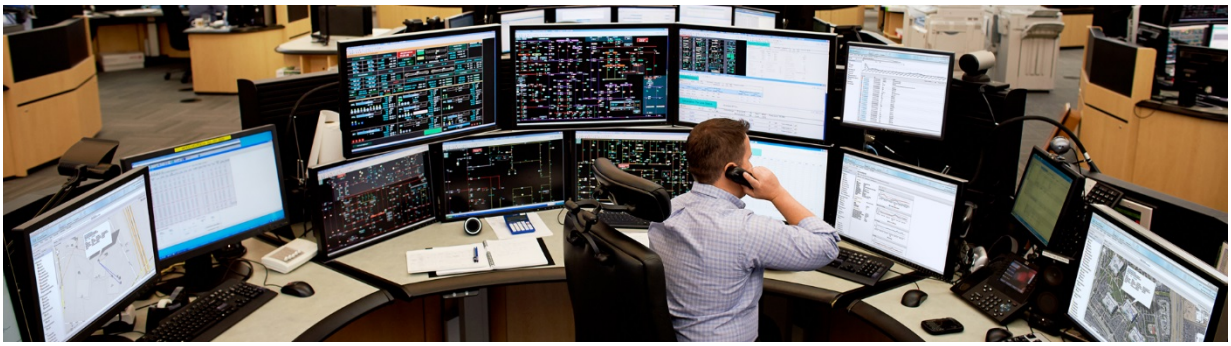

Cisco AMP Threat Grid: torne-se proativo com a segurança de malware avançado

VANTAGENS

- Obter uma percepção mais profunda para uma defesa mais forte com a análise estática e dinâmica de malware
- Identificar ataques com precisão, quase em tempo real, com análises de segurança focadas no contexto
- Proteger de forma proativa as empresas usando inteligência de ameaças dos melhores feeds de ameaça
- Acelerar os recursos de detecção e de resposta a ameaças com uma API poderosa que integra e automatiza produtos e processos de segurança existentes
- Defender-se de ameaças de qualquer lugar com a escala e a força de um serviço em nuvem que analisa centenas de milhares de amostras todos os dias

O malware avançado atual se esconde debaixo dos nossos olhos, escapa das defesas e aguarda pacientemente a hora de atacar. As equipes de segurança enfrentam o desafio de detectar e analisar ameaças avançadas quando suas tecnologias de segurança não têm os conhecimentos e a interconexão necessários para bloqueá-las.

As empresas estão sob ataque constante, com violações de segurança que ocorrem diariamente. Os ataques de maior visibilidade estão virando notícias de primeira página. Uma comunidade global de invasores está criando malwares avançados e lançando-os por meio de ataques multifacetados e de vários vetores de ataque em empresas de todos os portes. As empresas ainda estão usando ferramentas desatualizadas e métodos parcialmente eficazes para proteger seus dados confidenciais, principalmente com tecnologia de assinaturas. As equipes de segurança agora têm uma janela muito mais curta para identificar e corrigir o malware. Além disso, as empresas estão enfrentando uma escassez significativa de pessoal com o conhecimento e a experiência necessários para entender e oferecer proteção contra malwares avançados.

O Cisco® AMP Threat Grid combina análise estática e dinâmica de malware com inteligência de ameaças em uma única solução disponibilizada na nuvem ou como uma solução local. Ele integra análise comportamental e feeds de inteligência de ameaças atualizados à sua infraestrutura de segurança atual. Com o AMP Threat Grid, você entende o que o malware está fazendo ou tentando fazer, o tamanho da ameaça que ele traz e como se defender contra ele.

Os ataques crescentes enfraquecem as abordagens de segurança tradicionais

De acordo com o Relatório de Segurança Anual da Cisco de 2015, os criminosos digitais estão projetando malware que usa ferramentas de confiança dos usuários para infectar de maneira persistente seus computadores, escondendo-se diretamente neles. O relatório da Pesquisa Global de Segurança da Informação promovida pela PWC em 2014 descobriu que as empresas estão detectando 25% mais incidentes do que no ano anterior. As perdas geradas por esses incidentes tiveram alta de 18% ao longo de um ano. O Relatório de Investigações sobre Violações de Dados publicado pela Verizon em 2014 mostra que três quartos dos ataques agora comprometem as empresas em dias e até mesmo em horas. A pesquisa mostra também que pode levar semanas ou até meses para uma empresa perceber que está sendo atacada. E esse período está aumentando.

De acordo com a pesquisa de gastos de TI de 2015 da ESG Global, 28% das empresas de médio e grande porte dizem estar enfrentando uma escassez crescente de expertise relacionada à segurança de TI em suas empresas.

As empresas de segurança estão sobrecarregadas, travando uma difícil batalha contra o desafio imposto pelas ameaças avançadas. Elas têm janelas muito mais curtas para identificar e responder a ataques, e é muito mais difícil entender o que está acontecendo em um ambiente corporativo grande e moderno, devido em parte à falta de comunicação entre as tecnologias de segurança. E, como existem poucos funcionários especializados em segurança disponíveis e orçamentos limitados para as novas defesas, as empresas estão se tornando cada vez mais vulneráveis.

Resumo do Cisco AMP Threat Grid

O AMP Threat Grid fornece informações detalhadas necessárias para proteger melhor as empresas contra o malware. Com sua base de conhecimento robusta e contextual sobre malware, as empresas podem entender o que o malware está fazendo ou tentando fazer, qual o tamanho da ameaça e como se defender contra ela. A solução inclui os seguintes recursos:

Análises de malware

O AMP Threat Grid coleta informações sobre malware de maneira segura de uma comunidade fechada e analisa todas as amostras usando técnicas próprias altamente seguras que incluem análise estática e dinâmica. Ao contrário das tecnologias de sandboxing tradicionais, nossa análise proativa fica fora do ambiente virtual, identificando códigos mal-intencionados que são projetados para evitar a análise. Como parte da análise, o recurso Glovebox interage com o malware em tempo real, registrando todas as atividades para reprodução futura e criação de relatórios.

Integração da borda da rede aos endpoints

O AMP Threat Grid é integrado às tecnologias de segurança da Cisco para oferecer análise de malware da borda da rede aos endpoints. Essas tecnologias incluem o Cisco AMP for Networks, o Cisco ASA com FirePOWER™ Services, o Cisco Email Security Appliance, o Cisco Web Security Appliance e o Cisco AMP for Endpoints. A capacidade combinada do AMP Threat Grid com essas tecnologias de detecção significa que as empresas obtêm mais visibilidade em mais lugares do que nunca. Agora é possível compartilhar, correlacionar e sintetizar informações em vários pontos de controle de segurança para que as empresas possam tomar melhores decisões mais rapidamente, a fim de eliminar as ameaças e reduzir o dano de violações causadas por malware com mais rapidez.

Capacitação de tecnologias de segurança atuais

O AMP Threat Grid integra-se de modo transparente à infraestrutura segura atual de uma empresa. Ele pode consumir automaticamente envios de agentes de endpoint, plataformas de inspeção profunda de pacotes, ferramentas de investigação forense e muito mais com a API de transferência de estado representativo (REST) e de várias integrações de solução de parceiros.

Pontuação de ameaças

Com mais de 450 indicadores de comportamento e uma base de conhecimento de malware com dados coletados do mundo todo, o AMP Threat Grid faz análises contextuais de malware avançado mais precisas do que nunca. As amostras de malware enviadas ao AMP Threat Grid fornecem uma pontuação de ameaças com base em dois elementos principais: gravidade e confiança. Com os indicadores de comportamento, o AMP Threat Grid informa se uma amostra é mal-intencionada, suspeita ou benigna e por quê. Isso elimina as suposições e capacita os analistas de segurança júnior a tomar decisões melhores mais rapidamente.

Glovebox

O malware avançado utiliza inúmeras técnicas de evasão para verificar se está sendo analisado em um sandbox. Algumas dessas amostras exigem interação do usuário. O AMP Threat Grid disponibiliza o Glovebox, um ambiente seguro para analisar em detalhes essas amostras sem infectar a rede durante esse processo. O Glovebox é uma ferramenta versátil contra malware avançado que permite que os analistas abram aplicações e reproduzam um processo de fluxo de trabalho, vejam como o malware se comporta e até mesmo reiniciem a máquina virtual.

Feeds de ameaças que podem ser lidos pela máquina

O AMP Threat Grid fornece feeds altamente precisos de conteúdo premium. Tudo isso ajuda as empresas a gerar uma inteligência de ameaças contextual que, além de útil, seja específica. Usando uma API eficiente, você pode importar as informações de ameaças diretamente para as tecnologias de segurança atuais, incluindo soluções de gerenciamento de eventos e informações de segurança (SIEM), gateways, proxies, ferramentas de visualização e muito mais, a fim de automatizar a detecção e as respostas até mesmo para as ameaças mais sofisticadas.

Potência e escala da nuvem

O AMP Threat Grid coleta informações sobre malware de maneira segura de uma comunidade fechada e analisa todas as amostras usando técnicas próprias altamente seguras que incluem análise estática e dinâmica. Ele correlaciona os resultados com centenas de milhões de amostras de malware analisadas para apresentar uma visão global de ataques, de campanhas e de distribuição de malware. As equipes de segurança podem correlacionar rapidamente uma única amostra de atividade e as características observadas e compará-la com milhões de outras amostras para entender o seu comportamento em um contexto histórico e global.

A solução de nuvem do AMP Threat Grid permite que os usuários enviem milhares de amostras de cada vez para análise, recebendo relatórios abrangentes, com a identificação de indicadores importantes de comportamento e a atribuição de pontuações de ameaças em poucos minutos. Essas informações ajudam as equipes de segurança a priorizar e se recuperar rapidamente de ataques avançados.

Análise no local

O dispositivo AMP Threat Grid oferece uma análise local sobre malwares avançados com dados de análise e conteúdo minuciosos sobre a ameaça. As empresas com restrições de conformidade e políticas enviam amostras de malware ao dispositivo para análise, ajudando a garantir a conformidade com os requisitos organizacionais. Com o AMP Threat Grid, todas as amostras são analisadas usando técnicas proprietárias e altamente seguras de análise dinâmica e estática. Ele correlaciona os resultados aos bilhões de artefatos analisados de malware sem enviar informações fora dos limites lógicos de sua empresa.

Fortaleça sua equipe de segurança

Independentemente de estarem trabalhando no local ou na nuvem, as equipes de segurança podem usar o AMP Threat Grid para correlacionar rapidamente uma única amostra ou centenas de atividades e características observadas em contraponto a outras milhões de amostras para que você possa compreender totalmente o comportamento do malware em um contexto histórico e global. Isso ajuda você a preparar uma defesa eficaz contra ataques e ameaças direcionados de malwares avançados. Os relatórios detalhados do AMP Threat Grid, incluindo a identificação de indicadores importantes de comportamento e a atribuição de pontuação de ameaças, permitem que você priorize ataques avançados e se recupere rapidamente deles.

Como as equipes de segurança podem usar o Cisco AMP Threat Grid

A Tabela 1 ilustra como os diferentes integrantes de seu departamento de segurança podem usar o AMP Threat Grid.

Tabela 1. AMP Threat Grid em toda a empresa

Departamento/pessoal	Benefícios relevantes
Resposta a incidentes	• Analisa um único envio ou centenas de envios em minutos • Busca amostras mal-intencionadas usando endereços IP, hashes de arquivo, mutexes (objetos de exclusão mútua), nomes de domínios, teclas de registro e URLs • Interage com a amostra de malware usando o Glovebox
Operações de segurança	• Gera uma pontuação de ameaças para todos os envios de malware • Apresenta indicadores de comportamento de fácil compreensão para todos os analistas • Envia automaticamente amostras suspeitas para análise
Diretor executivo de segurança da informação	• Integra-se com tecnologias de segurança atuais • Acelera a detecção de ataques avançados e direcionados • Capacita as equipes de segurança para reagir mais rapidamente

Cisco Advanced Services para AMP Threat Grid

Integrar, automatizar e corrigir

As empresas usam o AMP Threat Grid para entender e proteger melhor seu ambiente contra o malware avançado atual. O Cisco Advanced Services pode ajudar sua empresa a integrar totalmente o mecanismo dinâmico de análise de malware e os envios automatizados de amostras do AMP Threat Grid. O Cisco Advanced Services ajuda você a aproveitar com rapidez os feeds de inteligência de ameaças do AMP Threat Grid, de modo que você possa usar as tecnologias de segurança atuais para enviar ou consumir automaticamente informações úteis.

"A integração do AMP Threat Grid em nosso ambiente complementa nossas tecnologias de proteção empresarial de segurança, riscos e privacidade com a inteligência de ameaças automatizada e integrada, o que aumenta sua eficácia e melhora nossa postura geral de defesa digital. Essa imagem de ameaça avançada permite que nossos centros básicos de resposta a incidente analisem e mitiguem a possibilidade da presença de malware mais rapidamente."

— Roland Global Cloutier, CSO, ADP

Cisco Capital

Financiamento para ajudar você a alcançar seus objetivos

A Cisco Capital pode ajudar você a adquirir a tecnologia necessária para alcançar seus objetivos e permanecer competitivo. Podemos ajudar a reduzir seu CapEx. Acelerar o crescimento. Otimizar o investimento e o ROI. O financiamento da Cisco Capital oferece flexibilidade na aquisição de hardware, software, serviços e equipamentos complementares de terceiros. E há apenas um pagamento previsível. A Cisco Capital está presente em mais de 100 países. Saiba mais.

Por que escolher a Cisco

As redes atuais alcançam os funcionários onde quer que eles estejam e se estendem aos dados, não importa onde estejam ou de onde possam ser acessados. Sendo assim, as tecnologias também devem se concentrar na detecção, compreensão e interrupção das ameaças. Concentrar-se nas ameaças significa aplicar a visibilidade e o contexto para compreender e se adaptar às mudanças no ambiente e, depois, desenvolver proteções para agir e interromper ameaças. O AMP Threat Grid apresenta o nível de análise minuciosa e o conteúdo da ameaça necessários para oferecer à sua empresa a proteção de que ela precisa hoje.

Próximas etapas

Para obter mais informações ou para ver exemplos reais de empresas que estão combatendo ameaças avançadas com o AMP Threat Grid, acesse http://www.cisco.com/go/amptg.

Sede - América
Cisco Systems. Inc
San Jose. CA

Sede - Ásia e Pacífico
Cisco Systems (USA) Pad Ltd.
Cingapura

Sede - Europa
Cisco Systems International BV Amsterdam,
Países Baixos

A Cisco possui mais de 200 escritórios no mundo todo. Os endereços, números de telefones e fax estão disponíveis no site **www.cisco.com/go/offices**.

Impresso nos EUA C22-734156-01 10/15