Estudo de Caso

Gestão Global de Segurança Facilitada para Prestador de Serviços de TI

Computer Sciences Corporation

Um engenheiro de segurança da informação e sua equipe protegem esse prestador global de serviços de TI e seus inúmeros clientes de maneira muito mais fácil e eficiente graças ao gerenciamento centralizado do software McAfee® ePolicy Orchestrator® (McAfee ePO™) e à plataforma unificada da Intel® Security.

Perfil do cliente

MSSP global para uma empresa de entretenimento global.

Setor

Entretenimento.

Ambiente de TI

200 mil endpoints em 70 países, com 'todos os tipos' de sistema operacional.

Desafios

- Falta de visibilidade entre endpoints devido ao ambiente de segurança diverso com múltiplas soluções pontuais.
- Proteger uma empresa geograficamente vasta e múltiplos clientes.
- Falta de gerenciamento de segurança centralizado.

Soluções McAfee

- Software McAfee VirusScan Enterprise
- Software McAfee VirusScan for Storage
- McAfee Host Intrusion Prevention for Servers
- Software McAfee ePolicy Orchestrator

Resultados

- Gerenciamento, geração de relatórios e implementações mais fáceis graças ao controle centralizado.
- Visibilidade em tempo real de todos os endpoints ao redor do mundo.
- Mais rapidez na detecção de incidentes e na correção de ameaças.
- Economia de tempo devido a uma administração mais eficiente e efetiva.

Como engenheiro de segurança da informação na Computer Sciences Corporation (CSC), uma das principais prestadoras de serviços de TI do mundo, Christopher Sacharok gerencia a segurança de endpoints diariamente para empresas clientes além de solucionar problemas de segurança para outras equipes de consultores da CSC. À medida que grandes quebras de sigilo de dados foram tomando as manchetes nacionais, Sacharok viu clientes da CSC, de grandes agências federais a pequenas corporações, empregando cada vez mais recursos na segurança.

"O lado bom dessas quebras de sigilo das quais todos ouviram falar é que a segurança está tomando seu devido lugar como prioridade", disse Sacharok. "Na CSC, nossa principal prioridade é fornecer um ambiente seguro que proteja os dados, garanta a continuidade dos negócios e atenda a todos os regulamentos necessários. Garantir que as operações de nossos clientes sejam realizadas o mais eficiente e efetivamente possível vem em seguida, mas a segurança vem em primeiro lugar".

Soluções pontuais representam uma carga de gerenciamento

"Um dos maiores desafios que vejo na maioria dos ambientes de TI é fazer com que as soluções de segurança se comuniquem", declarou Sacharok. "Os operadores de segurança precisam gastar muita energia tentando reunir dados de todos os produtos de hardware e software próprios e de terceiros em um local centralizado onde possam ser gerenciados eficientemente. Também é extremamente difícil gerenciar e proteger recursos ou cumprir com PCI e outros regulamentos".

Com soluções pontuais de múltiplos fornecedores protegendo seus próprios endpoints, a CSC costumava ter o mesmo problema.

Sem o gerenciamento central, não havia como checar o status da segurança em todos os 200 mil endpoints espalhados por 70 localidades e quatro continentes. Demonstrar conformidade com regulamentações de PCI e HIPAA para a Sarbanes-Oxley era difícil e demorado. Também é vantajoso ter um único painel para visualizar produtos similares de proteção de endpoints para diferentes sistemas operacionais. É um bônus adicional ter produtos individuais que relatam ao software McAfee ePO e que sejam melhores do que as proteções padrão do SO.

Solução: plataforma de segurança unificada com gerenciamento central

Após pesquisar opções de proteção de endpoints, a CSC adotou as soluções da Intel Security para ter uma plataforma de segurança unificada com gerenciamento centralizado e fácil de usar. A CSC implementou o software McAfee VirusScan® Enterprise para proteger seus 200 mil endpoints ao redor do mundo contra malware e spyware, além do McAfee VirusScan for Storage para ampliar a proteção para dispositivos de armazenamento conectados a 18 redes. Além disso, a empresa implementou o McAfee Host Intrusion Prevention for Servers para proteger proativamente cerca de 5600 servidores contra ataques conhecidos e de dia zero novos e o McAfee Vulnerability Manager para detectar imediatamente vulnerabilidades no sistema.

O que diferencia esses produtos, no entanto, é o console de gerenciamento central do software McAfee ePO que acompanha cada um deles e permite que sejam gerenciados em uma única tela em comum. "O software McAfee ePO se destaca em comparação com outras soluções", disse Sacharok, que assistiu um bom número de provas de conceito

> *"O software McAfee ePO se destaca em comparação com outras soluções. É uma aquisição única para nossa proteção de endpoints. Posso ver tudo que preciso de todos* os nossos produtos McAfee em um único painel. Os dashboards fáceis de usar e a funcionalidade integrada tornam tudo – visibilidade, geração de relatórios, implementação, atualização, manutenção, tomada de decisão – muito mais fácil".
>
> —Christopher Sacharok, Engenheiro de Segurança da Informação, Computer Sciences Corporation

de uma grande variedade de produtos de segurança. "É uma compra única para nossa proteção de endpoints. Posso ver tudo que preciso de todos os nossos produtos McAfee em um único painel. Os dashboards fáceis de usar e a funcionalidade integrada tornam tudo – visibilidade, geração de relatórios, implementação, atualização, manutenção, tomada de decisão – muito mais fácil".

Como o software McAfee ePO torna as operações de segurança mais fáceis e mais eficientes

Além de Sacharok, mais sete pessoas em sua equipe e dois administradores de segurança em outras equipes da CSC contam com o software McAfee ePO para obter uma visão centralizada do status da segurança em todos os 200 mil endpoints corporativos e de clientes. Eles também dependem dele para a geração de relatórios – relatórios agendados regularmente para fins de conformidade e consultas imediatas. Sacharok e os outros muitas vezes consultam uma série de relatórios prontos para uso, incluindo principais ameaças por organização interna, 10 principais computadores com detecção de malware e uma listagem de todos os novos incidentes de segurança.

Em média, a empresa enxerga 200 eventos de ameaça únicos a cada 24 horas e 4100 a cada mês. "Em operações diárias, os dashboards intuitivos do McAfee ePO são simplesmente inigualáveis", afirmou Sacharok. "Posso ver instantaneamente se um evento precisa de minha atenção e me aprofundar nos detalhes. O software McAfee ePO me torna mais eficiente e alivia muitas das dores de cabeça".

A equipe de Sacharok também usa o software McAfee ePO para escanear regularmente em busca de vulnerabilidades, enviar atualizações de software de segurança e realizar atividades de resolução de problemas e correção. Quando outras equipes de segurança da informação da CSC – equipe de firewall, equipe de gateway de e-mail etc. – precisam solucionar problemas de proteção de endpoints, eles chamam a equipe de Sacharok. "Quando precisamos escrever uma nova regra de exclusão ou atualizar DATs ou HIPS, por exemplo, ou sempre que um incidente de segurança ocorre na rede, somos capazes de detectar imediatamente onde e o que está acontecendo em tempo real e realizar ações corretivas", disse.

Economia de tempo com ferramentas integradas de alto nível de detalhes

Sacharok também menciona como extremamente útil o recurso dentro do software McAfee ePO que utiliza uma estrutura de sistemas e ordena dinamicamente em um nível muito detalhado. Ele pode ver as informações de status de endpoints por continente, cidade, prédio ou até mesmo andar, então é fácil determinar exatamente onde corrigir se for necessária uma intervenção física. "Você não vê esse nível de detalhes de gerenciamento em muitas outras ferramentas de segurança", observa Sacharok. "Isso definitivamente dá uma vantagem à Intel Security".

As ferramentas de correção integradas ao software McAfee ePO também facilitam a simplificação das operações de segurança. Por exemplo, com o software, Sacharok pode transferir um endpoint diretamente de uma organização para outra e aplicar as políticas desta a ele ou executar uma varredura de antivírus de alta prioridade nele. "Poder realizar muitas ações de correção remotamente pelo software McAfee ePO também alivia a necessidade de ter um técnico local e o subsequente grau de separação entre minha equipe e o usuário final", complementou Sacharok. "Menos tempo presencial economiza significativamente tempo e recursos para as Operações de Segurança".

Suporte robusto e uma estratégia para o futuro

Além da tecnologia da Intel Security, Sacharok e outros na CSC dependem do suporte técnico Platinum da Intel Security. "Estamos muito satisfeitos com o nível de suporte que recebemos", observou Sacharok. "Sempre que temos uma dúvida, consultamos a base de conhecimento do suporte e, nas raras ocasiões em que precisamos falar com alguém, a resposta é sempre muito rápida".

Assim como o software McAfee ePO se destaca na opinião de Sacharok, a Intel Security também se destaca como empresa. “Quando você olha para os fornecedores de segurança, a estratégia está acima de todo o resto”, explica Sacharok. “O fornecedor obviamente precisa ter um produto com boa relação custo/benefício que funcione bem, mas no fim das contas, o fornecedor também precisa ter uma estratégia para tornar nosso ambiente mais seguro que seja melhor do que a da concorrência. A Intel Security tem de longe a visão e a estratégia de segurança mais abrangente dentre todos os fornecedores que já vi”.

Sacharok está se referindo à estratégia da Intel Security de uma arquitetura aberta e interligada, que simplifica o ciclo de vida da defesa contra ameaças para ajudar organizações a solucionar mais ameaças de forma mais rápida e com menos utilização de mão de obra. “No futuro próximo, integrar nossas diferentes soluções umas às outras definitivamente será essencial para nos tornar uma empresa de segurança mais holística”, disse Sacharok. “Eu espero que a Intel Security tenha um papel fundamental nesse processo”.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com