LISTA DE VERIFICAÇÃO

Coisas a se ter em mente ao tomar uma decisão de compra de cibersegurança

As organizações que procuram se manter competitivas estão atravessando um turbilhão de aceleração digital, procurando continuamente inovações que possam trazer para o mercado. No entanto, embora cada investimento em tecnologia possa levar uma organização adiante, a pressão que eles colocam nas redes pode ser uma bomba-relógio esperando que o ataque cibernético certo ocorra.

O motivo? O aumento da complexidade em um ambiente já muito complexo. A mistura aleatória de tecnologias de rede e segurança no ambiente corporativo médio resulta de uma mistura de inovação tecnológica, mudança de objetivos estratégicos, hesitação em se afastar dos fornecedores estabelecidos e uma crença comum na abordagem de "melhor da categoria" ou produto pontual.

No entanto, muitas das tecnologias de segurança e rede atualmente em vigor que são necessárias para fazer as coisas funcionarem não operam juntas. Assim, à medida que a rede se expande, são criadas novas lacunas de segurança e desempenho que os agentes mal-intencionados são capazes de explorar e estão muito dispostos a fazê-lo. Em vez de visibilidade e controle contínuos em toda a rede, muitos líderes de TI enfrentam um ambiente de segurança complexo, atormentado pela expansão de fornecedores e soluções, soluções de segurança isoladas e em silos e a falta de uma estratégia coerente de gerenciamento, orquestração e fiscalização.

Embora a abordagem tradicional de melhor produto possa ter funcionado no passado, a rápida expansão da rede, juntamente com um aumento notável no volume e na sofisticação do atual cenário de ameaças, exige algo mais. O que é necessário é uma estratégia de consolidação para reduzir a complexidade, convergindo rede e segurança, combinada com uma abordagem de plataforma de cibersegurança que reduza o número de fornecedores para alcançar uma resposta aprimorada a incidentes e permitir a orquestração e automação em todo o sistema.

Dez coisas a se considerar para compras de cibersegurança

É vital alcançar o nível de consolidação e convergência que as redes em expansão de hoje exigem. Os gerentes de TI devem fazer as seguintes perguntas essenciais ao considerar qualquer novo investimento em segurança:

- ☑ A solução pode convergir as principais funcionalidades de rede e segurança em uma única solução para reduzir a complexidade e melhorar a proteção?
- ☑ A solução é uma continuação de uma abordagem de produto pontual ou faz parte de uma abordagem de plataforma de cibersegurança para consolidar tecnologias para reduzir o número de fornecedores que precisam ser gerenciados?
- ☑ A solução pode funcionar com soluções de vários fornecedores por meio de APIs abertas e outros recursos?
- ☑ A solução pode ser provisionada e implantada com intervenção mínima no local, às vezes chamada de provisionamento e implantação sem toque?
- ☑ A solução é suficientemente granular para permitir que as organizações se expandam holisticamente a partir de seu investimento inicial?

- ☑ A solução pode abranger todos os vetores e bordas de ataque potenciais, incluindo aqueles ainda não implantados?
- ☑ A solução é suportada por uma única fonte de inteligência de ameaças derivada de sua pesquisa interna de ameaças e colaboração com os principais membros da comunidade de cibersegurança?
- ☑ A solução suporta uma filosofia de gerenciamento de painel de controle único?
- ☑ A solução oferece flexibilidade de implantação e escolha entre appliance de hardware, máquina virtual (VM), nuvem e contêiner?
- ☑ A solução se estende aos ambientes de tecnologia operacional (TO), possibilitando a convergência TI/TO?

Não se trata de produtos. Trata-se de entregar resultados e negócios

Os dias de simplesmente conectar uma solução de segurança de ponto isolado em algum segmento de rede para monitorar o tráfego acabaram há muito tempo. A segurança de hoje é uma jornada de integração, otimização e domínio. As soluções de segurança precisam ser capazes de se adaptar dinamicamente a uma superfície de ataque em constante evolução. Isso começa com a escolha de fornecedores capazes de trilhar esse caminho.

Eles devem ser capazes de fazer duas coisas:

1. Eles devem ser capazes de convergir rede e segurança para que as proteções possam se adaptar dinamicamente às mudanças resultantes da inovação digital.
2. E eles devem oferecer uma plataforma de cibersegurança consolidada que forneça um conjunto completo de proteções avançadas, suporte um ecossistema aberto usando APIs e padrões comuns e possa ser implantada universalmente para proteger consistentemente a superfície de ataque em expansão de hoje.

Isso deve incluir ferramentas que coletam, correlacionam e compartilham informações sobre ameaças e que possam participar de uma resposta unificada a ameaças, independentemente de onde tenham sido implantadas ou do modelo de entrega delas.

Essa abordagem integrada permite que as equipes de segurança avaliem continuamente o estado atual até mesmo da infraestrutura mais dinâmica, abrangendo cada canto e cada ecossistema. Essa plataforma de cibersegurança também deve fornecer um caminho para aprimorar e fortalecer constantemente a postura de segurança ao longo do tempo, com soluções projetadas para funcionar em conjunto. Essa abordagem permite que as organizações aproveitem ao máximo seus investimentos em segurança, pois cada elemento pode funcionar como parte de uma estratégia abrangente e em evolução.

outubro 26, 2023 12:18 PM

2182765-0-0-PT