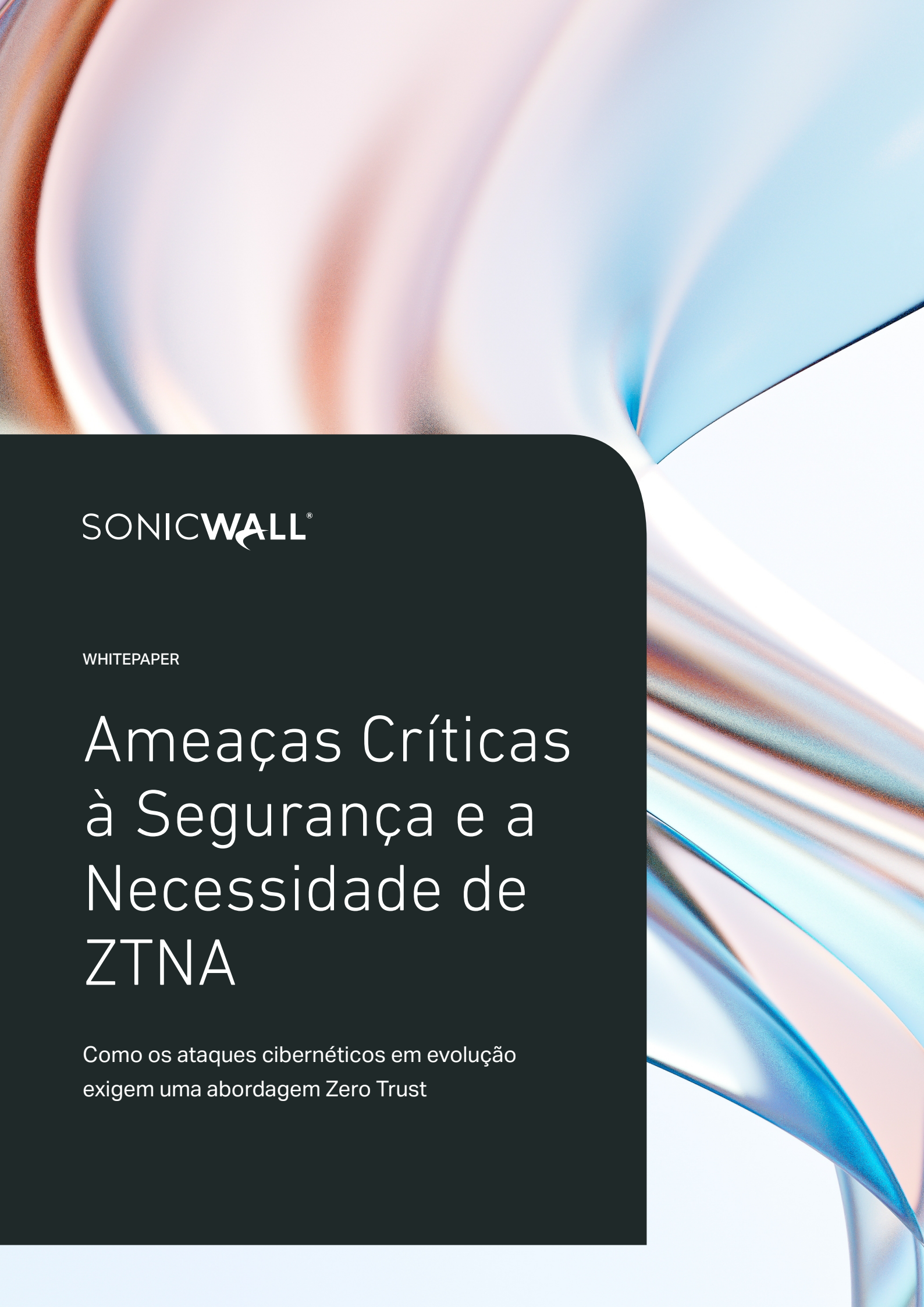

SONICWALL®

WHITEPAPER

Ameaças Críticas à Segurança e a Necessidade de ZTNA

Como os ataques cibernéticos em evolução exigem uma abordagem Zero Trust

Índice

SONICWALL®

1

Resumo Executivo

As ameaças cibernéticas tornaram-se mais **frequentes** e **sofisticadas**, tendo como alvo organizações de todos os tamanhos e de todos os setores. Desde o **comprometimento** de e-mails comerciais até **ransomware** e **escalonamento de privilégios**, os adversários estão capitalizando os **pontos fracos das defesas tradicionais baseadas em perímetro**. Dados recentes da SonicWall revelam:

- **O Business Email Compromise** está relacionado a **1 em cada 3 reivindicações de seguro**.
- **O ransomware** continua a crescer, com um **aumento de 259%** em determinadas regiões (por exemplo, América Latina) e **198 milhões de registros de pacientes** afetados somente em 2024.
- **A SSRF (Server-side Request Forgery, falsificação de solicitação no lado do servidor)** registrou um **aumento de 452%** nos incidentes, impulsionado em parte pela **verificação de vulnerabilidades com IA**.

Esses números enfatizam que **os atacantes não só podem como vão obter acesso inicial e se mover lateralmente**. Uma vez dentro, eles contam com táticas como **escalonamento de privilégios** ou **"living off the land binaries"** (LOLBins) para aprofundar o controle sem acionar alertas. Enquanto isso, os funcionários trabalham cada vez mais remotamente usando **dispositivos móveis não gerenciados**, ampliando a superfície de ataque.

O Zero Trust Network Access (ZTNA) é uma estratégia essencial: ele **não** presume nenhuma confiança implícita – esteja o usuário na LAN corporativa ou remota – e verifica continuamente a identidade, a postura do dispositivo e os sinais de risco. A solução **Cloud Secure Edge** da SonicWall se alinha a esse modelo, oferecendo **segmentação**, **confiança no dispositivo**, **inteligência contra ameaças** e **visibilidade em tempo real** para mitigar essas ameaças crescentes.

259%

Aumento de ransomware em determinadas regiões

198

milhões de registros de pacientes afetados

SONICWALL

2

Cenário de ameaças em evolução

Historicamente, as organizações dependiam de fortes defesas de perímetro – firewalls projetados para manter as ameaças "do lado de fora". No atual ambiente de trabalho híbrido e habilitado para a nuvem, os usuários geralmente estão fora da proteção da rede corporativa, o que os torna mais vulneráveis a ataques de phishing, credenciais roubadas e explorações de aplicativos. Uma vez dentro da rede, os atacantes podem se mover lateralmente com facilidade se a rede não tiver uma segmentação adequada e uma forte verificação de identidade.

Principais fatores de aumento das ameaças

Trabalho híbrido
Os funcionários e prestadores de serviços acessam os sistemas em qualquer lugar, muitas vezes usando seus próprios dispositivos pessoais.

Proliferação de serviços em nuvem
Aplicativos de missão crítica (por exemplo, Microsoft 365, Google Workspace) devem ser acessíveis pela Internet, ampliando a possível superfície de ataque.

Automação e IA
Os adversários usam grandes modelos de linguagem (LLMs) para desenvolver e-mails de phishing sofisticados, gerar scripts de exploração em escala e automatizar a descoberta de vulnerabilidades.

SONICWALL

3

Principais vetores de ameaças

3.1 Business Email Compromise (BEC)

O BEC é uma tática de engenharia social altamente eficaz em que os **criminosos se fazem passar por** um indivíduo confiável – geralmente um executivo – para enganar funcionários ou parceiros e fazê-los **transferir fundos** ou **revelar dados sensíveis**.

Impacto

- Um dos principais fatores de **perdas financeiras**; vinculado a **1 em cada 3 reivindicações de seguro cibernético** em 2024.
- Difícil de detectar porque os atacantes utilizam **contas de e-mail legítimas** (credenciais roubadas ou regras de encaminhamento).

Padrão de ataque comum

- Os atacantes obtêm **acesso inicial à conta de e-mail** (phishing ou reutilização de senha).
- Configuram **regras de encaminhamento furtivas**, às vezes excluindo mensagens encaminhadas da caixa de entrada da vítima.
- Aguardam **transações financeiras** (faturas, transferências eletrônicas) para desviar ou se passar por aprovações internas.

Mitigação de Zero Trust

- Impõe a **MFA adaptável** em todos os acessos a e-mails corporativos.
- Restringe o acesso ao e-mail a **dispositivos gerenciados** ou dispositivos com um **certificado válido** e postura aceitável.
- Monitora os locais de **login anômalos** (também conhecidos como sinalizadores de **"viagem impossível"**).

SONICWALL

3.2 Malware e Ransomware

259%

aumento de ataques de ransomware

O ransomware criptografa dados e exige pagamento pelas chaves de descriptografia, enquanto o malware pode roubar informações ou **estabelecer persistência** para violações mais profundas.

Tendências recentes

- **Houve um aumento de 259%** nos ataques de ransomware em algumas regiões.
- **198 milhões de** registros de pacientes da área da saúde foram afetados por ransomware somente em 2024.
- Os atacantes usam técnicas de **evasão de EDR**, muitas vezes aproveitando o **PowerShell** (LOLBins) para evitar a detecção.

198

milhões de registros de pacientes afetados

Táticas de propagação

- **Os links ou anexos de phishing** fornecem cargas úteis maliciosas.
- Exploração de **sistemas sem patches**.
- Movimento lateral em **redes planas**.

Mitigação de Zero Trust

- **A microssegmentação** e o controle de acesso garantem que um endpoint infectado não possa espalhar o ransomware lateralmente.
- **A filtragem automatizada de URLs** bloqueia sites mal-intencionados.
- **As verificações de postura do endpoint** verificam se os dispositivos executam EDR e patches atualizados antes de conceder acesso à rede.

3.3 Falsificação de solicitações do lado do servidor (SSRF)

Os ataques **SSRF** induzem os aplicativos da Web a fazer **solicitações não autorizadas** a serviços internos. Muitas estruturas (WordPress, Drupal, etc.) apresentam vulnerabilidades SSRF, permitindo aos atacantes:

- **Exfiltrar** dados internos.
- **Verificar portas de rede internas**.
- **Abusar dos serviços de "metadados"** em ambientes de nuvem (por exemplo, AWS, Azure).
- **452% de crescimento**:
  - As ferramentas modernas **orientadas por IA** podem fazer **uma varredura em massa** dos pontos de entrada de SSRF.
  - Uma vez descobertos, os atacantes se movimentam em uma rede supostamente "interna".

- **Mitigação de Zero Trust**:
  - Limite o acesso aos **serviços de aplicativos internos** apenas para usuários e dispositivos **autenticados** e autorizados.
  - **Aplicação contínua** de patches em estruturas da Web.
  - Controles da **camada de aplicativos** (por exemplo, WAF) integrados a uma arquitetura Zero Trust para **negar solicitações internas não autorizadas**.

3.4 Superfície de ataque móvel

Como os funcionários dependem cada vez mais de **smartphones** e **tablets** para realizar tarefas corporativas, os atacantes veem uma oportunidade:

- **Códigos QR maliciosos**, aplicativos de produtividade falsos ou **SMS de phishing**.
- **Fadiga de MFA** – bombardear os usuários com solicitações replicáveis de MFA até que eles aprovem por hábito.
- **Sistemas operacionais não corrigidos** ou dispositivos com **jailbreak** que não possuem controles de segurança.
- **Mitigação de Zero Trust**:
  - Restringir o acesso de aplicativos a dispositivos **que atendam aos requisitos de postura** (por exemplo, sem jailbreak, com patches de segurança atualizados).
  - Análise de **geolocalização** e de "viagens impossíveis" para detectar logins incomuns.
  - Políticas condicionais que podem **limitar determinadas operações de alto risco** (por exemplo, acesso ao repositório de códigos) em dispositivos móveis.

3.5 Escalonamento de privilégios e Living off the Land (LOLBins)

Os atacantes presumem que **o comprometimento inicial** é inevitável, geralmente por meio de credenciais roubadas ou ameaças internas. Uma vez lá dentro:

Escalonamento de privilégios

- Explorar vulnerabilidades do sistema operacional para obter **privilégios de administrador**.
- Em 2024, 38% das vulnerabilidades exploradas da Microsoft eram para **elevação de privilégios**.

Living off the Land Binaries (LOLBins)

- Ferramentas como o **PowerShell** ou o **schtasks.exe** vêm pré-instaladas no Windows, o que dificulta sua **detecção**.
- Os atacantes podem fazer download de malware adicional, criar backdoors ou exfiltrar dados sem usar executáveis maliciosos "tradicionais".

Mitigação de Zero Trust

- Aplicar o **privilégio mínimo**: os usuários normais não obtêm direitos de administrador, a menos que sejam expressamente concedidos.
- **Monitorar** o uso da linha de base das ferramentas incorporadas para detectar anomalias (por exemplo, comandos suspeitos do PowerShell).
- A microssegmentação garante que, mesmo com privilégios elevados em um sistema, **os atacantes não consigam acessar** os ativos críticos sem reautenticação e verificações de postura.

4

Ameaças cibernéticas impulsionadas por IA

Os atacantes utilizam cada vez mais **grandes modelos de linguagem** e automação de IA para:

- Gerar campanhas de **phishing altamente sofisticadas** que imitam uma comunicação genuína.
- **Automatizar o SSRF** e a varredura em busca de explorações conhecidas.
- Produzir scripts para evitar a detecção de endpoints.

O Zero Trust é especialmente crítico aqui porque a IA torna mais rápido e mais barato para os atacantes lançarem ataques **personalizados** em escala. Os defensores humanos, por sua vez, se beneficiam das **ferramentas de segurança com IA/ML** – como as do mecanismo de detecção de ameaças da SonicWall – que identificam **padrões incomuns** no comportamento da rede ou do usuário.

5

Zero Trust: Princípios e Benefícios

O Zero Trust **não pressupõe nenhuma confiança implícita** – dentro ou fora da LAN corporativa. Em vez disso, **cada** solicitação de acesso a dados ou a um aplicativo passa pelo seguinte:

1. **Autenticação do usuário** (por exemplo, MFA forte vinculada a políticas baseadas em funções)
2. **Verificação de dispositivos** (verificações de postura, certificados, nível de patch do sistema operacional)
3. **Autorização contínua** (pontuação de risco baseada em sessão, detecção de anomalias)

Benefícios

- **Redução da superfície de ataque**: os atacantes não podem se mover livremente em seu interior.
- **MFA mais forte**: isso minimiza o sucesso do roubo de credenciais ou phishing.
- **Visibilidade abrangente**: a TI pode ver e controlar quem está acessando o quê, de onde e em qual dispositivo.

SONICWALL®

6

ZTNA em ação: Como a SonicWall pode ajudar você

A SonicWall desenvolveu um conjunto completo de soluções para segurança de endpoints, serviços de identidade e inteligência contra ameaças que oferece acesso **Zero Trust** para avaliação de riscos em tempo real.

6.1 SonicWall Cloud Secure Edge (CSE)

Plataforma unificada Zero Trust: integra identidade, verificações de postura de endpoint e acesso a aplicativos.

Acesso orientado por políticas: regras granulares de **permissão/negação** com base na sensibilidade do usuário, do dispositivo, do local e dos recursos.

Detecção dinâmica de ameaças: a pesquisa de ameaças da SonicWall atualiza continuamente as assinaturas de detecção para bloquear URLs maliciosos, arquivos suspeitos e técnicas de exploração conhecidas (por exemplo, padrões SSRF).

6.2 Firewalls de última geração e Proteção avançada contra ameaças

Segurança em camadas: os NGFWs da SonicWall realizam **inspeção profunda de pacotes**, **decodificação de SSL e análise avançada de ameaças**.

Telemetria capturada: a inteligência em nuvem de milhões de pontos de dados em todo o mundo ajuda a identificar novas variantes de malware e domínios maliciosos em tempo real.

7

Recomendações e Melhores práticas

Adote uma "mentalidade de violação"

- Parta do princípio de que os atacantes já têm acesso inicial.
- Crie uma microssegmentação para minimizar os danos.

Aplique MFA forte e Postura do dispositivo

- Elimine a dependência de senhas estáticas e verifique a integridade do dispositivo (patch, AV/EDR em execução).

Monitore e analise o comportamento do usuário

- Detecte anomalias como aprovações de **fadiga de MFA** ou uso suspeito do PowerShell.

Gerenciamento regular de patches

- Elimine rapidamente as vulnerabilidades conhecidas, especialmente nos serviços voltados para a Internet.

Estratégia abrangente de backup

- O ransomware prospera em backups desprotegidos.
- Cópias offline protegidas ou somente de leitura são essenciais.

Aproveite a inteligência sobre ameaças

- Use feeds de dados em tempo real (como os da SonicWall) para bloquear ameaças emergentes.

Eduque sua força de trabalho

- O treinamento frequente de conscientização sobre segurança evita o phishing, especialmente o BEC.

SONICWALL

8

Conclusão

As ameaças cibernéticas – **BEC**, **ransomware**, **SSRF**, **escalonamento de privilégios**, **explorações móveis** – estão aumentando em frequência e potência. Os atacantes exploram a confiança implícita onde quer que ela seja dada, aproveitando a **IA** para dimensionar e personalizar seus ataques.

O **Zero Trust Network Access**, com verificação contínua em cada etapa, é a estratégia comprovada para mitigar esses riscos e **abordar as lacunas de segurança das soluções de rede tradicionais**. Combinando um forte gerenciamento de identidade, postura de dispositivo, segmentação de rede e inteligência contra ameaças em tempo real, as organizações podem reduzir drasticamente a chance de uma violação catastrófica.

A SonicWall se dedica a ajudar as **organizações** a adotar uma postura holística de Zero Trust. Por meio de soluções como Cloud Secure Edge, Next-Gen Firewalls e SonicSentry, a SonicWall integra pesquisa robusta de ameaças, gerenciamento simplificado de políticas e análises avançadas para defender ativos críticos contra ameaças cibernéticas modernas.

9

Apêndice: Etapas práticas e Glossário

9.1 Etapas práticas de implementação do ZTNA

1. Identifique e classifique os ativos: catalogue seus aplicativos e dados, mapeando quem precisa de acesso.
2. Implante um piloto: comece com um grupo piloto (por exemplo, um departamento específico) para ajustar as políticas do Zero Trust.
3. Estabeleça requisitos de postura do dispositivo: defina versões mínimas do sistema operacional, padrões de proteção de endpoints, níveis de patches, etc.
4. Configure o MFA: use MFA baseada em aplicativo ou token (evite SMS básico, se possível); integre com soluções IdP.
5. Implemente a microssegmentação: separe os bancos de dados ou servidores essenciais para que um invasor em um segmento não possa passar para outro.
6. Monitore continuamente: use os recursos do SIEM ou do SOC para observar padrões anômalos e refinar as políticas.

9.2 Glossário

- **BEC (Business Email Compromise)**: representação de uma conta de e-mail confiável para iniciar uma fraude.
- **MFA (autenticação multifator)**: requer dois ou mais fatores (por exemplo, senha + token) para acesso.
- **SSRF (Server-Side Request Forgery)**: explora a confiança de um aplicativo em si mesmo para chamar serviços internos.
- **LOLBins (Living off the Land Binaries)**: utilitários legítimos do sistema operacional (PowerShell, etc.) usados maliciosamente para evitar a detecção.
- **Zero Trust Network Access (ZTNA)**: uma estrutura de segurança que exige verificação contínua de cada usuário ou dispositivo que tenta acessar recursos.

Para mais informações

Visite SonicWall.com para explorar nossas Soluções Zero Trust ou saiba mais sobre como iniciar sua jornada Zero Trust com nosso eBook, Zero Trust Simplificado: Um guia prático para a segurança moderna.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 | Consulte nosso site para obter informações adicionais.