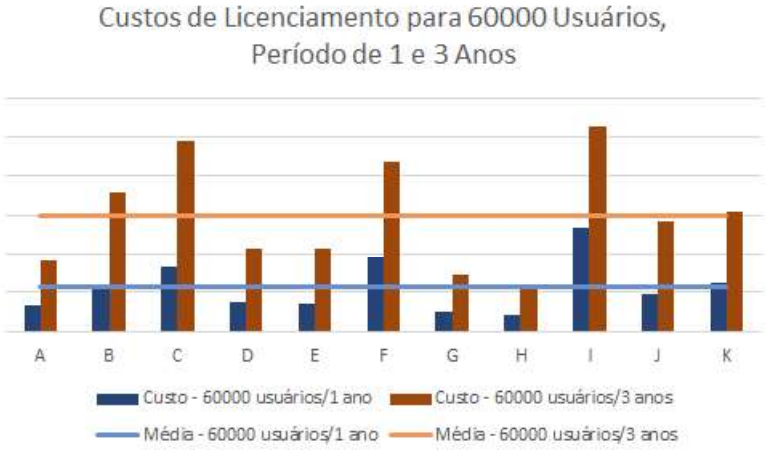


Comparação entre os custos de licenciamento para 30000 usuários por períodos de 1 e 3 anos de contrato.
Fonte: Elaboração própria.

menor resultado. Visto que ocorre troca na ordem dos fornecedores E e H, em benefício de E, em comparação com a análise de Utilidade, conclui-se que o peso de cada critério exerce de fato relevância na análise considerando-se as necessidades da Vale. Observa-se ainda uma aderência de aproximadamente 91% da solução do fornecedor K aos critérios mapeados, o que evidencia um maior nível de maturidade desta em comparação às demais. Este resultado sugere a solução do fornecedor K como mais adequada para ser implementada no ambiente da Vale.

A Tabela 16 apresenta os valores de Utilidade apenas para os requisitos mandatórios. Observa-se que apenas o fornecedor K atende completamente a todos os critérios

Figura 12 – Gráfico de Estatística de Custos de Licenciamento para 60000 Usuários



Comparação entre os custos de licenciamento para 60000 usuários por períodos de 1 e 3 anos de contrato.

Fonte: Elaboração própria.

Tabela 13 – Tabela de Pontuação por Categoria

	A	B	C	D	E	F	G	H	I	J	K
Categoria	S	S	S	S	S	S	S	S	S	S	S
Arquitetura	0,0750	0,0750	0,0750	0,0375	0,0750	0,0750	0,0375	0,0688	0,0375	0,0375	0,0875
Implementação e Gerenciamento	0,0563	0,0625	0,0625	0,0563	0,0563	0,0563	0,0563	0,0688	0,0563	0,0563	0,0750
Infraestrutura	0,0754	0,0689	0,0446	0,0579	0,0969	0,0567	0,0312	0,0751	0,0618	0,0703	0,0805
Capacidades SASE	0,0750	0,0188	0,0813	0,1000	0,1000	0,0750	0,1000	0,1000	0,0813	0,0813	0,1000
Gestão de Identidades	0,1313	0,1000	0,1125	0,1125	0,1063	0,1219	0,1000	0,0938	0,1250	0,1250	0,1250
Integração com Outros Sistemas	0,0750	0,0875	0,0750	0,0750	0,0875	0,0750	0,0750	0,0875	0,0750	0,0750	0,0875
Licenciamento	0,0923	0,0442	0,0117	0,0965	0,0779	0,0210	0,1093	0,1110	0,0315	0,0848	0,0635
Modo com Agente	0,0813	0,1375	0,1188	0,1000	0,1188	0,0813	0,1375	0,1188	0,1375	0,1375	0,1375
Modo Sem Cliente	0,0438	0,0500	0,0375	0,0375	0,0500	0,0188	0,0500	0,0281	0,0375	0,0188	0,0500
Painel de Gerenciamento	0,0188	0,0188	0,0000	0,0000	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Segurança Cibernética	0,0750	0,0188	0,0750	0,0594	0,0750	0,0688	0,0563	0,0813	0,0563	0,0563	0,0813
Total	0,7990	0,6818	0,6938	0,7325	0,8623	0,6683	0,7717	0,8517	0,7183	0,7614	0,9065

Fonte: Elaboração própria.

obrigatórios. Este e resultados anteriormente observados permitem concluir que a solução de arquitetura SASE do fornecedor K é a mais adequada, considerando-se as necessidades do ambiente tecnológico da Vale.

Tabela 14 – Tabela de Utilidade por Critério

		A	B	C	D	E	F	G	H	I	J	K
Critério/Requisito	M/D	U	U	U	U	U	U	U	U	U	U	U
Marketplace (Azure)	D	0	0	0	0	0	0	0	1	0	0	1
Marketplace (AWS)	D	0	1	0	0	0	0	0	1	0	0	1
Marketplace (GCP)	D	0	0	1	0	0	0	0	0	0	0	1
Marketplace (Oracle)	D	0	0	0	0	0	0	0	0	0	0	0
Marketplace (SAP)	D	0	0	0	0	0	0	0	0	0	0	0
Download através da Internet	M	1	1	1	1	1	1	1	1	1	1	1
Instalação e Atualizações Manuais	M	1	1	1	1	1	1	1	1	1	1	1
Instalação e Atualizações Gerenciadas	M	1	1	1	1	1	1	1	1	1	1	1
Painel Único de Gerenciamento	M	1	1	0	0	1	1	1	1	1	1	1
ZTNA Iniciado por serviço	M	1	1	1	0	1	1	0	1	0	0	1
Conectores em Nuvem	M	1	1	1	1	1	1	1	1	1	1	1
Conectores On-premise	M	1	1	1	1	1	1	1	1	1	1	1
Broker On-premise	D	0	0	0	0	0	0	0	1	0	0	1
Suporte à Proxy para o Conector	M	1	1	1	0	1	1	0	0	0	0	1
Datacenters no Brasil	M	0,04	0,04	0,04	0,09	1,00	0,04	0,00	0,17	0,13	0,09	0,13
Datacenters no Canada	M	0,33	0,17	0,33	0,33	0,50	0,00	0,67	0,50	0,50	1	0,5
Disponibilidade	M	0,98	0,8	0	1	1	0,98	0,998	0,998	0,998	0,998	0,998
Suporte à IPv4 e IPv6	D	1	1	0	1	1	0	0	0,5	1	1	1
Gateway de Web Seguro (SWG)	M	1	0	1	1	1	1	1	1	1	1	1
Acesso de Confiança Zero à Rede (ZTNA)	M	1	1	1	1	1	1	1	1	1	1	1
Intermediador de Segurança de Acesso à Nuvem (CASB)	M	1	0	1	1	1	1	1	1	1	1	1
Isolamento Remoto do Navegador (RBI)	M	0	0	1	1	1	1	1	1	0	0	1
Segurança de DNS	M	1	0	0	1	1	0	1	1	1	1	1
Firewall como Serviço (FWaaS)	D	0	0	1	1	1	0	1	1	1	1	1
Acesso Remoto RDP Sem Cliente	M	1	1	1	1	1	0	1	0,5	1	0	1
Verificação de Postura de Segurança	M	1	0	1	1	1	1	1	1	1	1	1
Prevenção de Perda de Dados (DLP)	M	1	0	1	1	1	1	1	1	1	1	1
Inspeção SSL/TLS	M	1	0	1	0	1	0,5	0	1	0	0	1
Proteção Contra DDoS	M	1	1	1	1	1	1	1	1	1	1	1
Suporte à Windows OS	M	1	1	1	1	1	1	1	1	1	1	1
Suporte à Linux OS	M	1	1	1	1	1	0	1	1	1	1	1
Suporte à Mac OS	M	1	1	1	1	1	1	1	1	1	1	1
Suporte à Android OS	M	0	1	1	1	1	0	1	1	1	1	1
Suporte à iOS	M	0	1	1	1	1	0	1	1	1	1	1
Modo Sem Cliente	M	1	1	1	1	1	1	1	1	1	1	1
Cliente Único	M	1	1	1	0	1	1	1	1	1	1	1
Suporte a Múltiplos Usuários	M	0	1	0	0	0	1	1	0	1	1	1
Múltiplos Perfis de Usuário	D	1	1	1	1	1	1	1	1	1	1	1
Autenticação via Certificado Digital de Usuário	M	1	1	1	1	1	1	1	1	1	1	1
Autenticação via Single-Sign-On	M	1	0	0	1	0	0,5	0	0	1	1	1
Autenticação Manual	M	1	1	1	1	1	1	1	1	1	1	1
Acesso Remoto Sob Demanda	D	0,5	1	0	0	1	0	1	0	0	0	1
Infraestrutura Redundante Intra Datacenters	M	1	1	1	1	1	1	0	1	0	0	1
Infraestrutura Redundante Inter Datacenters	M	1	1	1	0	1	1	0	1	1	1	1
Suporte à Autenticação Multifator (MFA)	M	1	1	1	1	1	1	1	1	1	1	1
Expiração de Sessão e Reautenticação Forçada	M	1	1	1	1	1	1	1	1	1	1	1
Suporte à Autenticação Moderna	M	1	1	1	1	1	1	1	1	1	1	1
IDP Local	D	1	1	1	0	0	1	1	0	0	0	0
Suporte a Diferentes IDPs Simultaneamente	D	1	0	1	0	1	1	0	0	1	1	1
Integração com IDP Externo para Autenticação e Autorização	M	1	1	1	1	1	1	1	1	1	1	1
Integração SIEM	M	1	1	1	1	1	1	1	1	1	1	1
Integração Syslog	M	1	1	1	1	1	1	1	1	1	1	1
Integração ITSM/ITOM	D	0	1	0	0	1	0	0	1	0	0	1
Integração com infraestrutura de redes	M	1	1	1	1	1	1	1	1	1	1	1
Descoberta de Aplicações	D	0	0	0	0,5	0	0,5	0	1	0	0	1
Custo - 3000 usuários/1 ano	n/a	0,79	0,12	0,08	0,94	0,66	0,00	1,00	0,95	0,89	0,89	0,51
Custo - 3000 usuários/3 anos	n/a	0,82	0,05	0,00	0,95	0,63	0,26	1,00	0,97	0,03	0,88	0,62
Custo - 30000 usuários/1 ano	n/a	0,78	0,56	0,00	0,82	0,63	0,02	0,97	1,00	0,20	0,71	0,49
Custo - 30000 usuários/3 anos	n/a	0,81	0,56	0,00	0,83	0,62	0,28	0,96	1,00	0,56	0,70	0,61
Custo - 60000 usuários/1 ano	n/a	0,88	0,65	0,46	0,85	0,86	0,34	0,97	1,00	0,00	0,76	0,63
Custo - 60000 usuários/3 anos	n/a	0,84	0,41	0,09	0,76	0,75	0,22	0,93	1,00	0,00	0,59	0,53
Total		44,78	39,36	40,00	41,07	48,66	37,64	43,49	49,59	40,31	42,61	54,02

Fonte: Elaboração própria.

Tabela 15 – Tabela de Pontuação por Critério

		A	B	C	D	E	F	G	H	I	J	K
Critério/Requisito	M/D	S	S	S	S	S	S	S	S	S	S	S
Marketplace (Azure)	D	0	0	0	0	0	0	0	0,0063	0	0	0,0063
Marketplace (AWS)	D	0	0,0063	0	0	0	0	0	0,0063	0	0	0,0063
Marketplace (GCP)	D	0	0	0,0063	0	0	0	0	0	0	0	0,0063
Marketplace (Oracle)	D	0	0	0	0	0	0	0	0	0	0	0
Marketplace (SAP)	D	0	0	0	0	0	0	0	0	0	0	0
Download através da Internet	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Instalação e Atualizações Manuais	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Instalação e Atualizações Gerenciadas	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Painel Único de Gerenciamento	M	0,0188	0,0188	0	0	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
ZTNA Iniciado por serviço	M	0,0188	0,0188	0,0188	0	0,0188	0,0188	0	0,0188	0	0	0,0188
Conectores em Nuvem	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Conectores On-premise	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Broker On-premise	D	0	0	0	0	0	0	0	0,0125	0	0	0,0125
Suporte à Proxy para o Conector	M	0,0188	0,0188	0,0188	0	0,0188	0,0188	0	0	0	0	0,0188
Datacenters no Brasil	M	0,0008	0,0008	0,0008	0,0016	0,0188	0,0008	0	0,0033	0,0024	0,0016	0,0024
Datacenters no Canada	M	0,0063	0,0031	0,0063	0,0063	0,0094	0	0,0125	0,0094	0,0094	0,0188	0,0094
Disponibilidade	M	0,0184	0,015	0	0,0188	0,0188	0,0184	0,0187	0,0187	0,0187	0,0187	0,0187
Suporte à IPv4 e IPv6	D	0,0125	0,0125	0	0,0125	0,0125	0	0	0,0063	0,0125	0,0125	0,0125
Gateway de Web Seguro (SWG)	M	0,0188	0	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Acesso de Confiança Zero à Rede (ZTNA)	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Intermediador de Segurança de Acesso à Nuvem (CASB)	M	0,0188	0	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Isolamento Remoto do Navegador (RBI)	M	0	0	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0	0	0,0188
Segurança de DNS	M	0,0188	0	0	0,0188	0,0188	0	0,0188	0,0188	0,0188	0,0188	0,0188
Firewall como Serviço (FWaaS)	D	0	0	0,0063	0,0063	0,0063	0	0,0063	0,0063	0,0063	0,0063	0,0063
Acesso Remoto RDP Sem Cliente	M	0,0188	0,0188	0,0188	0,0188	0,0188	0	0,0188	0,0094	0,0188	0	0,0188
Verificação de Postura de Segurança	M	0,0188	0	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Prevenção de Perda de Dados (DLP)	M	0,0188	0	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Inspeção SSL/TLS	M	0,0188	0	0,0188	0	0,0188	0,0094	0	0,0188	0	0	0,0188
Proteção Contra DDoS	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Suporte à Windows OS	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Suporte à Linux OS	M	0,0188	0,0188	0,0188	0,0188	0,0188	0	0,0188	0,0188	0,0188	0,0188	0,0188
Suporte à Mac OS	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Suporte à Android OS	M	0	0,0188	0,0188	0,0188	0,0188	0	0,0188	0,0188	0,0188	0,0188	0,0188
Suporte à iOS	M	0	0,0188	0,0188	0,0188	0,0188	0	0,0188	0,0188	0,0188	0,0188	0,0188
Modo Sem Cliente	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Cliente Único	M	0,0188	0,0188	0,0188	0	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Suporte a Múltiplos Usuários	M	0	0,0188	0	0	0	0,0188	0,0188	0	0,0188	0,0188	0,0188
Múltiplos Perfis de Usuário	D	0,0063	0,0063	0,0063	0,0063	0,0063	0,0063	0,0063	0,0063	0,0063	0,0063	0,0063
Autenticação via Certificado Digital de Usuário	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Autenticação via Single-Sign-On	M	0,0188	0	0	0,0188	0	0,0094	0	0	0,0188	0,0188	0,0188
Autenticação Manual	M	0,0188	0,01875	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Acesso Remoto Sob Demanda	D	0,0063	0,0125	0	0	0,0125	0	0,0125	0	0	0	0,0125
Infraestrutura Redundante Intra Datacenters	M	0,0188	0,01875	0,0188	0,0188	0,0188	0,0188	0	0,0188	0	0	0,0188
Infraestrutura Redundante Inter Datacenters	M	0,0188	0,01875	0,0188	0	0,0188	0,0188	0	0,0188	0,0188	0,0188	0,0188
Suporte à Autenticação Multifator (MFA)	M	0,0188	0,01875	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Expiração de Sessão e Reautenticação Forçada	M	0,0188	0,01875	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Suporte à Autenticação Moderna	M	0,0188	0,01875	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
IDP Local	D	0,0063	0,00625	0,0063	0	0	0,0063	0,0063	0	0	0	0
Suporte a Diferentes IDPs Simultaneamente	D	0,0125	0	0,0125	0	0,0125	0,0125	0	0	0,0125	0,0125	0,0125
Integração com IDP Externo para Autenticação e Autorização	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Integração SIEM	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Integração Syslog	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Integração ITSM/ITOM	D	0	0,0125	0	0	0,0125	0	0	0,0125	0	0	0,0125
Integração com infraestrutura de redes	M	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188	0,0188
Descoberta de Aplicações	D	0	0	0	0,0031	0	0,0031	0	0,0063	0	0	0,0063
Custo - 3000 usuários/1 ano	n/a	0,0148	0,0023	0,0015	0,0175	0,0124	0	0,0188	0,0179	0,0167	0,0167	0,0095
Custo - 3000 usuários/3 anos	n/a	0,0154	0,0009	0	0,0179	0,0119	0,0049	0,0188	0,0182	0,0006	0,0165	0,0115
Custo - 30000 usuários/1 ano	n/a	0,0146	0,0106	0	0,0154	0,0118	0,0003	0,0182	0,0188	0,0037	0,0132	0,0092
Custo - 30000 usuários/3 anos	n/a	0,0151	0,0104	0	0,0156	0,0116	0,0052	0,018	0,0188	0,0105	0,0131	0,0115
Custo - 60000 usuários/1 ano	n/a	0,0166	0,0122	0,0086	0,0159	0,0161	0,0064	0,0181	0,0188	0	0,0142	0,0118
Custo - 60000 usuários/3 anos	n/a	0,0157	0,0077	0,0017	0,0143	0,0141	0,0042	0,0174	0,0188	0	0,011	0,0099
Total		0,7990	0,6818	0,6938	0,7325	0,8623	0,6683	0,7717	0,8517	0,7183	0,7614	0,9065

Fonte: Elaboração própria.

Tabela 16 – Tabela de Utilidade dos Requisitos Mandatórios

		A	B	C	D	E	F	G	H	I	J	K
Critério/Requisito	M/D	U	U	U	U	U	U	U	U	U	U	U
Download através da Internet	M	1	1	1	1	1	1	1	1	1	1	1
Instalação e Atualizações Manuais	M	1	1	1	1	1	1	1	1	1	1	1
Instalação e Atualizações Gerenciadas	M	1	1	1	1	1	1	1	1	1	1	1
Painel Único de Gerenciamento	M	1	1	0	0	1	1	1	1	1	1	1
ZTNA Iniciado por serviço	M	1	1	1	0	1	1	0	1	0	0	1
Conectores em Nuvem	M	1	1	1	1	1	1	1	1	1	1	1
Conectores On-premise	M	1	1	1	1	1	1	1	1	1	1	1
Suporte à Proxy para o Conector	M	1	1	1	0	1	1	0	0	0	0	1
Datacenters no Brasil	M	0,04	0,04	0,04	0,09	1,00	0,04	0,00	0,17	0,13	0,09	0,13
Datacenters no Canada	M	0,33	0,17	0,33	0,33	0,50	0,00	0,67	0,50	0,50	1	0,5
Disponibilidade	M	0,98	0,8	0	1	1	0,98	0,998	0,998	0,998	0,998	0,998
Gateway de Web Seguro (SWG)	M	1	0	1	1	1	1	1	1	1	1	1
Acesso de Confiança Zero à Rede (ZTNA)	M	1	1	1	1	1	1	1	1	1	1	1
Intermediador de Segurança de Acesso à Nuvem (CASB)	M	1	0	1	1	1	1	1	1	1	1	1
Isolamento Remoto do Navegador (RBI)	M	0	0	1	1	1	1	1	1	0	0	1
Segurança de DNS	M	1	0	0	1	1	0	1	1	1	1	1
Acesso Remoto RDP Sem Cliente	M	1	1	1	1	1	0	1	0,5	1	0	1
Verificação de Postura de Segurança	M	1	0	1	1	1	1	1	1	1	1	1
Prevenção de Perda de Dados (DLP)	M	1	0	1	1	1	1	1	1	1	1	1
Inspeção SSL/TLS	M	1	0	1	0	1	0,5	0	1	0	0	1
Proteção Contra DDoS	M	1	1	1	1	1	1	1	1	1	1	1
Suporte à Windows OS	M	1	1	1	1	1	1	1	1	1	1	1
Suporte à Linux OS	M	1	1	1	1	1	0	1	1	1	1	1
Suporte à Mac OS	M	1	1	1	1	1	1	1	1	1	1	1
Suporte à Android OS	M	0	1	1	1	1	0	1	1	1	1	1
Suporte à iOS	M	0	1	1	1	1	0	1	1	1	1	1
Modo Sem Cliente	M	1	1	1	1	1	1	1	1	1	1	1
Cliente Único	M	1	1	1	0	1	1	1	1	1	1	1
Suporte a Múltiplos Usuários	M	0	1	0	0	0	1	1	0	1	1	1
Autenticação via Certificado Digital de Usuário	M	1	1	1	1	1	1	1	1	1	1	1
Autenticação via Single-Sign-On	M	1	0	0	1	0	0,5	0	0	1	1	1
Autenticação Manual	M	1	1	1	1	1	1	1	1	1	1	1
Infraestrutura Redundante Intra Datacenters	M	1	1	1	1	1	1	0	1	0	0	1
Infraestrutura Redundante Inter Datacenters	M	1	1	1	0	1	1	0	1	1	1	1
Suporte à Autenticação Multifator (MFA)	M	1	1	1	1	1	1	1	1	1	1	1
Expiração de Sessão e Reautenticação Forçada	M	1	1	1	1	1	1	1	1	1	1	1
Suporte à Autenticação Moderna	M	1	1	1	1	1	1	1	1	1	1	1
Integração com IDP Externo para Autenticação e Autorização	M	1	1	1	1	1	1	1	1	1	1	1
Integração SIEM	M	1	1	1	1	1	1	1	1	1	1	1
Integração Syslog	M	1	1	1	1	1	1	1	1	1	1	1
Integração com infraestrutura de redes	M	1	1	1	1	1	1	1	1	1	1	1

Fonte: Elaboração própria.

5 CONCLUSÕES

Este trabalho teve como objetivo a elaboração de uma análise quantitativa das soluções de arquitetura SASE disponíveis no mercado, a fim de permitir a seleção por um ou mais fornecedores que melhor atendem às necessidades da Vale.

A metodologia empregada na coleta de informações - RFI e reuniões com representantes de cada fornecedor - mostrou-se eficiente, ainda que alguns fornecedores não tenham respondido da forma esperada a todas as perguntas do questionário aplicado.

A análise das respostas dos fornecedores permitiu identificar tendências de mercado, como a preferência por um modelo de licenciamento baseado em número de usuários e adoção de uma arquitetura ZTNA do tipo iniciada por serviço. Esta última está alinhada com o requisito de arquitetura-alvo definida para a Vale.

A metodologia utilizada para o cálculo das pontuações revelou-se assertiva, visto que permitiu uma análise quantitativa das diferentes soluções avaliadas, levando-se em consideração especificidades, necessidades e restrições do ambiente da Vale, mapeados na forma de critérios, requisitos e grau de relevância (peso). A definição dos critérios e a escolha de um método de cálculo foram as contribuições mais relevantes deste estudo, visto que podem ser podem ser replicadas em futuras avaliações.

A análise dos resultados permitiu determinar o fornecedor K como o mais adequado para a implantação de uma solução baseada em SASE na Vale, cumprindo-se assim o objetivo do estudo. Verificou-se ainda que requisitos de arquitetura tiveram baixa aderência em um grupo de fornecedores - D, G, I e J - e uma grande disparidade nos custos de licenciamento, em alguns casos como resultado do modelo adotado pelo fornecedor. Os três fornecedores mais bem avaliados, em ordem decrescente, foram K, E e H. A falta de suporte a funcionalidades de acesso remoto sem uso de um agente prejudicou a pontuação do fornecedor H.

6 SUGESTÕES PARA TRABALHOS FUTUROS

Visto que soluções baseadas em uma arquitetura SASE são relativamente recentes e novas tecnologias surgem a todo momento, é importante acompanhar a evolução das soluções disponíveis no mercado e reavaliar as opções disponíveis quando necessário. Importante salientar que projetos de adoção de ferramentas do *framework* SASE são geralmente plurianuais, abrindo espaço para soluções emergentes no decorrer do processo de implantação. Da mesma forma, os critérios de avaliação são mutáveis de acordo com as necessidades de uma organização. Portanto, embora seja possível determinar no momento presente um fornecedor mais adequado, é necessário revisitar o estudo sempre que novas variáveis - de mercado ou de negócio - sejam identificadas. Este estudo se concentrou nas capacidades de ZTNA. Uma análise mais criteriosa - em especial, dos custos envolvidos - de outras capacidades do *framework* SASE pode ser necessária a depender dos requisitos da organização. É recomendável também a realização de uma Prova de Conceito (PoC) anteriormente a um projeto de implantação de SASE, visando avaliar o desempenho e experiência do usuário em um ambiente de testes.

REFERÊNCIAS

ARUBA. **O que é SD-WAN?** 2023. Disponível em: <https://www.arubanetworks.com/br/faq/o-que-e-sd-wan/>. Acesso em: 14 de novembro de 2023. Citado na página 23.

BMC. **IT Operations Management (ITOM)**. 2023. Disponível em: <https://www.bmcsoftware.pt/it-solutions/it-operations-management.html>. Acesso em: 13 de novembro de 2023. Citado na página 23.

CLOUDFLARE. **O que é um IdP (provedor de identidade)?** 2023. Disponível em: <https://www.cloudflare.com/pt-br/learning/access-management/what-is-an-identity-provider/>. Acesso em: 14 de novembro de 2023. Citado na página 23.

ENTRUST. **WHAT IS AN IDENTITY PROVIDER (IDP)?** 2023. Disponível em: <https://www.entrust.com/resources/faq/what-is-an-identity-provider>. Acesso em: 14 de novembro de 2023. Citado na página 22.

GRADY, J.; LALIBERTE, B. 2021 sase trends. Enterprise Research Group, 2021. Citado na página 16.

HOLMES, D.; BLANKENSHIP, J.; PROVOST, C.; DOSTIE, P. The forrester new wave™: Zero trust network access, q3 2021. 2021. Disponível em: <https://www.forrester.com/report/the-forrester-new-wave-zero-trust-network-access-q3-2021/RES176124>. Citado na página 26.

IBM. **O que é SIEM?** 2023. Disponível em: <https://www.ibm.com/br-pt/topics/siem>. Acesso em: 13 de novembro de 2023. Citado na página 23.

LAWSON, C.; RILEY, S. Magic quadrant for cloud access security brokers. 2020. Disponível em: <https://www.gartner.com/en/documents/3992205>. Citado na página 21.

MACDONALD, N.; ORANS, L.; SKORUPA, J. The future of network security is in the cloud. Gartner, 2019. Citado na página 19.

MACDONALD, N.; SMITH, N.; ORANS, L.; SKORUPA, J. 2021 strategic roadmap for sase convergence. Gartner, 2021. Citado 3 vezes nas páginas 16, 19 e 21.

MEF. **SASE Service Attributes and Service Framework**. 2022. Disponível em: <https://www.mef.net/resources/mef-117-sase-service-attributes-and-service-framework/>. Acesso em: 05 de fevereiro de 2024. Citado 2 vezes nas páginas 21 e 22.

ORANS, L.; RILEY, S. Market guide for zero trust network access. Gartner, 2020. Citado 4 vezes nas páginas 19, 20, 24 e 31.

POINT, C. **What is a Device Posture Check (DPC)?** 2023. Disponível em: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-security/what-is-a-device-posture-check-dpc/>. Acesso em: 14 de novembro de 2023. Citado na página 25.

SERVICENOW. **O que é ITSM?** 2023. Disponível em: <https://www.servicenow.com/br/products/itsm/what-is-itsm.html>. Acesso em: 14 de novembro de 2023. Citado na página 23.

SHIMIZU, T. **Decisão nas Organizações**. [S.l.]: Editora Atlas, 2010. Citado na página 26.

TELECO. **Disponibilidade de Sistemas**. 2023. Disponível em: <https://www.teleco.com.br/disponibilidade.asp>. Acesso em: 13 de novembro de 2023. Citado na página 23.

THALES. **Perpetual vs. Subscription Licenses: Long-Term Effects on Revenue**. 2023. Disponível em: <https://cpl.thalesgroup.com/software-monetization/perpetual-vs-subscription-licenses>. Acesso em: 14 de novembro de 2023. Citado na página 25.

TIBCO. **O que é a análise de correspondência?** 2024. Disponível em: <https://www.tibco.com/pt-br/reference-center/what-is-correspondence-analysis>. Acesso em: 04 de fevereiro de 2024. Citado na página 27.

WATTS, J.; LAWSON, C.; WINCKLESS, C.; MCQUAID, A. Magic quadrant for security service edge. 2022. Disponível em: <https://www.gartner.com/en/documents/4011551>. Citado na página 26.

Apêndices

APÊNDICE A – Questionário RFI Enviado aos Fornecedores

Features	Question
Solution Architecture and Components	
Architecture	What are the components involved in the SASE solution? Describe their names and functionalities.
	What is the conceptual model to enable access to applications? Service-Initiated ZTNA or Endpoint-Initiated ZTNA? Describe how it works.
	Please list and attach the application architecture diagram, presenting layers involved, connectors, gateways, etc.
	Please describe and attach the corresponding diagram for the recommended infrastructure scenarios, considering enabling remote access to on-premises, cloud and OT applications.
	Please detail the main ports, protocols used for supported sources and destinations. Describe the direction of each connection among components.
	Which protocols are supported for Remote Access? Are there any restrictions?
Application Connector and Gateways	Are there components hosted in the cloud? If so, please list the different cloud marketplaces (Azure, AWS, GCP, SAP, Oracle, etc.) in which components are available.
	Are there on-premises components? If so, please list the different operating systems in which the solution components are available. Describe minimum and recommended OS settings.
	What are the components footprint (CPU, memory and disk usage)? Describe minimum and recommended hardware settings.
Client	Please list the different operating systems (including OS for mobile devices) compatible with solution client software.
	Is there a clientless option? Which protocols does it support for Remote Access? Which browsers are supported ? Does it require any plugin?
	Is the solution composed by a single client or does it require additional clients/modules depending on the tasks performed?
	Is the client installation package available on the Internet?
	Does the client support multiple users on the same machine? Is it possible to seamless transition from one user to another?
	Does the client support multiple user profiles?
	Does the client support manual authentication (user credentials are entered manually)?
	Does the client support certificate-based authentication? User cert, machine or both?
	Does the client support Sigle-Sign-On (SSO) Authentication?
	Is it possible to install and upgrade the client manually (and not strictly through a management platform)?
	What is the client footprint (CPU, memory and disk usage)?
Identity Management	Does the solution support external IDP Integration for authentication and authorization? Which vendors are supported?
	Is there support for concurrent IDP configuration?
	Does the solution offers a local/proprietary IDP?
	Is the solution compatible with modern authentication?
	Is there support for MFA configuration?
	Is there an on-demand access provisioning capability? Describe how it works.
	Is there support for authentication time-out/forced re-authentication configuration?
Management	Is there a single panel management? Is it offered as a virtual machine, SaaS or both? Is it wel-based or not? Does it integrate with external IDP for user authentication and authorization?
	Which consoles does the solution provide? Are all of them web-based or are there consoles that cannot be accessed using browsers? Is there integration with external IDP for user auth/auth?
	Is there an application discovery tool/capability to identify applications running in the datacenter/cloud?
	Is there a proprietary platform to manage deployments and upgrades? Describe how this process works.
	Is there integration with MDM platforms like SCCM, Intune or JAML for client installation, configuration and upgrade? Which ones? Describe how it works.
	Please elaborate the minimum and recommended hardware & network configuration for workstations to access the consoles (management, administration, etc.).
Security Features	
	Does the solution include compliance check capabilities prior to enabling access to requested applications? Describe how it works, its features and limitations.
Compliance and Posture	Does the solution include posture capabilities prior to enabling access to requested applications? Describe how it works, its features and limitations.
	What is the effort to enable/disable compliance/posture checks? Does it require additional software/hardware/license?
Secure Web Gateway (SWG)	Does the solution include SWG capabilities? Describe how it works, its components and limitations.
	What is the assertiveness of SWG filtering/rating? How does it compare with other solutions in the market. Provide references/evidences.
	What is the assertiveness of SWG filtering/rating? How does it compare with other solutions in the market. Provide references/evidences.
	What is the effort to enable/disable SWG? Does it require additional software/hardware/license?
Zero Trust Network Access (ZTNA)	Does the solution have ZTNA built-in capabilities? Describe how it works, its components and limitations.
	What are the possible settings for context-based access? Which parameters can be verified prior to enabling access to a resource?
	Does the solution include Proxy capabilities? Describe how it works, its components and limitations.
Proxy	What is the assertiveness of Proxy filtering/rating? How does it compare with other solutions in the market. Provide references/evidences.
	What is the effort to enable/disable Proxy? Does it require additional software/hardware/license?
CASB	Does the solution include CASB? Describe how it works, its components and features.
	Is CASB mandatory to deploy the solution or can it be added as necessary to the architecture?
Remote Browser Isolation (RBI)	Does the solution include RBI capabilities? Describe how it works, its components and limitations.
	What is the effort to enable/disable RBI? Does it require additional software/hardware/License?
DNS Security	Does the solution include DNS filtering? Describe how it works, its components and features.
	What is the assertiveness of DNS filtering/rating? How does it compare with other solutions in the market. Provide references/evidences.
	What is the effort to enable/disable DNS Security? Does it require additional software/hardware/license?
Firewall as-a-Service (FWaaS)	Does the solution include FWaaS? Describe how it works, its components and features.
	What is the effort to enable/disable FWaaS functionality? Does it require additionsl software/hardware/License?
Data Loss Prevention (DLP)	Does the solution include DLP mechanisms? Describe how it works, its components and features.
	What is the effort to enable/disable DLP functionality? Does it require additional software/hardware/License?
SSL/TLS Inspection	Does the solution allow SSL/TLS inspection? Describe how it works, its components and limitations.
	What is the effort to enable/disable SSL/TLS inspection? Does it require additional software/hardware/License?
DDoS Protection	Does the solution provides DDoS protection mechanisms? Describe how it works, its components and features.
	What is the effort to enable/disable DDoS inspection? Does it require additionsl software/hardware/License?
Network Infrastructure	
Load Balancing (LB)	Does the solution support load balancing intra datacenters? Describe how it works, its components and limitations.
	Does the solution support load balancing inter datacenters? Describe how it works, its components and limitations.
Rate Limit	Does the solution support data rate limit configuration? Describe how it works and where it applies (SWG, Proxy, Remote Access,...).
Datacenters	What is the number of datacenters worldwide?
	What is the number of datacenters in Brazil? In which regions are they located?
	What is the number of datacenters in Canada? In which regions are they located?
Availability	Considering only the solution provider's infrastructure, what is the solution/infrastructure availability?
IPv6 Support	Is the solution compatible with IPv6?
Integration	
Systems/tools Integration	Is there integration support for SIEM tools? Which ones? Describe how it works and necessary effort to enable it.
	Is there integration support for Syslog tools? Which ones? Describe how it works and necessary effort to enable it.
	Is there integration support for ITSM/ITOM tools? Which ones? Describe how it works and necessary effort to enable it.
	Is the solution compatible with network and security technologies like SD-WAN and firewalls from other vendors?
	Is the solution interoperable with other vendors? Describe if there are any limitations?

Features	Question
Roadmap and Implementation	
Vendor Stability	Please provide a brief description of the company (number of employees, foundation date, stock holders, gross sales, ...)
Solution Stability	How many customers does the proposed solution currently serve? Please provide major reference customers.
	What is the name of the solution for Secure Access Service Edge (SASE)? Is it a standalone solution, requires a combination of multiple solutions or is part of a platform?
	Does the solution depends on components or modules (connectors, drivers, etc.) from other vendors to provide all the functionalities required?
	Have the solution being tested and rated by recognized consulting/auditing companies? Please provide details and evidence of the results.
	Is the proposed solution considering the newest released version for all modules? If not, please detail the reason why it's not being proposed.
Product Roadmap	Does the solution have a product roadmap? If so, please detail this roadmap for the next three years, listing all major enhancements and capabilities that will be gained in each release.
	For how many years the solution will be supported (patches, enhancements, etc.)?
	Has the solution been implemented internationally? If so, please describe the case.
	Has the solution been implemented in Brazil? If so, please describe the case.
Implementation	Has the solution been implemented for other mining or oil & gas companies? If so, please describe the case.
	Typically, how long does it takes to completely implement the solution (in months)?
	Please detail vendor geographic reach including which regions or countries it has qualified resources to support the solution implementation.
	Does the vendor provide dedicated assisted operation after implementation? Please describe its typical period and solution stability metrics.
Architecture & Compatibility	
Virtual Server Compatibility	Vale environment expects all application environments to be hosted on a standard virtualized environment. Are there any conditions that would prevent virtualization?
Virtual Server Compatibility	Is the solution compatible with market standard virtualization software? Please detail any existing restrictions for each server type.
Server SW Requirements	Do the solution servers, connectors / gateways require specific software (.NET framework, office plugin, Java, etc.)? If so, please detail the required software by component type.
Required Batch Processing	Does the solution have any required batch processing? If so, please detail the related batches and their corresponding purpose, frequency and estimated duration.
Network and Bandwidth	What is the payload added to user-application traffic for encryption/tunneling data?
	Disregarding data replication / transfer scenarios, does the solution itself have any restrictions regarding network latency and jitter? If, so please describe these limitations.
Process Concurrency	Are certain functions restricted when other processes (e.g.: database administrative procedures, batches processing...) are occurring within the application? If so, please detail these functions.
Transaction Processing	From the largest implementation case, what is the maximum number of simultaneous data replication / data transfer flows processing per minute? What influences this number (CPU, Memory, etc.)?
Transaction Processing	From the largest implementation case, what is the maximum amount of data processed per minute?
Internal Database	Does the solution requires an internal database? Which ones are supported and for which modules? Please list the compatible DBMS for the solution (not related to data capture / replication flows) and the requirements.
	From the largest implementation case, what is the maximum database size for the solution (in GB)?
Internal Database	From the largest implementation case, what is the period of time stored in the database (in years)?
Internal Database	From the largest implementation case, what is the maximum volume of records stored in the most critical table? Please list the top 10 most critical solution's tables and their corresponding records volume
	Does the amount of data involved in replication scenarios / data transfer influence solution's internal database size? Does the data is stored in the server before delivered to the destinations?
Internal Database	Does the solution provide any mechanisms for data archiving? Please describe such mechanisms, storage layers, security access control and read/write permissions.
	Can the solution make use of database clusterization capabilities? Please detail any possible restrictions.
Scale Up x Scale Out	Does the solution support scaling up? If so, please list the products in the solution that can be scaled up.
	Does the solution support scaling out? If so, please list the products in the solution that can be scaled out.
Scale Up x Scale Out	Does the solution have a cluster management solution through a command line and graphical web-based interface?
	Does the solution provide any auto-scale feature?
	Can the application work in a distributed fashion having multiple application/web servers connected to one or more database servers all presenting the same set of data? Please detail the supported solutions.
Application Farm & Load Balancing	Does the solution provide options for load balancing? If so, please detail these options.
	Does the solution provide any mechanisms for a multiple-instances topology? If so, please describe these mechanisms.
Recover Capabilities	Does the solution has recover capabilities (e.g.: rollback not committed transactions, automatic services start...) ? Please detail these capabilities.
Type of Storage	Vale has multiple tier storage. Does this solution require high performance storage? Please detail which kind of storage is required.
Uptime	Is the solution designed to be available 24x7? Please indicate the standard uptime SLAs that can be achieved, in terms of hours per year of unplanned downtime.
Internationalization & Localization	Does the solution support Unicode at all layers of its architecture?
Internationalization & Localization	Please describe how the solution attends internationalization and localization needs (Currencies, languages, calendar, number and date formats, etc.).
Exception Handling	Please detail how the solution handles with errors and exceptions throughout the architectural layers. Describe how errors and warnings are logged and exception reports are provided.
Ongoing Support Procedures	Does the solution require ongoing support procedures (e.g.: reindex, data archiving...) to keep application operational and performative? If so, please detail.
Job Processing	Does the solution provide a job scheduler mechanism? Please describe the way the solution jobs can be scheduled.
Job Processing	Does the solution provide a job monitor mechanism? Please describe the way the solution jobs can be monitored.
	Does the solution provide an automated mechanism for job execution status report? If so, please describe this mechanism.
	Does the solution provide a notification events for job processing? if so, please describe this mechanism.
Job Processing	Does the solution provide a error handling for job processing? If so, please describe this mechanism.
Accessibility	Does the solution provide accessibility options? Please elaborate.
Security, Conformity and Data Privacy	
User Profiles	Where can application user profiles be maintained/stored (e.g.: application database, active directory...)? Please detail the way that user profiles and user groups can be defined.
User Profiles	Does the solution impose limitations on or apply validation to the size or format of supplied usernames? If so, please detail these restrictions.
User Profiles	Does the solution apply password rules (e.g., minimum length, aging, etc.)? Please detail these rules.
	Does the application has its own password repository, are the passwords encrypted? Please describe the architecture.
	Does the solution provide any mechanisms for user profiles functional conflict check (e.g.: if an user issue a PO he shouldn't be allowed to approve it)? Please describe such mechanisms and corresponding reporting options.
Authentication	Does the solution support authentication against Vale standards services (Novell eDirectory, Active Directory, Webservices, REST, etc.)? Please list the supported directory services.
Authentication	Is possible to encrypt the login information? If so, describe this mechanism.
Authorization	Are security rules hard-coded or flexibly maintained in the database? Please detail the process to maintain these rules.
Authorization	Which granularity levels are provided for user access control (e.g.: module, screen, functionality, information...)? Please describe the process to configure these different levels.
Authorization	Is the solution able to associate functional profiles to user groups defined in directory services?
Sensitive and Critical Data	Does the solution have encryption mechanisms to store sensitive and critical data? If so, please detail these mechanisms and available key repositories.
Sensitive and Critical Data	Does the solution have any other security mechanism to store sensitive and critical data? If so, please detail these mechanisms.
Sensitive and Critical Data	Does the solution provide data security mechanisms between client, server, connectors, gateways, etc.? Please describe the architecture and supported security standards.
Sensitive and Critical Data	Does the solution provide data security mechanisms for communication with other applications? If so, please describe these mechanisms. Please describe the architecture and supported security standards.
Secure Communication	Apart from developed data flows, does the solution expose information to internet? If so, which information?
Secure Communication	Is the communication among server / databases / connectors / gateways encrypted? Please describe the architecture and supported security standards.
Audit Logging	Does the solution have mechanisms for audit trail and log storage? If so, please detail these mechanisms and the way that system activities are logged.
	Is there a tool to visualize the logs in a web? if so, please detail the features available.
Audit Logging	Please describe the available audit log repositories for rastreability purposes.
User Session	Does the solution work with the creation of user session? If so, please detail the storage repository options available.
User Session	Does the solution has a session timeout flexibly parameterized?
User Session	Is the concept of user exits supported (e.g.: close sessions, rollback transaction not committed...)?
Evolution & Extensibility	
Deployment Packages	Is the solution installation process encapsulated in deployment packages? Please describe the technical process of performing a full install and a version upgrade.
Release Schedule	Please describe how patches and new solution releases are distributed. Does the solution has a formal release schedule?
Backward Compatibility	When releasing new versions, is backward compatibility maintained?
Customization	Does the vendor provide services for solution enhancement and customization? Please list available partners and detail possible customization restrictions.
	Are customizations and enhancements handled during upgrades? Please describe this process.
Support	
Services	Are all the components and modules included maintained and supported by the same vendor?
	Any additional skills necessary to administrate the product (e.g., Azure SDK, Amazon SDK, Database Administration, Server Management, etc.)?
	Does the vendor have a certified architecture team to work in a pilot solution and support activities such as Planning, Architecture Design, Capacity Planning,...)?
	Does the vendor have specialists to support Vale and perform quality-assurance reviews in the solutions?
	Please describe the available models for providing support and maintenance.
	Does the support contract covers upgrades? If not, describe how they can be contracted.
	Does the license acquisition includes a support period of time? If so, please detail conditions and the covered period.
Support & Maintenance Contract Model	Please list the standard service levels agreement by contract type. Please describe the available staffed hours by contract type.
	In which time zones there is a support structure available?
	What is the typical response time for regular situations (in hours)?
	Will the vendor provide second level support as well as 3rd Level support (in case the vendor owns the product).
Supported Languages	Please describe the supported languages by support type and what are the locations where the Support is based? (Off-shore, like India, centers/offices in Brazil)? Use its own facilities and staff?
Knowledge Base	Does the solution have a knowledge base available?
	Does the support contract cover access to the knowledge base?
	Please describe the channels where application support is available (Mail, Chat , Phone , online, ...), existing conditions and restrictions.
Support	Does the vendor is able to use Vale's official ITIL tool (ServiceNow) or does Vale need to use a different tool to interact with the vendor?
	Does the vendor also provide Enhancement Support (development)?
Technical Manual	Are technical manuals provided? If so, please attach an illustrative document.
User Manual	Are user manuals provided? If so, please attach an illustrative document.
User Manual	Is an online help available in the solution?
Data Model	Is data model provided with appropriate data dictionary and documentation to allow retrieval solution's internal data? If so, please attach an illustrative document.
Required Training	Does the solution require specific training? If so, please supply suggested training curriculum, courses and costs by role, available session for the next year, training formats (e.g.: online, face-to-face...), available languages and locations.
	Are training days included in a standard contract? If so, please detail how many training days by role are included in a standard contract.
Required Training	Does the provider have a certification program for professionals in the market?
Training Material	Does the vendor provide training material? If so, please attach an illustrative document. Is it possible to schedule an on-site training? Please detail training conditions.
ESG	
Carbon Footprint	What is the carbon footprint of the supplier?

Features	Question
Commercial Features	
Licensing	What type of licensing is practiced (for example: per user, per device, per developer, by CPU, Size where the product is installed, volume of data processed, number of data flows, number of users, connectors, etc.)? How is the software contracting model and maintenance (procurement, subscription, IaaS). Provide a list of license prices.
	Does the license model include all features in the solution portfolio or is it necessary to acquire new licenses according to the required capabilities? Please detail.
Support & Maintenance Contract Model	Please describe the available models for providing support and maintenance.
	Does the support contract covers upgrades, updates? Describe the types of upgrades covered by maintenance and support. If not, describe how they can be contracted.
Support Lifetime	Does the license acquisition includes a support period of time? If so, please detail conditions and the covered period.
Contract Model	Describe how your company will change the licenses and how will provide the services in case of signature a contract. 1) Describe if it will be necessary to do agreement with another partner in case in one of this services (license, implementation and support). Are there any representatives in Brasil?
	Can the vendor provide a consulting contract for solution implementation? If so, please detail this contract model.
Price adjustment	How is the unit price adjustment for contracts with a term longer than one year work? Inform the index used to readjust the prices.
Dollar Trigger	Explain how will be the invoices for payments in Reais that has the prices based in dollars. Is there any kind of dollar trigger?
Budget Estimate	Please provide budget estimate to enable Secure Remote Access to cloud and on-premises applications in 3 scenarios: 3000 users, 30000 users and 60000 users, for 1 and 3 years. Consider only license costs.
Payment Models	Describe payment methods for services, licenses, and support. If they will be for the year, monthly, milestones, hours, etc.
Robustness	
Vendor Maturity	Have the company received any awards that would highlight its capabilities in this area? Please list these awards.
	Have the company been assessed against its capability maturity model? If so, please detail when the assessment was done and the results by key process area.
Vendor Roadmap	Does the company have a growth strategy plan? If so, please detail this plan for the next three years.
Affiliations & Partcerships with Other Vendors	Does the vendor have any affiliations & partnership with other vendors? If so, please list these affiliations & partcership.
Package Certifications	Have the solution received any package certifications? If so, please list these certifications.