A Arquitetura de Zero Trust: Fundamentos e Aplicações

O propósito desse artigo é fazer uma revisão do conceito de Zero Trust desde sua concepção, até os dias de hoje. Revisando diversas fontes de informações e esclarecendo os principais falsos conceitos.

Por fim, com uma lupa no pilar de Acesso Seguro, destacar como a solução Harmony SASE pode ajudar clientes a estabelecer acessos seguros entre usuários e aplicações, onde quer que eles estejam.

O Problema

Historicamente, muitas organizações tiveram um modelo de segurança focado no perímetro. Este modelo é semelhante ao de um castelo, onde uma parede perimetral mantém os potenciais atacantes afastados, enquanto tudo dentro do perímetro é considerado “confiável”. Neste modelo de segurança, as defesas de segurança cibernética são implantadas no perímetro da rede e inspecionam o tráfego de entrada e saída para bloquear ameaças potenciais antes que possam causar danos a uma organização.

No entanto, este modelo de segurança tem seus problemas. Como um castelo, se alguém dentro do perímetro for uma ameaça, as defesas não oferecem proteção contra ele. Além disso, quaisquer recursos fora do perímetro de rede protegido – incluindo a infraestrutura em nuvem de uma organização, trabalhadores remotos, etc. – não estão protegidos de forma alguma.

Desperimetralização e a origem do modelo Zero Trust.

O conceito de Zero Trust parte de uma discussão inicado em 2004, no Jericho Forum.

O modelo onde o perímetro é definido pela rede interna de uma organização começa a ser desafiado, destacando inúmeros desafios e vulnerabilidades do mesmo e propõe-se alternativas baseadas no conceito de desperimetralização.

(Imagem 1 – Jericho Forum Commandments)

Em 2010, o conceito aparece novamente, em artigo de um analista do Forrester, pela primeira vez relacionado ao termo Zero Trust.

"*No More Chewy Centers: Introducing The Zero Trust Model Of Information Security*".

Desde então, foi utilizado de forma prática pelo Google (2014) em suas operações internas, alimentando o mercado com diversos artigos sobre o tema.

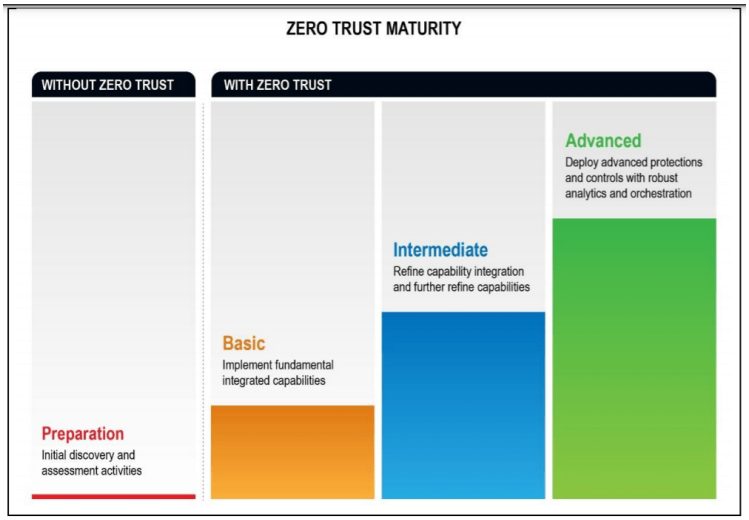
Também em 2014 foi incluído no framework CARTA (Continuous Adaptive Risk and Trust Assesment) do Gartner, aumentando cada vez mais sua popularidade no setor.

De 2020 em diante, Zero Trust se mantém no topo das tendências discutidas entre CISO de diversas organizações e continua a evoluir como framework e como conceito.

Zero Trust – produto, framework, conceito ?

Um erro comum que muitas organizações cometem é pensar no Zero Trust como destino. Se eles simplesmente comprarem a ferramenta certa, terão implementado a confiança zero em seus ambientes. Não é assim que funciona. É claro que as ferramentas podem ajudar a implementar aspectos de confiança zero e aproximar sua organização de uma arquitetura de Zero Trust, mas não são uma panaceia. Tal como acontece com a maioria das coisas em TI e segurança cibernética, consiste em pessoas, processos e tecnologia.

Conforme estabelecido na publicação da Agência de Segurança Nacional (NSA), "Embracing a Zero Trust Security Model", as principais recomendações incluem abordar a confiança zero a partir de uma perspectiva de maturidade. Isto inclui a preparação inicial e os estágios de maturidade básico, intermediário e avançado, conforme descrito pela NSA.



(Imagem 2 – NSA Zero Trust Maturity Model)

Assim sendo, o primeiro passo é a preparação. Identificar onde você está, onde existem lacunas, como sua arquitetura, práticas e processos se alinham com os princípios de confiança zero estabelecidos acima e, em seguida, criar um plano para resolvê-los – e o mais importante, aceitar que isso levará tempo.

Check Point & Zero Trust

Reconstruir a infraestrutura de segurança em torno de uma abordagem Zero Trust usando soluções pontuais pode levar a implantações complexas e lacunas de segurança inerentes. Para evitar isso, a Check Point oferece uma abordagem mais prática para implementar o Zero Trust, baseada na arquitetura consolidada de cibersegurança, Check Point Infinity. A Segurança Absoluta Zero Trust, entregue pelo Check Point Infinity, oferece uma implementação, eficiente e preventiva para auxiliar na jornada Zero Trust.

A arquitetura Check Point Infinity consolida uma ampla gama de funções e soluções de segurança que permitem implementar todos os oito princípios do modelo de Segurança Zero Trust.

Redes: Os Gateways de Segurança da Check Point permitem criar segmentação granular de rede em ambientes de nuvem pública/privada e LAN. Com visibilidade detalhada sobre usuários, grupos, aplicações, máquinas e tipos de conexão na sua rede, você pode definir e aplicar uma política de acesso "Privilégio Mínimo", permitindo que apenas os usuários e dispositivos corretos acessem seus ativos protegidos.

Workloads: O CloudGuard CWPP da Check Point protege cargas de trabalho, especialmente aquelas que estão em execução na nuvem pública. A integração nativa com qualquer infraestrutura de nuvem pública ou privada oferece total visibilidade e controle sobre esses ambientes em constante mudança, incluindo AWS, GCP, Microsoft Azure, Oracle Cloud, IBM Cloud, Alibaba Cloud, NSX, Cisco ACI, Cisco ISE, OpenStack, etc.

Pessoas: O Identity Awareness da Check Point e o CloudGuard garantem que o acesso aos seus dados seja concedido apenas a usuários autorizados, e somente após suas identidades terem sido rigorosamente autenticadas; usando Single Sign-On, Autenticação Multifatorial, políticas baseadas em contexto (por exemplo, hora e geo-localização da conexão) e detecção de anomalias.

Dados: O Check Point Infinity oferece proteção de dados em várias camadas que protege proativamente os dados contra roubo, corrupção e perda acidental, onde quer que estejam. Isso inclui criptografia de dados (Full Disk Encryption, Media Encryption e IPsec) e Prevenção de Perda de Dados (Data Loss Prevention).

Dispositivos: As soluções da Check Point permitem bloquear dispositivos infectados de acessar dados corporativos e ativos, incluindo dispositivos móveis e estações de trabalho

de funcionários, dispositivos IoT e sistemas de controle industrial. Além disso, o Harmony Endpoint protege os dispositivos dos funcionários o tempo todo e mantêm a política de segurança corporativa em redes não confiáveis.

Visibilidade e analítica: O Check Point Infinity proporciona visibilidade completa sobre sua postura de segurança inteira, permitindo detectar e mitigar rapidamente ameaças em tempo real. Visualize e analise bilhões de registros de log com Smart Log, investigue eventos com forense em tempo real e mantenha a conformidade com políticas corporativas e regulamentações de proteção de dados com o Check Point Compliance.

Automação e orquestração: O Check Point Infinity inclui um conjunto rico de APIs que suportam integração automatizada com o ambiente de TI mais amplo da organização, permitindo velocidade e agilidade, melhor resposta a incidentes, precisão de políticas e delegação de tarefas. Mais de 160 parceiros tecnológicos da Check Point utilizam essas APIs para desenvolver soluções integradas.

Acessos: O pilar de acesso, envolve elementos citados nos demais pilares, como Rede, Pessoas, Dispositivos, etc. Para garantir que a interação entre esses elementos ocorra de forma segura, independente da sua ampla gama de variações, vamos discutir nos tópicos abaixo um pouco sobre o Zero Trust Network Access (ZTNA) e a solução Harmony SASE.

Harmony SASE

À medida que as organizações adotam o SASE, suas soluções atuais comprometem a experiência do usuário com conexões lentas e gerenciamento complexo. Oferecendo uma alternativa revolucionária, o Harmony SASE proporciona segurança na internet 2x mais rápida combinada com Full Mesh Private Access e desempenho otimizado de SD-WAN, com ênfase em facilidade de uso e gerenciamento simplificado.

Oferecendo uma experiência de navegação local com segurança e privacidade reforçadas, o Harmony SASE apresenta suas proteções no dispositivo, garantindo uma arquitetura híbrida, e garante a segurança de qualquer aplicação empresarial com uma política centrada em identidade que abrange todos: funcionários, contratados e terceiros.

Sua solução SD-WAN unifica prevenção avançada de ameaças líder do setor com conectividade otimizada, garantindo videoconferências ininterruptas graças a failover de link e uma política de direcionamento integrada para mais de 10.000 aplicativos.

Benefícios:

- SASE de um único fornecedor com console unificado para todas as funcionalidades e o seu ambiente de firewall local e na nuvem;

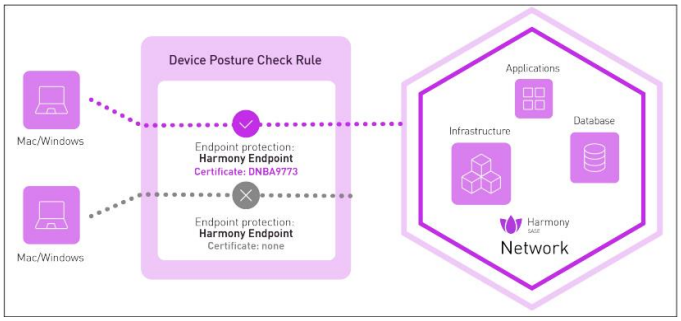
- Acesso seguro à Internet ultra-rápido para usuários remotos e escritórios filiais;
- Experiência de navegação localizada com segurança reforçada e maior privacidade;
- Acesso de Confiança Zero com conectividade Full Mesh entre usuários, filiais e aplicações;
- Conectividade SD-WAN otimizada com stack completo de segurança e prevenção avançada de ameaças líder do setor;
- Solução SASE mais fácil de implementar com implantação em apenas uma hora e administração intuitiva.

Full Mesh Private Access – Zero Trust Network Access (ZTNA)

Aqui voltamos a abordar o oitavo pilar (acesso seguro) de forma prática, focado em entender como a funcionalidade de Full Mesh Private Access contida na solução Harmony Access, pode ajudar a provisionar em minutos, controlar e monitorar os acessos dos usuários a aplicações, abrangendo múltiplos cenários de localidade tanto do usuário quanto da aplicação a ser acessada.

As capacidades de Full Mesh Private Access da solução Harmony SASE, garantem o acesso seguro e segmentado dos usuários as aplicações de forma moderna e segura.

- A solução permite estabeler conexões para aplicações on-prem ou em núvens públicas, possibilitando a criação de regras em todas as portas e protocolos (Camada 3 a Camada 7).
- Agentes disponíveis para dispositivos Windows, Mac, Linux, Chromebook, iOS e Android.
- Acesso sem dependência de agente, para dispositivos não gerenciados (BYOD), através de portal de aplicações.
- Centrado em identidade – Integração com todos os Identity Providers (SAML 2.0) e suporte a MFA.
- Verificação de postura da máquina – por versão de SO, verificação de anti-malware, criptografia, certificado, processos, domínio, entre outros atributos.



(Imagem 3 – Harmony SASE Device Posture Check)

Considerações Finais

O conceito de Zero Trust Security tem evoluído significativamente desde sua concepção, desafiando os modelos tradicionais de segurança baseados em perímetro. Ao migrar para abordagens como o Harmony SASE, as organizações podem não apenas garantir acessos remotos seguros, mas também integrar políticas de Confiança Zero de maneira eficiente e escalável. Com soluções como Full Mesh Private Access, o Harmony SASE oferece uma arquitetura híbrida robusta que protege usuários, dispositivos e aplicações em qualquer ambiente, promovendo uma experiência de usuário aprimorada e uma segurança reforçada em toda a rede corporativa.

Ao adotar o Harmony SASE, as organizações não apenas fortalecem sua postura de segurança cibernética, mas também capacitam seus colaboradores a trabalhar de forma mais flexível e eficiente, independentemente da localização. A solução não só proporciona uma segurança robusta através de políticas de Confiança Zero e Full Mesh Private Access, mas também promove uma experiência de usuário aprimorada, garantindo que os recursos críticos estejam sempre acessíveis de maneira segura e eficiente.

Além disso, a integração simplificada com Identity Providers (como SAML 2.0) e suporte a Autenticação Multifatorial (MFA) asseguram que apenas usuários autorizados tenham acesso aos dados e aplicações corporativas, mantendo a conformidade com regulamentações de segurança e proteção de dados. Isso é essencial em um cenário onde ameaças cibernéticas estão cada vez mais sofisticadas e as empresas precisam proteger seus ativos de forma proativa.

Por fim, a flexibilidade do Harmony SASE em suportar uma variedade de dispositivos (incluindo Windows, Mac, Linux, Chromebook, iOS e Android), juntamente com sua capacidade de fornecer acesso seguro mesmo para dispositivos não gerenciados (BYOD), posiciona a solução como uma escolha estratégica para empresas que buscam não apenas melhorar a segurança, mas também otimizar a produtividade e a eficiência operacional.

Fontes

Check Point - What is zero trust?

https://www.checkpoint.com/pt/cyber-hub/network-security/what-is-zero-trust/what-is-a-zero-trust-architecture/

Spiceworks - The 10 commandments of zero trust.
https://static.spiceworks.com/attachments/post/0016/4842/commandments_v1.2.pdf

CSO Online - 7 tenets of zero trust explained.
https://www.csoonline.com/article/571067/7-tenets-of-zero-trust-explained.html

Check Point - Check Point Infinity: Absolute zero trust security solution brief.
https://www.checkpoint.com/downloads/products/check-point-infinity-absolute-zero-trust-security-solution-brief.pdf

Autor: Victor Rossetti Santiago
Security Engineer