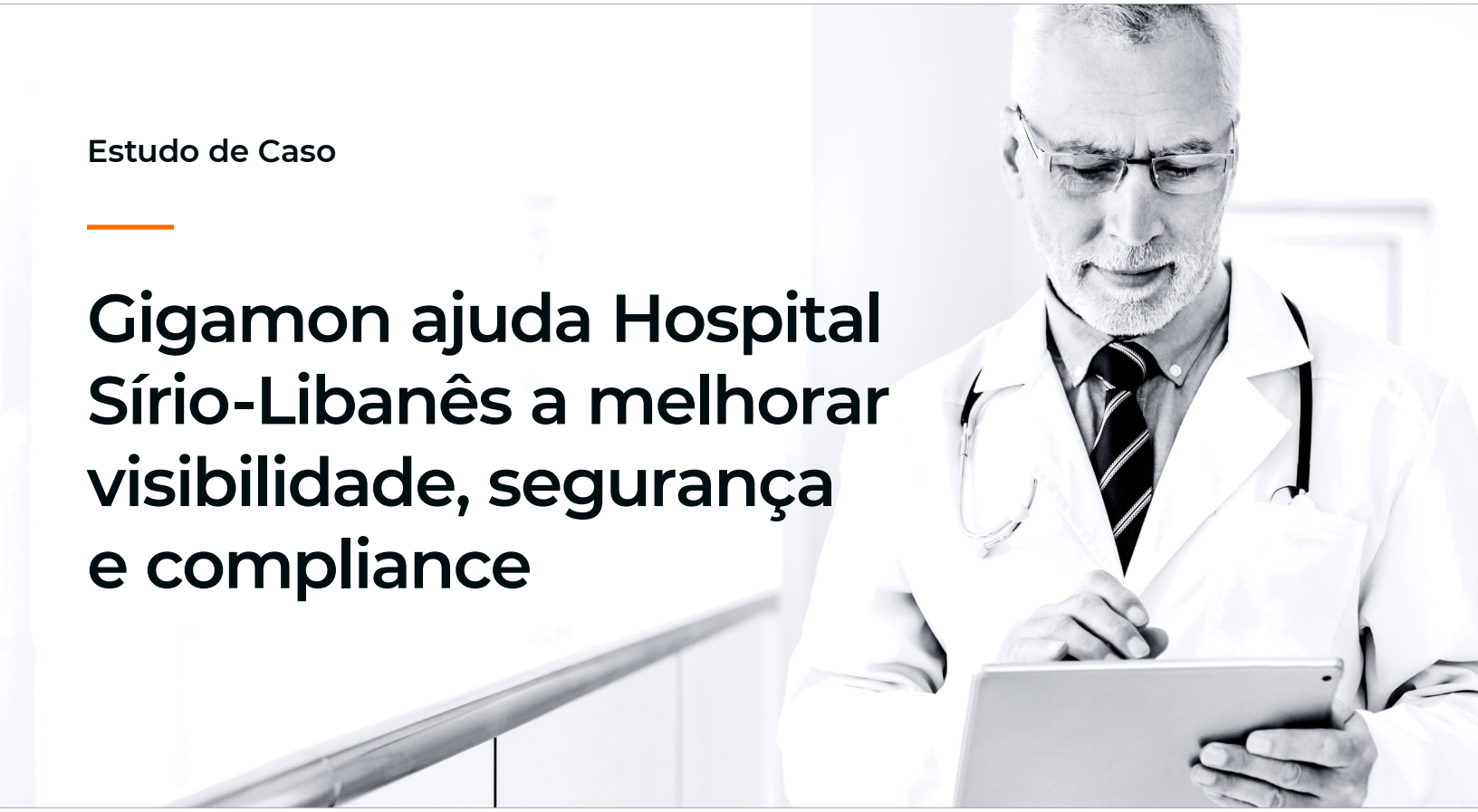
Estudo de Caso

Gigamon ajuda Hospital Sírio-Libanês a melhorar visibilidade, segurança e compliance



Quando buscamos observabilidade profunda, a Gigamon nos oferece visibilidade completa de todas as camadas da nossa infraestrutura, incluindo a nuvem. Podemos monitorar o tráfego da rede de acesso, pacotes, fluxos e assim por diante — todas as informações extraídas dos metadados dos nossos aplicativos.

LEANDRO RIBEIRO
Diretor de Segurança da Informação
do Hospital Sírio-Libanês

Desafios

- Visibilidade abrangente das ameaças de rede
- Segurança na nuvem para aplicativos e infraestrutura
- Segurança da Internet das Coisas (IoT) para dispositivos
- Conformidade com as regulamentações regionais sobre proteção de dados pessoais e de saúde

Benefícios para o cliente

- Compreensão mais profunda do tráfego de rede
- Capacidade aprimorada de identificar ameaças internas
- Redução da necessidade de ferramentas adicionais
- Segurança reforçada para dados confidenciais de pacientes

Solution

- GigaVUE Cloud Suite™
- GigaVUE® HC Series
- GigaVUE TA Series
- GigaVUE-FM fabric manager
- GigaSMART®

Sobre o cliente

O Hospital Sírio-Libanês é um dos principais provedores de saúde do Brasil, com 103 anos de experiência, unidades médicas de última geração, equipes altamente especializadas, investimentos contínuos em ensino e pesquisa, além de iniciativas pioneiras. A instituição, que abriga um dos maiores centros médicos de diagnóstico por imagem do Brasil, está classificada entre os 100 melhores hospitais do mundo e possui 9 unidades em São Paulo e Brasília, empregando cerca de 14 mil funcionários.

O hospital possui um ambiente de TI híbrido, com 70% a 80% de seus aplicativos e infraestrutura hospedados na nuvem, principalmente na Amazon AWS. Leandro Ribeiro, diretor de segurança da informação, é um profissional com mais de 15 anos de experiência em segurança cibernética e 20 anos de atuação na área da saúde. Ele se juntou ao Hospital Sírio-Libanês com o objetivo de aprimorar o programa de segurança cibernética da instituição. Antes de ingressar no hospital, Leandro trabalhou em grandes empresas de saúde, incluindo o UnitedHealth Group. Sua vasta experiência em segurança cibernética no setor de saúde faz dele um recurso valioso para a organização.

Desafio Comercial

Quando Ribeiro ingressou no Hospital Sírio-Libanês, percebeu que a infraestrutura de segurança legada não oferecia a visibilidade e os recursos necessários para que a equipe de segurança detectasse e respondesse de forma eficaz às ameaças cibernéticas, especialmente no ambiente de nuvem.

Como resultado, Ribeiro e sua equipe de 22 profissionais de rede e segurança cibernética enfrentaram três preocupações principais. Primeiro, a equipe de segurança cibernética teve dificuldade em monitorar o tráfego de rede de todas as direções, especialmente o tráfego leste-oeste dentro do data center. Essa visibilidade limitada tornou desafiador identificar e lidar com ameaças paralelas de TI e com possíveis riscos internos de segurança que poderiam surgir dentro da própria rede. Em segundo lugar, o aumento no número de dispositivos IoT, como equipamentos médicos e dispositivos wearables, trouxe novas vulnerabilidades, ampliando a superfície de ataque e colocando em risco tanto a saúde dos pacientes quanto a segurança dos dados pessoais. Esses dispositivos, geralmente com controles de segurança limitados, podem ser explorados por invasores para obter acesso não autorizado à rede do hospital. Por fim, o hospital precisava garantir conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira, que exige medidas rigorosas de segurança cibernética para a proteção dos dados e da privacidade dos pacientes. Deixar de cumprir essas regulamentações pode acarretar multas pesadas e danos à reputação da instituição.

Em suas funções anteriores em outras organizações de saúde, Ribeiro teve uma experiência positiva com o Deep Observability Pipeline e com a equipe que o apoiou. “Trabalhei em estreita colaboração com a equipe da Gigamon no Brasil, que foi proativa na resolução de problemas de visibilidade específicos do nosso ambiente. Minhas equipes nem sempre estavam familiarizadas com as ferramentas, então o suporte que recebemos da Gigamon foi inestimável para que todos se atualizassem rapidamente”, afirmou ele. “Eu soube imediatamente que a Gigamon era a melhor solução para o Hospital Sírio-Libanês”.

Solução

Os desafios de negócios enfrentados pelo Hospital Sírio-Libanês foram resolvidos por meio de uma compreensão mais profunda da atividade de rede, o que permitiu identificar e abordar potenciais riscos de segurança de maneira mais eficaz.

O hospital implementou uma solução abrangente de segurança cibernética com a Gigamon, ExtraHop e Claroty Medigate, dois parceiros de segurança cibernética da Gigamon. A Gigamon oferece uma visão unificada dos dados em movimento por toda a rede, permitindo que o hospital monitore o tráfego em todas as direções (Norte-Sul e lateral Leste-Oeste). A ExtraHop, uma solução de Detecção e Resposta em Rede (NDR), complementa a Gigamon ao oferecer recursos avançados de detecção e análise de ameaças. “A solução integrada torna mais fácil para nós descobrir ameaças internas e comportamento anômalo de endpoints e servidores”, observou Ribeiro.

Especificamente, o Deep Observability Pipeline oferece um conjunto completo de ferramentas de segurança e desempenho, eliminando pontos cegos e proporcionando visibilidade completa de toda a infraestrutura. A ExtraHop recebe pacotes brutos fornecidos pela Gigamon de toda a infraestrutura, extrai metadados dos pacotes utilizando aprendizado de máquina e analisa a inteligência com mais de 1 milhão de modelos preditivos diferentes, proporcionando uma compreensão detalhada da atividade de rede do hospital. Os algoritmos de aprendizado de máquina da ExtraHop analisam o tráfego de rede para identificar atividades suspeitas e técnicas de movimentação lateral, que podem indicar a presença de ameaças nos estágios iniciais, como malware, ransomware e ameaças internas, para ajudar a mitigar riscos e evitar violações de segurança.

A solução também permite que o hospital descubra, monitore e gerencie de forma eficaz dispositivos de IoT, identificando vulnerabilidades e impedindo acessos não autorizados a esses ativos críticos — sem a necessidade de investir em hardware caro que exija muita manutenção. “Foi aqui que a Gigamon nos ajudou a economizar. Até então, não sabíamos realmente quantos dispositivos tínhamos em nossa rede. Agora que temos visibilidade total de todos os nossos dispositivos, podemos implementar a segmentação de rede para protegê-los melhor”, afirmou Ribeiro.

Graças à combinação da Gigamon e ExtraHop, o hospital consegue demonstrar conformidade regulatória, fornecendo evidências claras de medidas robustas de segurança cibernética. Isso resulta, em última análise, em uma melhoria significativa na segurança dos pacientes e na proteção dos dados confidenciais.

Benefício

A implementação da Gigamon trouxe vantagens significativas para o Hospital Sírio-Libanês. Com uma compreensão abrangente do tráfego de rede, Ribeiro consegue identificar e abordar possíveis riscos de segurança de maneira mais rápida e eficaz, tanto no ambiente local quanto na AWS.

Quando buscamos observabilidade profunda, a Gigamon nos oferece visibilidade completa de todas as camadas da nossa infraestrutura. Podemos monitorar o tráfego da rede de acesso, pacotes, fluxos e assim por diante — todas as informações extraídas dos metadados dos nossos aplicativos”, declarou Ribeiro.

A solução combinada permite que o hospital detecte e responda a ameaças mais rapidamente, reduzindo a frequência e o impacto de incidentes de segurança. Além disso, o hospital consegue proteger seus dispositivos de IoT, impedindo acesso não autorizado e reduzindo o risco de violações de dados. Consolidando várias ferramentas de segurança em uma única plataforma, o hospital também obtém economias de custos significativas. Por exemplo, a Gigamon potencializa a eficácia da detecção de ameaças da Claroty Medigate, uma plataforma SaaS voltada para a saúde, que protege tecnologias e dispositivos médicos conectados, como bombas intravenosas e ultrassons.

A integração da Gigamon com a Claroty expande significativamente a visibilidade do tráfego de rede que atravessa dispositivos médicos XIoT/OT no hospital, permitindo uma detecção e resposta a ameaças mais rápidas e precisas.

Por fim, a solução ajuda a atender aos requisitos de conformidade ao fortalecer a postura de segurança cibernética. Com essa proteção robusta, o hospital consegue garantir a segurança dos dados confidenciais dos pacientes e assegurar a continuidade dos serviços essenciais, o que, por sua vez, melhora tanto a segurança dos pacientes quanto a eficiência operacional geral.

“No ambiente de saúde, oferecer o melhor atendimento possível aos nossos pacientes é essencial, então tudo o que fazemos é crítico. Graças à visibilidade expandida e profunda proporcionada pela Gigamon, agora estamos vários passos à frente quando um incidente ocorre. Logo que identificamos uma ameaça, podemos detê-la imediatamente e garantir que ela não impacte as operações hospitalares nem a saúde e segurança dos nossos pacientes”, destacou Ribeiro.

Em um futuro próximo, ele e sua equipe planejam explorar ainda mais os recursos da Gigamon, incluindo integração com SIEM, descriptografia TLS/SSL para todo o tráfego e a tecnologia Gigamon Precryption™ para eliminar pontos cegos no tráfego de nuvem Leste-Oeste.

About Gigamon

A Gigamon® oferece uma abordagem de observabilidade profunda, que fornece inteligência de rede de forma eficiente para ferramentas de nuvem, segurança e observabilidade. Isso ajuda a eliminar pontos cegos de segurança e reduzir os custos com ferramentas, permitindo uma proteção e gestão mais eficaz da infraestrutura de nuvem híbrida. A Gigamon atende a mais de 4 mil clientes em todo o mundo, incluindo mais de 80% das empresas da Fortune 100, nove dos dez maiores provedores de redes móveis, além de centenas de agencias governamentais e instituições educacionais. Para saber mais, visite gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

01.25_01