illumio

Líder em Segmentação Zero Trust

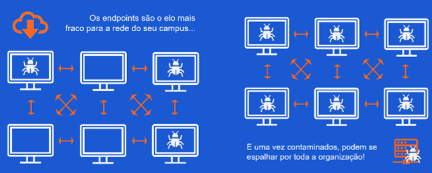
Proteja sua empresa, pare o ciberataque enquanto acontece e construa a organização digital da sua empresa com confiança.

A microssegmentação desempenha um papel fundamental para alcançar a segurança Zero Trust.
A microssegmentação surgiu como uma das melhores técnicas para proteger as organizações contra violações, restringindo o movimento lateral do invasor e reduzindo a superfície de ataque.

PROTEJA-SE DO RANSOMWARE

Proteja seus aplicativos e dados mais importantes com o líder em segmentação Zero Trust.

COMO ACONTECE O ATAQUE?



A MICROSEGMENTAÇÃO PODE AJUDAR!

É um dos sistemas mais eficientes para se chegar ao Zero Trust — uma proteção granular, de confiança zero.

Illumio Edge

Segurança de Endpoints

Visibilidade e segmentações para impedir o movimento lateral entre os endpoints.

Estamos mais conectados do que nunca. E um ataque de ransomware ou malware em um único endpoint pode se mover lateralmente para centenas ou milhares de endpoints em pouco tempo. Todos sabemos como essa história termina.
Illumio Edge é a única maneira de conter ransomware e malware a um único endpoint – mesmo que ainda não tenha sido detectado.

Illumio Core

Segurança de Workloads

Microsegmentação para proteger contra o ataque enquanto ele acontece.

Impeça o movimento lateral em seu data center e ambientes de nuvem com o Illlumio Core™. Tenha visibilidade de como os aplicativos estão se comunicando, obtenha insights quanto à exposição a vulnerabilidades e, em seguida, assuma o controle.
Crie políticas de segmentação que funcionam em qualquer local: servidores físicos, máquinas virtuais e contêineres.

Por que Microssegmentar?

- Dissociar a segurança dos elementos de rede;
- Aumentar de 3 a 9 vezes a dificuldade de movimentação lateral;
- Reduzir seu score de vulnerabilidade;
- Criar sinergia entre os times de redes e de aplicações;
- A primeira máquina infectada tende a ser a última.

Por que agora?

- Retorno da força de trabalho no pós pandemia;
- Crescimento constante dos ataques de phishing, malwares e ransomwares;
- O gerenciamento de políticas só vai ficar mais difícil e complicado enquanto estiver atrelada à infraestrutura uma vez que os aplicativos estão se tornando mais complexos (micro serviços, contêineres, nuvem híbrida)

Por que com Illumio?

- Agnóstico à rede;
- Seguro para implementar;
- Comprovadamente escalável;
- Suporte a ambientes heterogêneos;
- Experiência operacional;
- Libera o seu time de redes para outras funções.

1 Constrói um mapa do seus servidores, aplicativos e conectividade.

2 Segmenta com base em políticas, garantindo que a comunicação entre elementos/ferramentas aconteçam apenas se for definida anteriormente.

CONTROLE DE ACESSO INVISÍVEL

O agente é leve e invisível para usuários finais e permite uma implementação de baixo contato, sem interrupção para usuários ou operações.

COMPANHEIRO FIEL AO EDR E SEGURANÇA DE ENDPOINT

Ao impedir que o malware se espalhe utilizando técnicas de peer-to-peer, você dá às suas outras ferramentas de segurança de endpoint mais tempo para detectar e responder a ameaças.

ENDPOINTS ZERO TRUST

Um modelo de política comprovado baseado em listas de permissão transforma seus laptops em endpoints Zero Trust. Permite tráfego de entrada apenas a partir de aplicativos peer-to-peer aprovados.

REGRAS SEGUEM O USUÁRIO

Segmentação de endpoint que não está ligada à rede como o NAC. Vamos aonde seus usuários vão e damos visibilidade de cada fluxo dentro e fora de suas máquinas.

CONTENÇÃO POR PADRÃO

A contenção por padrão reduz drasticamente a área da infecção. Ele deixa o Ransomware e malware sem ter pra onde ir.

O nosso negócio é proteger o seu!

Fale conosco!
contato@leadcomm.com

leadcomm
trusted digital security