PRISMA CLOUD
BY PALO ALTO NETWORKS

Prisma Cloud para Microsoft Azure

Proteja todos os recursos em seu ambiente Azure com o Prisma Cloud

Benefícios do Prisma Cloud para Azure

- Visualize todos os recursos conectados em todo o ambiente Azure.
- Mantenha conformidade ininterrupta e gere relatórios com facilidade em todo o ambiente Azure.
- Habilite DevOps seguras ao definir as proteções com monitoramento em tempo real de ameaças, como configurações arriscadas, atividades sigilosas de usuários, intrusões de rede e vulnerabilidades de host.
- Use os recursos de detecção de anomalias para erradicar comprometimentos de contas e ameaças internas.
- Investigue ameaças atuais ou incidentes anteriores e descubra com rapidez as causas raíz.
- Obtenha alertas contextuais para ajudar sua equipe a priorizar os problemas e resolvê-los com mais rapidez.
- Integração perfeita com os serviços nativos Azure, incluindo o Azure Security Center.

O Prisma Cloud simplifica as defesas contra ameaças da nuvem para o Microsoft Azure

A adoção da computação na nuvem pública está superando as defesas da segurança cibernética. A ausência de limites de uma rede física para a Internet, o risco de exposição acidental por usuários inexperientes, a visibilidade descentralizada e a natureza dinâmica da nuvem aumentam a superfície do ataque por ordem de grandeza. Embora os produtos pontuais de segurança possam resolver desafios singulares, eles não podem oferecer proteção holística em um ambiente em que os recursos estão em constante mudança como no Microsoft Azure®.

O Prisma™ Cloud (antigo RedLock) é um serviço de segurança e conformidade que descobre dinamicamente mudanças nos recursos da nuvem e correlaciona continuamente fontes de dados brutos e em silos, incluindo atividade do usuário, configurações de recursos, tráfego de rede, inteligência de ameaças e feeds de vulnerabilidade, para fornecer uma visão completa do risco da nuvem pública. Por meio de uma abordagem inovadora e impulsionada pelo aprendizado de máquina, o Prisma permite que as organizações priorizem com rapidez os tipos de riscos, mantenham agilidade no desenvolvimento e cumpram suas obrigações de forma eficiente no Modelo de Responsabilidade Compartilhada.

Principais recursos e benefícios para proteger o Azure

Visibilidade inigualável

Visualize todo o ambiente Azure, cada componente. O Prisma Cloud descobre dinamicamente os recursos e aplicativos da nuvem, correlacionando continuamente a configuração, a atividade do usuário e os dados de tráfego da rede. Combinando esse conhecimento abrangente do ambiente Azure com os dados de fontes externas, como feeds de inteligência de ameaças e testes de vulnerabilidade, o Prisma entrega um contexto completo de cada risco.

Conformidade simplificada da nuvem

O Prisma Cloud inclui políticas pré-integradas que aderem às melhores práticas padrão do setor, como as que foram apresentadas por CIS, GDPR, NIST, SOC 2 e PCI. Você também pode criar políticas personalizadas com base nas necessidades específicas de sua organização. O Prisma monitora continuamente a violação das políticas em todos os recursos conectados e suporta relatórios com um clique para a realização de auditorias simplificadas de seu ambiente Azure.

Proteções de política

O Prisma Cloud permite definir proteções para DevOps a fim de manter o rápido desenvolvimento sem sacrificar a segurança. Isso permite que você detecte ameaças, como configurações arriscadas, atividades sigilosas de usuários, intrusões na rede e vulnerabilidades de hosts. O Prisma classifica automaticamente as escalas de riscos para todos os recursos, com base na magnitude dos riscos para os negócios, violações e anomalias; o que ajuda as SecOps a identificar com rapidez os recursos mais arriscados e priorizar as ações de correção.

Detecção de ameaças

O Prisma Cloud detecta automaticamente anomalias no comportamento de usuários e terceiros em todo o ambiente Azure, definindo parâmetros comportamentais e identificando quaisquer desvios. Por exemplo, um possível comprometimento de chave de acesso será sinalizado se um usuário estiver tentando usar chaves a partir de dois locais ao mesmo tempo que, geograficamente, são incompatíveis.

Investigação de incidentes

Com ampla compreensão do ambiente Azure, o Prisma Cloud reduz o tempo de investigação para segundos. Você pode identificar com rapidez os problemas, realizar análises de impacto de upstream e downstream e revisar o histórico de mudanças de um recurso, para entender melhor a causa raiz de um incidente. Por exemplo, você pode realizar uma pesquisa para encontrar todos os bancos de dados que estavam se comunicando diretamente pela internet no último mês. O mapa resultante encontrará todos os casos e destacará os recursos que podem estar comprometidos.

Alertas contextuais e respostas adaptativas

O Prisma Cloud permite que suas equipes respondam com rapidez aos problemas com base em alertas contextuais. Esses alertas, acionados com base em metodologias de classificação de riscos com pendência de patente, oferecem contexto para todos os fatores de risco associados a um recurso, simplificando a priorização dos problemas mais importantes. Você pode enviar alertas, orquestrar políticas ou realizar correções automáticas. Você também pode direcionar alertas para ferramentas como Slack®, Splunk® e nosso próprio Demisto® para corrigir problemas. No caso de um banco de dados de risco, o Prisma vai gerar um alerta contextual com informações sobre os fatores de risco para habilitar uma resposta automática.

Integração com o Azure Security Center

O Prisma Cloud se integra com o Azure Security Center para oferecer visibilidade centralizada da segurança e dos riscos de conformidade em todo o ambiente Azure. Com isso, as equipes de segurança podem coletar dados com rapidez, identificar ameaças e tomar providências antes que haja danos ou perdas para o negócio.

Desenvolvimento de roteiro de defesa contra ameaças na nuvem do Microsoft Azure

O Prisma Cloud permite o desenvolvimento de um programa de defesa de ameaças na nuvem em todo o ambiente Azure, desde a gênese até a maturidade, com os seguintes recursos:

- **Garantia de conformidade:** o mapeamento das configurações dos recursos da nuvem para frameworks de conformidade, como CIS, GDPR, PCI DSS e HIPAA, pode ser muito demorado. Usando as políticas predefinidas, o Prisma permite o monitoramento contínuo, as correções automáticas e os relatórios com um clique, simplificando o processo de permanecer em conformidade.
- **Governança da segurança:** visibilidade incompleta e controle impreciso sobre as mudanças em ambientes de computação em nuvem pública podem dificultar a governança da segurança. O Prisma habilita a validação de arquiteturas definindo proteções de políticas para detectar e corrigir imediatamente os riscos em todas as configurações de recursos, arquitetura de rede e atividades de usuários. Com o Prisma, você pode finalmente suportar a agilidade das DevOps sem sacrificar a segurança.
- **Habilitação do SOC:** as equipes de operações de segurança são bombardeadas com alertas que oferecem pouco contexto sobre os problemas, o que dificulta a triagem desses problemas em tempo hábil. O Prisma possibilita a identificação de vulnerabilidades, detecta ameaças, investiga incidentes atuais e passados e resolve esses problemas em todo o ambiente Azure em minutos.

Estágio 1: Adotar	Estágio 2: Ampliar	Estágio 3: Dimensionar
Mapeamento da nuvem: • Dezenas de cargas de trabalho • Poucas contas na nuvem	**Mapeamento da nuvem:** • Centenas de cargas de trabalho • Muitas contas na nuvem	**Mapeamento da nuvem:** • Vários provedores de nuvem • Milhares de cargas de trabalho • Dezenas de contas na nuvem
Objetivos: • Garantia de conformidade • Governança da segurança	**Objetivos:** • Visibilidade centralizada • Detecção de ameaças • Gerenciamento de vulnerabilidades **+ Objetivos do estágio 1**	**Objetivos:** • Correção automática • Investigação de incidentes **+ Objetivos do estágio 1**

Figura 1: Modelo de maturidade das defesas de ameaças na nuvem

Pacote de segurança do Prisma Cloud

O Prisma Cloud oferece ampla visibilidade, detecção de ameaças e resposta rápida em todo o seu ambiente de nuvem pública, inclusive no Amazon Web Services, Microsoft Azure e Google Cloud Platform. Uma combinação exclusiva de monitoramento contínuo, garantia de conformidade e análise de segurança permite que as equipes de segurança respondam com mais rapidez às ameaças mais críticas substituindo investigação manual por relatórios automáticos, priorização de ameaças e correção. Com a sua abordagem baseada em API, o Prisma entrega uma segurança superior nativa na nuvem.

PRISMA CLOUD
BY PALO ALTO NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087

www.paloaltonetworks.com

prisma-cloud-for-microsoft-azure-ds-052119