

A reformulação da proteção de endpoint viabiliza a inovação e reforça a postura de segurança

Empresa inovadora e global de transformação de processos empresariais transforma seus próprios processos de segurança com ajuda da McAfee



Sutherland Global Services

Perfil do cliente

Empresa multinacional de transformação de processos empresariais

Setor

Serviços de tecnologia e empresariais

Ambiente de TI

Aproximadamente 50.000 endpoints em 16 países de seis continentes

A Sutherland Global Services ajuda mais de 100 empresas da *Fortune 1000* em 16 países a repensar e a recriar processos empresariais para a era digital utilizando análise de dados e outras tecnologias, expertise em idealização de projetos e conhecimentos específicos de cada setor. A empresa sediada em Pittsford, Nova York, investiu na transformação de sua própria segurança de endpoint, melhorando consideravelmente sua postura geral de segurança e, ao mesmo tempo, economizando tempo e dinheiro. Além disso, ao aproveitar o Open Data Exchange Layer (OpenDXL), a empresa está criando uma defesa unificada na qual vários sistemas de segurança funcionam juntos, apoiando e reforçando uns aos outros.

Conecte-se conosco



ESTUDO DE CASO

Proteção contra violações e interrupção de negócios

“Cada minuto em que um sistema fica indisponível e um usuário corporativo precisa dele constitui um custo muito elevado”, afirma Prashanth M J, chefe global de infraestrutura de tecnologia da Sutherland Global Services. “Violações e interrupção de negócios são um risco significativo contra o qual queremos nos proteger. Estamos trabalhando constantemente para assegurar que todos os controles necessários estejam em vigor para minimizar esses riscos e nos permitir continuar oferecendo soluções e serviços inovadores e personalizados para nossos clientes”.

Com aproximadamente 50.000 nós para proteger, incluindo 1.000 servidores, mais de 80 centros de dados/entrega e uma infraestrutura digital espalhada por 16 países e seis continentes, minimizar os riscos à segurança é uma tarefa gigantesca que exige muitas soluções de segurança. Parte da batalha diária da equipe de infraestrutura de tecnologia é fazer com que todos os diversos sistemas e controles comuniquem-se uns com os outros e compartilhem inteligência sobre segurança para manter seguro todo o ambiente corporativo estendido.

Necessidade: parceiros estratégicos que apoiam a inovação

Para realizar uma proposta tão ambiciosa, a Sutherland Global Services depende da ajuda de parceiros estratégicos como a McAfee. “Desenvolvemos um alto nível de confiança na McAfee porque ela sempre atendeu nossas expectativas corporativas, incluindo a necessidade de inovação constante”, disse Prashanth.

“A inovação é o que mantém nossa empresa viva e prosperando”.

“Nossos serviços inovam na intersecção entre negócios e tecnologia, transformando processos para concretizar as visões de nossos clientes”, prossegue Prashanth. “A McAfee vem consistentemente introduzindo soluções que atendem diretamente nossas exigências corporativas — por exemplo, para nos ajudar a fechar a lacuna entre detecção e correção ou para que avancemos em nossa transformação digital”.

Criação de defesas unificadas aproveitando o OpenDXL

Prashanth também exalta a McAfee pelo desenvolvimento do OpenDXL, uma iniciativa do setor de tecnologia para criar sistemas adaptáveis de soluções interconectadas que se comuniquem e compartilhem informações para viabilizar decisões de segurança precisas e em tempo real. Utilizando OpenDXL, a Sutherland Global Services vem trabalhando atualmente no sentido de integrar sua solução de gerenciamento de eventos e informações de segurança (SIEM), que não é da McAfee, com a proteção de endpoint da McAfee. A integração com o gateway de Web e o firewall da empresa também estão no planejamento de OpenDXL da Sutherland.

“Vejo um enorme potencial no OpenDXL”, observa Prashanth. “Temos vários produtos de segurança de fornecedores diferentes, todos operando isoladamente. Para criar uma defesa unificada contra ataques cibernéticos, é importantíssimo que a inteligência de um sistema possa ser utilizada por outro sistema”.

Desafios

- Oferecer disponibilidade 24 horas por dia, sete dias por semana, a usuários corporativos do mundo inteiro
- Integrar soluções de segurança para uma defesa cibernética unificada
- Cumprir eficientemente com regulamentações, particularmente nos setores de saúde e serviços financeiros

Soluções da McAfee

- McAfee® Advanced Threat Defense
- McAfee® DLP Endpoint
- McAfee® Endpoint Encryption
- McAfee® Endpoint Security
- McAfee® Endpoint Threat Defense and Response
- McAfee® ePolicy Orchestrator®
- McAfee® File Integrity Monitoring
- Serviços profissionais da McAfee®
- McAfee® Threat Intelligence Exchange

ESTUDO DE CASO

A consolidação da proteção de endpoint reduz custos e aumenta o potencial de geração de receita

Para proteger seus endpoints no mundo inteiro, a Sutherland Global Services não prescinde do console de gerenciamento central do McAfee ePolicy Orchestrator (McAfee ePO™). Utilizando o software McAfee ePO, os administradores gerenciam e monitoram diversos produtos da McAfee e funcionalidades de segurança — antivírus, prevenção de perda de dados no host, prevenção de intrusão no host, criptografia de endpoint, monitoramento de integridade de arquivos e muito mais — tudo em um único painel.

“O (software) McAfee ePO nos oferece a vantagem de gerenciar nossa corporação global com perfeição”, afirma Prashanth. “Além disso, ele é tão fácil de usar que não é preciso incorrer no custo de engenheiros de segurança de nível 2 ou 3”.

Nos últimos dois anos, como parte de uma atualização e transformação completa de sua proteção de endpoint, a empresa consolidou sete servidores globalmente dispersos do software McAfee ePO em apenas um. Atualmente, a proteção de todos os aproximadamente 50.000 endpoints é gerenciada por meio de um console central do McAfee ePO dentro do centro de operações de segurança da empresa.

“

Quando retiramos de operação os outros seis servidores do [software] McAfee ePO, começamos imediatamente a economizar”, lembra Prashanth. “Além de reduzir os custos de hardware e software, o consumo de energia do data center e o tempo gasto em manutenção e revisão despencaram. Também acrescentamos novas funcionalidades sem a necessidade de recrutar funcionários e liberamos funcionários para dedicar seu tempo a atividades de maior valor.”

“Além disso, a revisão da proteção de endpoint aumentou a disponibilidade dos sistemas em todo o âmbito corporativo”, acrescenta Prashanth. “O aumento da disponibilidade também aumentou nosso potencial de gerar receita adicional”.

Relatórios de conformidade mais rápidos e mais fáceis elevam os níveis de conformidade para mais de 95%

A consolidação em um único console central proporciona uma imensa economia de tempo na área de conformidade, especialmente nos setores de saúde e serviços financeiros. “Com um único console central, os relatórios de conformidade se tornaram muitas vezes mais eficientes”, afirma Prashanth. “Podemos oferecer, com rapidez e facilidade, dashboards personalizados e contextualizados aos responsáveis pela segurança em diversas geografias, clientes ou setores. Consequentemente, tornou-se muito mais fácil produzir os relatórios exigidos e o nosso nível de conformidade aumentou para mais de 95%”.

Resultados

- Redução da sobrecarga administrativa e dos custos de hardware e software
- Aumento da disponibilidade dos sistemas
- Maior potencial para gerar mais receita
- Gerenciamento mais fácil da proteção de endpoint, liberando administradores no mundo todo
- Defesa multicamada mais forte contra malware, inclusive ameaças de dia zero
- Relatórios de conformidade muito mais eficientes mundialmente
- Níveis de conformidade aumentados para mais de 95%
- Menos tempo entre a detecção e a resposta às ameaças

ESTUDO DE CASO

Proteção multicamada e com compartilhamento de ameaças reforça defesa contra ameaças de dia zero

A migração do McAfee® VirusScan® Enterprise para o McAfee Endpoint Security foi mais um elemento fundamental na reformulação da proteção de endpoint da organização. “Sabíamos que era hora de um antimalware robusto, da próxima geração, com camadas extras de proteção e, felizmente, a McAfee tinha tudo o que precisávamos”, explica Prashanth. “Especificamente, queríamos usar a contenção dinâmica de aplicativos para colocar em quarentena arquivos desconhecidos e a funcionalidade de autoaprendizagem Real Protect para analisar arquivos suspeitos imediatamente”.

A empresa também migrou para o McAfee Endpoint Security para aproveitar o McAfee Threat Intelligence Exchange, que armazena inteligência global e local sobre ameaças, atualizada continuamente, e que a compartilha bidirecionalmente por meio do Data Exchange Layer (DXL) para todos os sistemas conectados via DXL. O McAfee Endpoint Security conecta-se diretamente ao DXL. “Assim, quando um de nossos endpoints encontra um arquivo malicioso ou quando um centro global de pesquisa encontra uma ameaça de dia zero, em vez de ter de esperar que assinaturas sejam disponibilizadas e fornecidas via push por um administrador, todos os nossos endpoints são informados automaticamente”, explica Prashanth.

A Sutherland Global Services recrutou os serviços profissionais da McAfee para ajudar a realizar uma migração suave e em fases para o McAfee Endpoint Security, com impacto zero sobre a disponibilidade dos sistemas para os usuários corporativos em todo o mundo. A migração de todos os endpoints para o McAfee Endpoint Security incluiu o módulo Advanced Threat Protection da solução, o qual contém as tecnologias de contenção dinâmica de aplicativos e Real Protect. A empresa também distribuiu a malha DXL e o McAfee Threat Intelligence Exchange por meio de sua rede.

Aceleração da resposta a incidentes

Como parte de sua transformação da proteção de endpoint, a Sutherland Global Services também implementou um appliance McAfee Advanced Threat Defense para análise dinâmica e estática em área restrita (sandbox). “O McAfee Advanced Threat Defense ajuda-nos de duas maneiras importantes”, observa Prashanth. “Primeiramente, quando nossos endpoints encontram um arquivo desconhecido e o colocam em quarentena, o arquivo é enviado diretamente ao appliance McAfee para uma análise detalhada. Concluída a análise, o resultado é compartilhado por meio do McAfee Threat Intelligence Exchange em toda a corporação. Dessa forma, capturamos um grande número de arquivos maliciosos e protegemos proativamente todos os nossos endpoints”.

“Nossos serviços inovam na intersecção entre negócios e tecnologia, transformando processos para concretizar as visões de nossos clientes. A McAfee vem consistentemente introduzindo soluções que atendem diretamente nossas exigências corporativas — por exemplo, para nos ajudar a fechar a lacuna entre detecção e correção ou para que avancemos em nossa transformação digital”.

— Prashanth M J, vice-presidente sênior e chefe global de infraestrutura de tecnologia da Sutherland Global Services

ESTUDO DE CASO

“Em segundo lugar, o McAfee Advanced Threat Defense acelera nosso processo de investigação de IoC”, prossegue Prashanth. “Antigamente, para cada IoC desconhecido, tínhamos de enviar uma amostra de hash para o suporte da McAfee e esperar que nos dissessem se era maliciosa. Agora, com o McAfee Advanced Threat Defense, podemos analisar o IoC nós mesmos e determinar mais rapidamente as providências adequadas a serem tomadas”.

Além disso, a empresa está no processo de adicionar o McAfee Endpoint Threat Defense and Response para aprimorar sua capacidade de caçar ameaças proativamente. “Queremos ser mais ofensivos, e não apenas defensivos”, afirma Prashanth. “Minha expectativa é que o McAfee Endpoint Threat Defense and Response seja uma das ferramentas mais importantes de nosso arsenal para proteção contra ameaças que podem estar em hibernação no nosso ambiente, apenas esperando um gatilho... Tudo se resume à velocidade de resposta. As ações certas são inúteis quando a resposta não é suficientemente rápida”.

Para estar preparado para o futuro, é preciso mais do que apenas produtos

“Nossa parceria com a McAfee tem sido extremamente frutífera por me dar a confiança de que nossos sistemas estão protegidos e prontos para o futuro”, afirma Doug Gilbert, CIO e diretor digital da Sutherland Global Services. “A escolha de uma parceria não é determinada apenas por um ou mais produtos — ela envolve todo o ecossistema. Com a McAfee, temos pessoas reunidas em torno de nós — não apenas para vender produtos, mas para nos ajudar a projetar, distribuir, manter e otimizá-los.”

Futuramente, conforme a Sutherland Global Services migrar cada vez mais para a nuvem e com sua transformação digital já em andamento, a McAfee continuará desempenhando um papel fundamental. Prashanth cita os novos produtos McAfee® MVISION como mais um exemplo de inovação que certamente ajudará sua empresa: “O cenário de ameaça é tão complicado que você precisa trabalhar em conjunto. A McAfee traz a tecnologia certa para nós. Nós trazemos o conhecimento do domínio de negócios. “Together is Power” é a maneira certa de seguir adiante”.

“Nossa parceria com a McAfee tem sido extremamente frutífera por me dar a confiança de que nossos sistemas estão protegidos. A escolha de uma parceria não é determinada apenas por um ou mais produtos — ela envolve todo o ecossistema. Com a McAfee, temos pessoas reunidas em torno de nós — não apenas para vender produtos, mas para nos ajudar a projetar, distribuir, manter e otimizá-los.”

— Doug Gilbert, CIO e diretor digital da Sutherland Global Services



Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br

McAfee e o logotipo da McAfee, ePolicy Orchestrator e McAfee ePO são marcas comerciais ou marcas registradas da McAfee, LLC ou de suas afiliadas nos EUA e em outros países. Outros nomes e marcas podem ser propriedade de terceiros. Copyright © 2019 McAfee, LLC. 4322_0719
JULHO DE 2019