Tripwire Enterprise 8.7

Detectar. Responder. Prevenir.

O Tripwire® Enterprise é um conjunto de SCM (security configuration management, gerenciamento de configurações de segurança) que oferece soluções totalmente integradas para o gerenciamento de políticas, integridade e correção de arquivos. As organizações podem usar essas soluções juntas para uma solução end-to-end completa de SCM ou usar as soluções de monitoramento da integridade de arquivos ou de gerenciamento de políticas separadamente, a fim de lidar com os desafios atuais de segurança e de conformidade, enquanto desenvolvem uma base que as direciona para o futuro.

O Tripwire tem mais de duas décadas de experiência no setor de segurança e conformidade, com tecnologia de base essencial para detectar ameaças cibernéticas, respostas rápidas e em tempo real e prevenção contra ataques futuros.

O Tripwire Enterprise manteve mais de metade das empresas Fortune 500 e muitas das mais sensíveis redes do mundo seguras e em conformidade, com suas capacidades, atendendo a muitos requisitos de segurança e conformidade com as políticas.

O conjunto permite que as equipes de segurança, conformidade e operações de TI atinjam rapidamente o nível fundamental de segurança em toda a infraestrutura de TI, reduzindo a superfície de ataque, aumentando a integridade do sistema e proporcionando conformidade contínua. Além disso, devido ao fato do Tripwire Enterprise integrar-se a aplicações empresariais para automatizar o fluxo de trabalho com soluções de ponta adicionais, como ferramentas de SIEMs e de gerenciamento de mudança, as organizações podem ampliar sua visão global de segurança e obter eficiências ainda melhores.

Uma solução empresarial chave para segurança de TI e conformidade, O Tripwire Enterprise suporta uma estratégia de detecção, resposta e prevenção pela:

- **Detecção** de ameaças cibernéticas e eventuais atividades de violação ao destacar possíveis indicadores de falhas
- **Resposta** a desvios com altos valores, alertas de baixo volume com orientações sobre como retornar o sistema a um estado de segurança conhecido
- **Prevenção** ao adaptar e priorizar ameaças e alterar desvios para manter uma visão consistentemente reforçada e objetiva da postura de segurança geral em todos os dispositivos e sistemas

Como isso funciona: Controles rigorosamente integrados

O Tripwire Enterprise oferece cinco recursos integrados que funcionam em conjunto para criar uma solução de SCM :

- **O Tripwire File Integrity Manager** é a primeira e melhor solução de monitoramento de integridade de arquivos (file integrity monitoring, FIM) do mundo. Ele verifica grandes ambientes heterogêneos para fornecer detecção de ameaças e percepções instantâneas sobre vulnerabilidades de configuração, aumentando a eficiência operacional ao reduzir o desvio de configuração e alterações não autorizadas.
  O FIM da Tripwire pode ser usado de maneira independente para fornecer inteligência de terminal granular

com uma percepção rápida da postura de segurança e de conformidade. Quando usado com o Tripwire Policy Manager, ele fornece avaliação de configuração acionada por alterações e outras respostas configuráveis pelo sistema. Isso torna uma avaliação de configuração "passiva" em uma solução de defesa dinâmica, contínua e em tempo real que detecta imediatamente os desvios de padrões de configuração e diretrizes de fortalecimento seguros e esperados.

» **O Tripwire Policy Manager** estabelece e mantém uma avaliação de configuração contínua consistente sem agente e com base em agente de conformidade com mais de 1.000 (mil) combinações de plataformas e políticas de segurança e conformidade, normas, regulamentos e diretrizes de fornecedores. O Policy Manager também oferece personalização completa de políticas, gerenciamento de isenções e exceções, opções de correção automatizada e pontuação de políticas priorizadas com limites, pesos e severidade. Ele faz tudo isso enquanto fornece auditores com evidências de conformidade e torna o status de políticas altamente visível e acionável para as equipes de conformidade.

» **O Remediation Manager** opera junto com o Tripwire Policy Manager para fornecer diretrizes integradas para que as equipes de segurança de TI e de conformidade reparem configurações de segurança alteradas e desalinhadas enquanto retém o gerenciamento com base em funções, aprovações e assinaturas para reparos. Isso ajuda as equipes de operações a saber com mais facilidade e eficiência o que falhou e como retornar os sistemas a um estado já pronto para produção e, uma vez em produção, mantê-los lá.

» **Investigações e recursos de detalhamento da causa raiz** oferecem às equipes de segurança e operações de TI a capacidade de investigar com rapidez e eficácia para determinar as causas raizes. Os sistemas inevitavelmente mudam à medida que as empresas revisam e mudam constantemente seus funcionários, processos e tecnologias. O Tripwire Enterprise pode oferecer detalhamentos granulares, comparações lado a lado, linhas de base e comparações históricas para fornecer rapidamente às equipes de investigação o que elas precisam saber: o que mudou, quando, por quem e com que frequência e com as informações sobre "como".

» **A plataforma Tripwire Axon®** permite a coleta flexível de dados e a comunicação robusta em uma ampla variedade de dispositivos, nuvem e ativos virtualizados. A plataforma Tripwire Axon aborda os desafios da coleta, utilizando um agente extensível e com recursos, técnicas de mensagens assíncronas e definições de mensagens neutras de produto e de plataforma. O agente Tripwire Axon é otimizado para recursos mínimos do sistema e utilização de largura de banda de rede. Os binários do agente são implementados em C++ para minimizar o rastro e maximizar o desempenho.

Recursos de segurança e de conformidades TI líderes na indústria

A Tripwire está adicionando continuamente novos recursos ao Tripwire Enterprise para atender aos crescentes desafios de segurança e conformidade. O Tripwire Enterprise agora tem novos recursos para monitorar ativos na nuvem, proteger dispositivos industriais e descobrir evidências de comportamento indevido em seu ambiente usando a estrutura MITRE ATT&CK.

» **Cloud Management Assessor** O Cloud Management Assessor da Tripwire ajuda os usuários do Tripwire Enterprise a determinar o estado de segurança de suas implantações do Amazon Web Services (AWS), do Microsoft Azure e do Google Cloud Platform ao reunir, analisar e pontuar dados de configuração de conta com base nas melhores práticas (como o Center for Internet Security AWS Foundations v1.1.0 Benchmark).

Além disso, o avaliador de gerenciamento de nuvem pode avaliar automaticamente seus depósitos do AWS S3 e o armazenamento do Azure para determinar se eles estão expostos para acesso anônimo e relatar os objetos que foram expostos recentemente.

» **Tripwire Data Collector** O Tripwire Data Collector amplia as principais capacidades do Tripwire Enterprise de detecção de alterações e conformidade com as políticas no ambiente industrial. O monitoramento de ambientes de tecnologia operacional (operational technology, OT) tem seu conjunto exclusivo de desafios. A arquitetura sem agente do Tripwire Data Collector foi projetada desde o início para avaliar configurações, segurança e status, incluindo firmware, revisão

A Tripwire pegou sua ferramenta original de detecção de intrusão com base em hosts, que poderia simplesmente detectar alterações em arquivos e pastas, e expandiu-a para uma robusta solução de monitoramento de integridade de arquivos (FIM), capaz de monitorar a integridade detalhada do sistema: arquivos, diretórios, registros, parâmetros de configuração, DLLs, portas, serviços, protocolos, etc. E as integrações corporativas fornecem inteligência de terminal granular que oferece suporte à detecção de ameaças e à conformidade de políticas e auditoria. Os anos foram gastos aprimorando a capacidade da Tripwire de detectar e julgar mudanças com políticas e priorizações de risco de segurança e refinamentos de integração para atingir alertas de alto valor e baixo volume de alterações. O Tripwire Enterprise ajuda as maiores empresas a gerenciar a integridade, segurança e conformidade da configuração do sistema.

de hardware, versões de software, níveis de correções e muito mais.

O Tripwire Data Collector tem a capacidade de se comunicar com dispositivos através de uma variedade de protocolos industriais, como Modbus TCP, Ethernet/IP CIP e SNMP. Para dispositivos que não podem ser tocados, as informações de configuração podem ser coletadas por meio de integrações com o FactoryTalk AssetCentre da Rockwell Automation, o MDS AutoSave e o KEPServerEX da Kepware. Os dados de configuração também podem ser coletados usando o Web Retriever, que pode verificar dados de configuração de páginas da web.

» **MITRE ATT&CK Framework**
Desenvolvido pela empresa MITRE, o ATT&CK Framework é um modelo útil de segurança cibernética que ilustra

Preparado para se aprofundar ainda mais?

Para saber mais sobre os recursos do Tripwire Enterprise, relatórios, políticas disponíveis, suporte à plataforma e mais, clique em ou visite o site tripwire.com para obter as seguintes especificações:

- » Catálogo de Relatórios do Tripwire Enterprise
- » Tripwire Enterprise Policy Manager
- » Tripwire Connect
- » Tripwire Enterprise Remediation Manager
- » Tripwire Enterprise Agent Platform Support
- » Tripwire Axon
- » Tripwire Axon Agent Platform Support

Recursos e benefícios

Plataforma de coleta e comunicação de dados atualizada	O Tripwire Enterprise oferece a melhor segurança, monitoramento de integridade e gerenciamento de configuração e conformidade com o Tripwire Axon®, uma plataforma de coleta e comunicação de dados de terminais , extensível e de alto desempenho. Os usuários se beneficiam da incomparável visibilidade e resistência cibernética enquanto reduzem os encargos operacionais e melhoram a capacidade de resposta.
Suporte para ambientes híbridos	O Tripwire Enterprise pode monitorar ambientes no local e na nuvem para segurança e conformidade. Os clientes podem reduzir custos e fornecer melhor visibilidade usando uma única solução para ambos os ambientes.
Um único ponto de controle para todas as configurações de TI	O Tripwire Enterprise oferece controle centralizado de configurações em toda a infraestrutura física e virtual de TI, incluindo servidores e dispositivos, e várias plataformas e sistemas operacionais.
Integração avançada por meio de REST APIs	Rest APIs atualizadas permitem que o valor do Tripwire Enterprise seja integrado a outros aplicativos. Rest APIs permitem o comando programático e o controle de aplicativos, comoo Tripwire Enterprise, e também a extração de informações coletadas. APIs de administração permitem a automação de tarefas, como ativar o monitoramento em tempo real ou executar políticas.
Monitoramento de rede OT	Usando o coletor de dados da Tripwire com o Tripwire Enterprise, os usuários podem monitorar sua rede industrial em busca de alterações e conformidade, resultando em um ambiente mais seguro sem comprometer a disponibilidade.
Recursos de Asset View consistentes	O Asset View permite que você classifique os ativos com marcações relevantes dos negócios como risco, prioridade, localização geográfica, políticas regulatórias e mais. Os recursos de visualização de ativos do Tripwire Enterprise agora oferecem provisionamento com um arquivo de tags de ativos, maior escala para grandes números de ativos e identificação de ativos importados da integração com o Tripwire IP360, proporcionando uma visualização mais nítida dos riscos em toda a organização.
Ferramentas de fluxo de trabalho para gerenciamento de configurações com falhas	O módulo Remediation Manager fornece ferramentas de fluxo de trabalho baseado em funções que permitem aos usuários aprovar, recusar, diferir ou executar o reparo de configurações com problemas.
Integração com sistemas de gerenciamento de alterações	Como o Tripwire Enterprise se integra às principais soluções de CMS (change management system), à medida que ocorrem alterações, o Tripwire Enterprise reconcilia automaticamente as alterações detectadas com os tíquetes de alteração e as solicitações de alteração.
Preparação de auditoria mais rápida e fácil	O Tripwire Enterprise reduz drasticamente o tempo e o esforço de preparo para auditorias, fornecendo linhas de base contínuas e completas da infraestrutura de TI juntamente com a detecção de alterações em tempo real e inteligência embutida para determinar o impacto da alteração.
Suporte para manutenção de um estado de conformidade seguro	O Tripwire Enterprise combina avaliação de configuração com monitoramento de integridade de arquivos (FIM) em tempo real para detectar, analisar e reportar alterações à medida que ocorrem e manter as configurações sempre em conformidade. Esse acesso imediato a informações sobre alterações permite que a TI corrija problemas antes que resultem em importantes violações de dados, problemas de auditoria ou paralisações de longo prazo.
Processos de conformidade automáticos de TI	O Tripwire Enterprise automatiza a conformidade com as regulamentações e os padrões da indústria a que as organizações agora estão sujeitas, desde PCI, a NERC, SOX, FISMA, DISA e muitos outros.

como os adversários se comportam e explica as táticas que você deve usar para atenuar riscos e melhorar a segurança. Usando o conteúdo da política do ATT&CK Framework para o Tripwire Enterprise, você pode detectar e relatar o comportamento não desejado em seu ambiente. O conteúdo do ATT&CK permite adicionar uma nova camada de defesa à sua estratégia de segurança.

Suporte corporativo

Tripwire Enterprise pode operar com ou sem agentes, e suporta:

- **Todos os principais sistemas operacionais:** Windows, Red Hat, CentOS, Ubuntu, SUSE e Debian
- **Muitos sistemas operacionais específicos de fornecedores:** AIX, Solaris, HP-UX, etc.
- **Serviços de diretório:** Active Directory, LDAP, etc.
- **Dispositivos de rede:** Configurações de firewall, IPS e IDS, roteadores, etc.
- **Bancos de dados:** Oracle, MS SQL, DB2 e PostgreSQL

Suporte abrangente e profundo a componentes na pilha de TI

Quer a TI precise monitorar todos os servidores críticos para a missão ou toda a infraestrutura de TI, incluindo ambientes e aplicativos virtualizados, o Tripwire Enterprise oferece a capacidade de acessar, validar e aplicar políticas, e de detectar todas as alterações qualquer que seja a fonte. A Tripwire oferece suporte aos seguintes componentes da pilha de TI.

Suporte Tripwire Enterprise de toda a pilha de serviços

Aplicativos	Tripwire Enterprise oferece recursos para gerenciamento de políticas de conformidade e monitoramento de integridade de arquivos para ajudar a garantir que os aplicativos suportados estejam adequadamente configurados para segurança, conformidade e desempenho e disponibilidade.
Serviços de diretório	Tripwire Enterprise oferece gerenciamento de políticas de conformidade independente para objetos e atributos de servidor de diretório compatível LDAP, como esquema, configurações de senha, permissões de usuário, recursos de rede, atualizações de grupo e políticas de segurança do LDAP.
Bancos de dados	Tripwire Enterprise funciona em conjunto com o componente File Systems da Tripwire para ajudar as empresas a colocarem seus servidores de bancos de dados Oracle, Microsoft e IBM em um estado seguro, com alto desempenho constante.
Sistemas de arquivos e áreas de trabalho	Tripwire Enterprise acessa as configurações do servidor físico e virtual, e os sistemas de arquivos de desktop, incluindo configurações de segurança, parâmetros de configuração e permissões.
Dispositivos de ponto de venda (Point-of-Sale, POS)	O Tripwire Enterprise protege dispositivos de POS contra ameaças cibernéticas, gerencia políticas de segurança e conformidade para esses dispositivos e fornece alertas, notificações e orientações de resposta às operações de TI quando houver suspeita de possíveis indicadores de violação ou "indicadores de comprometimento" nesses dispositivos.
Ambientes virtualizados	O Tripwire Enterprise funciona em ambientes virtualizados - nuvens privadas, públicas e híbridas. O console Tripwire Enterprise pode operar como uma máquina virtual e seus agentes podem monitorar qualquer terminal virtualizado aceito. Isso inclui proteção para ameaças cibernéticas em ambientes virtualizados/em nuvem, monitoramento da integridade do sistema, aplicação de políticas de segurança e conformidade, painéis, relatórios e alertas e notificações em tempo real.
VMware	O Tripwire Enterprise oferece visibilidade em toda a infraestrutura virtual VMware, permitindo o controle constante de configuração de ambientes virtuais.
Dispositivos de rede	O Tripwire Enterprise acessa as definições de configuração da maior gama de dispositivos de rede da indústria, incluindo qualquer dispositivo que execute um sistema operacional compatível com POSIX.

tripwire

A Tripwire é a líder mais confiável para estabelecer uma forte base de cibersegurança. Em parceria com empresas da Fortune 500, organizações industriais e agências governamentais, a Tripwire protege a integridade de sistemas críticos em ambientes físicos, virtuais, em nuvem e de DevOps. O premiado portfólio da Tripwire proporciona os mais importantes controles de segurança, inclusive descoberta de ativos, gerenciamento seguro de configurações, gestão de vulnerabilidades e de registros. Como pioneira no monitoramento da integridade de arquivos (file integrity monitoring, FIM), a experiência da Tripwire se fundamenta em uma trajetória de mais de 20 anos de inovação, ajudando organizações a descobrirem, minimizarem e monitorarem suas superfícies de ataque. **Mais informações em tripwire.com**

Saiba mais em tripwire.com e receba notícias, tendências e valiosas informações sobre segurança em tripwire.com/blog, ou conecte-se conosco no LinkedIn, no Twitter e no Facebook.

TEDS870aPTBR 1806