Introducing Cisco Hypershield

Contents

Segurança nativa de IA para data centers e nuvem. Sempre vigilante, em todos os lugares.

Na era dos data centers em escala de IA, gerenciar a segurança vai além da capacidade humana sozinha. As cargas de trabalho são comumente distribuídas em vários data centers e nuvens, levando a políticas fragmentadas que obscurecem a cobertura de proteção e atrasam a solução de problemas e incidentes. Ao mesmo tempo, os adversários estão explorando qualquer fraqueza cada vez mais rápido, uma tendência que se acelerará à medida que a IA for mais amplamente adotada. É necessário um novo e radicalmente novo abordagem para proteger aplicativos modernos e ambientes de computação dinâmicos.

O Cisco Hypershield revoluciona a segurança tanto em ambientes locais quanto na nuvem, capacitando as organizações a proteger aplicativos modernos com mais eficácia. Este produto inovador apresenta uma nova arquitetura distribuída que integra pontos de aplicação de rede e de execução de trabalho em um sistema de gerenciamento unificado. Com o Hypershield, as empresas obtêm uma proteção robusta e escalável, estendendo perfeitamente seu perímetro de segurança de infraestruturas tradicionais para a nuvem.

Benefícios

- **Protege em todos os lugares**. Implemente uma abordagem de segurança hiperdistribuída que abrange todas as áreas da sua rede, aproveitando uma ampla gama de pontos de execução de trabalho e aplicação anteriormente inacessíveis.
- **Elimina a lacuna de exploração.** Nosso sistema bloqueia exploits de aplicativos em minutos, não em semanas ou meses. Ele emprega controles de compensação cirúrgicos que são avaliados e testados em tráfego de produção ao vivo para obter uma eficácia ótima.
- **Segmentação que realmente funciona**. Alcance uma segmentação eficaz que se adapta e aprende continuamente. Nosso sistema ganha confiança ao longo do tempo e aplica controles altamente específicos, incluindo filtragem regex, garantindo segurança personalizada.
- **Se gerencia sozinho, quando ganha sua confiança**. Obtenha gerenciamento unificado em toda a rede e cargas de trabalho. Implante atualizações de software e políticas com confiança usando nossa abordagem de duplo plano de dados, permitindo testes seguros no tráfego ao vivo sem arriscar suas operações.

Recursos do Cisco Hypershield

Tornando realidades antes inimagináveis em realidade

O Hypershield é uma arquitetura totalmente nova construída do zero para enfrentar as realidades atuais.

Proteção distribuída contra exploits

No cenário digital atual, as vulnerabilidades são exploradas mais rapidamente do que nunca, às vezes em questão de horas por ataques impulsionados por IA. A aplicação tradicional de patches tem dificuldade em acompanhar o ritmo, geralmente levando semanas ou meses para implementar, o que pode interromper as operações e levar as organizações a adiar atualizações críticas para evitar tempo de inatividade.

O Hypershield enfrenta esse desafio diretamente com seu **módulo de Proteção Distribuída contra Exploits**, reduzindo drasticamente o tempo necessário para proteger contra novas vulnerabilidades. Este módulo automatiza todo o processo – desde a detecção, priorização e avaliação de controles até os testes e implantação – garantindo que as aplicações continuem funcionando sem interrupções.

Recursos principais:

- **Resposta acelerada por meio de fluxos de trabalho automatizados**. Nosso mecanismo nativo de IA detecta rapidamente vulnerabilidades e ajuda a priorizá-las, direcionando esforços onde são mais necessários. Ele avalia diferentes abordagens para recomendar a solução mais eficaz adaptada ao seu ambiente, construindo confiança continuamente.
- **Precisão com controles de compensação cirúrgicos**. Controles personalizados são implantados diretamente em uma malha distribuída de pontos de execução de trabalho e aplicação, permitindo uma mitigação precisa e eficaz.
- **Faça atualizações com confiança**. Todos os controles de compensação são testados em tráfego de produção ao vivo, garantindo sua eficácia e posicionamento ideal sem comprometer a aplicação.

Segmentação autônoma

Os desafios de segurança de hoje exigem mais do que as ferramentas tradicionais podem oferecer. Com o tempo médio para segmentar um único aplicativo excedendo 40 dias – e as regras muitas vezes se tornando desatualizadas quase assim que são implementadas – as organizações enfrentam lacunas significativas de segurança. Essas lacunas permitem que adversários se movam lateralmente pelas redes, aumentando exponencialmente o risco.

O **módulo de Segmentação Autônoma do** Hypershield revoluciona esse processo com um modelo de segmentação dinâmico e inteligente, informado por uma compreensão profunda dos comportamentos dos aplicativos e outras entradas críticas. Esse modelo se adapta continuamente com base em observações e políticas definidas pelo cliente, reduzindo significativamente o tempo e a complexidade tradicionalmente associados à segmentação.

Com a Segmentação Autônoma do Hypershield, proteja seus aplicativos de forma mais eficaz e preventiva, mantendo os adversários afastados.

Recursos principais

- **Adaptação contínua**. A rede se segmenta, ajustando-se dinamicamente às realidades atuais e garantindo uma proteção sempre atualizada.
- **Informado por dados abrangentes**. Nossa estratégia de segmentação vai além dos fluxos de rede, incorporando diversas entradas, como comportamentos de processos e atualizações de aplicativos. Essa abordagem holística garante uma segmentação sutil e altamente eficaz.
- **Controles de precisão, começando com macro-guardrails**. Começando com parâmetros de proteção amplos, o sistema ajusta seus controles até filtros regex específicos, garantindo uma mitigação de riscos precisa e eficaz.

Atualizações de autoqualificação

As atualizações de software tradicionais para infraestrutura ou mudanças de políticas representam um alto risco de interrupção das operações comerciais. Essas atualizações exigem tempo e recursos significativos para teste, limitando-as geralmente a algumas vezes por ano. Esse ciclo de atualização lento deixa as organizações vulneráveis a ameaças emergentes com defesas desatualizadas. O Hypershield apresenta uma solução inovadora para esse desafio com sua tecnologia de **dual dataplane**. Essa abordagem inovadora permite que o tráfego de produção ao vivo opere de acordo com as regras atuais, enquanto envia simultaneamente uma cópia desse tráfego para um dataplane sombra. Esse plano sombra testa novas atualizações de software ou mudanças de políticas sem impactar o ambiente de produção real.

Com o dual dataplane do Hypershield, as equipes de TI e segurança agora podem implantar atualizações com mais frequência e com maior confiança, garantindo defesas robustas contra as últimas ameaças sem interromper os processos comerciais.

Recursos principais

- **Teste não disruptivo**. O dataplane sombra avalia novas políticas e atualizações de software espelhando o tráfego ao vivo, garantindo que as operações de produção permaneçam inalteradas.
- **Melhoria contínua**. Ao testar as atualizações em tempo real, o Hypershield reduz significativamente o tempo e os recursos normalmente necessários para atualizações tradicionais.
- **Tomada de decisão informada**. Após o teste, o Hypershield gera relatórios detalhados e fornece recomendações com respaldo de IA sobre se as novas atualizações devem ser implantadas, aumentando a confiança e a eficiência operacional. Além disso, os operadores podem obter mais confiança por meio de um assistente de IA que ajuda a explicar os resultados e as recomendações.

Arquitetura do Cisco Hypershield

Não é a próxima geração de nada. É a primeira geração de algo novo.

Ao tornar a tecnologia hyperscaler acessível a empresas de todos os tamanhos, o Hypershield permite eficácia superior, experiências aprimoradas e melhores economias na segurança da infraestrutura e sistemas de aplicativos em escala de IA. **Mais uma estrutura do que uma cerca**, o Hypershield coloca a aplicação da segurança exatamente onde é necessário, de forma contínua eem alta velocidade na nuvem, em ambientes altamente distribuídos.

Aqui estão os principais componentes em torno dos quais a solução é arquitetada:

Agente de Segurança Tesseract (TSA): Esse agente seguro e de alto desempenho opera na carga de trabalho, interagindo com processos e o kernel do sistema operacional por meio do Extended Berkeley Packet Filter (eBPF[1]). Otimizado para implantação fácil em ambientes Kubernetes, o TSA também é totalmente funcional em configurações não-Kubernetes. Ele oferece visibilidade completa das ações da carga de trabalho, monitorando conexões de rede, chamadas de arquivo e sistema e funções do kernel, e alerta sobre atividades anômalas.

Pontos de aplicação de segurança baseados em máquina virtual e contêiner. O Hypershield inclui pontos de aplicação de segurança que operam dentro de uma máquina virtual ou contêiner.

Eles são estrategicamente colocados próximos à carga de trabalho para proteger ativos específicos de forma mais eficaz, afastando-se das abordagens tradicionais de aplicação centralizada.

Gerenciamento unificado na nuvem. Independentemente do formato ou localização do ponto de aplicação de segurança, todas as políticas são organizadas e gerenciadas centralmente por meio do console de gerenciamento do Hypershield. Políticas novas ou atualizadas são " compiladas" e distribuídas de forma inteligente para os pontos de aplicação de segurança apropriados. Esse sistema garante que os administradores de segurança mantenham uma visão geral abrangente de todas as políticas implantadas, que podem se adaptar dinamicamente a cargas de trabalho que se movem entre ambientes locais e nuvens públicas ou entre servidores.

Nativo de IA. Projetado desde o início com integração de IA, o Hypershield oferece alta eficácia, resposta rápida e proteção contínua. O sistema pode escrever, testar, implantar e gerenciar autonomamente suas próprias regras, aproveitando o dual dataplane e a visibilidade extensiva em toda a rede e cargas de trabalho. Um assistente de IA também está disponível para explicar a análise, comportamentos observados, recomendações e muito mais, ganhando confiança por meio de níveis apropriados de autonomia e controle.

Saiba mais

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C45-4333084-00 04/24