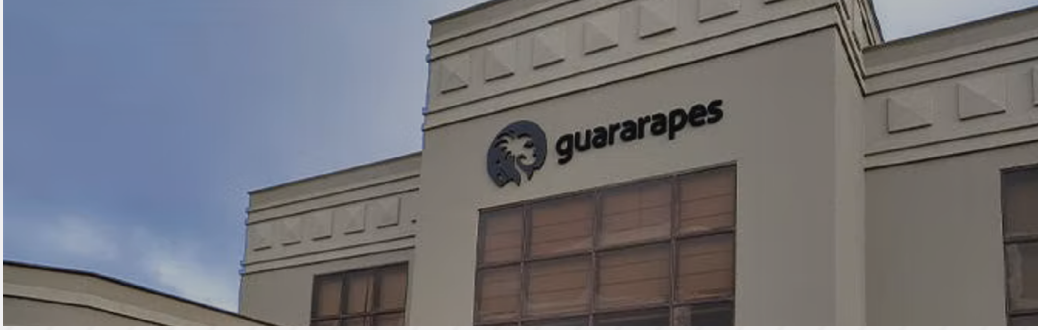
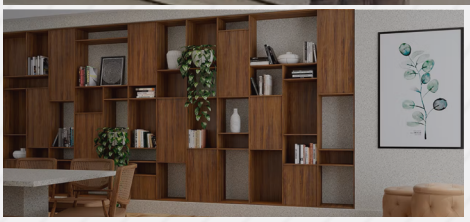
voices

CrowdStrike Customer Case Study





guararapes

Varejista brasileiro protege dados financeiros de 30 milhões de clientes com as soluções CrowdStrike

Quando o Grupo Guararapes, potência brasileira da moda, decidiu criar o banco Midway para oferecer serviços de financiamento a seus clientes, deu início à jornada da empresa para construir uma infraestrutura de segurança cibernética robusta e de classe financeira para todo o negócio. Tradicionalmente, a vertical de varejo fica atrás de outros setores no que diz respeito à segurança cibernética. Essa parte do grupo não tinha o nível de segurança que os setores financeiros tinham.

"É assim", disse Rodrigo Godoi, CISO do Grupo Guararapes. "Imagine que você tem uma casa simples. Então você faz uma reforma e a transforma em uma bela casa com piscina, carros de luxo e coisas do tipo, o que atrai os bandidos. Agora você precisa de uma parede e uma cerca elétrica, mas sem alarme você pode ter problemas. Quando montamos nosso banco, estávamos cientes de que um banco depende da confiança do cliente. Se a confiança for perdida por segurança inadequada, acabou."

O Guararapes é o maior grupo de moda do Brasil com uma operação de varejo nacional composta por mais de 360 lojas, incluindo a rede Lojas Riachuelo. A marca colabora com designers brasileiros e internacionais, além de celebridades da moda e nomes de luxo, como Daslu, Versace e Karl Lagerfeld. Os 40 mil funcionários do grupo participam de quase todo o ciclo de moda, da produção de insumos à venda de produtos. A empresa se descreve como "envolvida desde o fio até a última parcela".

O antivírus legado não conseguia proteger o novo banco digital

Os executivos da empresa perceberam que o grupo estava lidando cada vez mais com o dinheiro de seus clientes, oferecendo a eles serviços financeiros como cartões de loja, seguros e empréstimos. Decidiram então criar o Midway, um banco totalmente digital que daria suporte aos consumidores. Godoi foi contratado para implementar a segurança cibernética não apenas para o banco, mas para todos os negócios da Guararapes e seus 30 milhões de clientes. Ele formou um novo grupo de segurança com a missão de fortalecer suas defesas e elevar a empresa aos padrões de segurança cibernética financeira. Essa definição aconteceu em meio à estratégia de transformação digital de todo o grupo, mudança de serviços e aplicativos para a nuvem, melhoria do comércio eletrônico e desenvolvimento de um mercado digital. Havia também novas regulamentações de dados, como a Lei Geral de Proteção de Dados (LGPD), que precisava ser respeitada.

O grupo tinha uma solução antivírus tradicional, mas seu gerenciamento era difícil e demorado. O programa precisava ser instalado fisicamente em 10 mil dispositivos e reinstalado toda vez que uma máquina era substituída. Uma vez instalado, o aplicativo ainda desacelerava o endpoint, especialmente os computadores mais antigos, o que afetava a produtividade do usuário. "Tínhamos uma ferramenta obsoleta, trabalhosa, difícil de ser gerenciada pela equipe, o que causava baixo desempenho e desconforto aos usuários finais", disse Godoi.

INDUSTRY
Varejo

LOCATION/HQ
Natal, Brazil

DESAFIOS
- Lançamento de serviços bancários que exigem segurança de classe financeira
- Proteção de dados financeiros e de outros tipos para 30 milhões de clientes
- Baixo desempenho de antivírus legado e desatualizado que drenava recursos

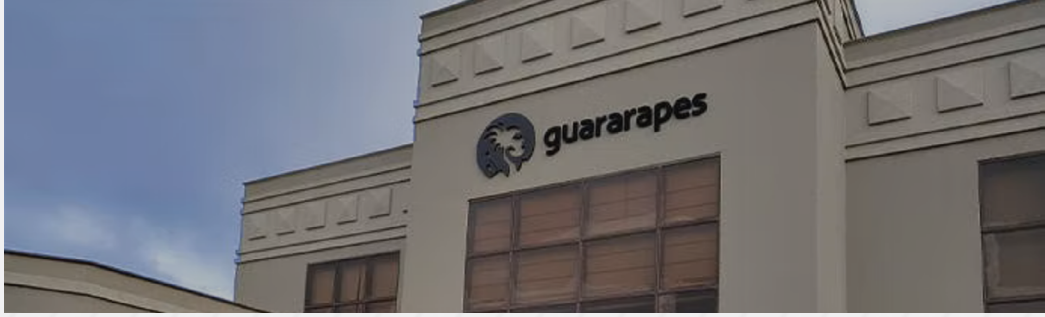
SOLUÇÃO
Quando o Grupo Guararapes criou um banco para oferecer serviços financeiros aos seus 30 milhões de clientes de varejo, utilizou a CrowdStrike para melhorar a segurança de endpoints do banco e do restante do grupo.

"A CrowdStrike realmente se destacou contra outras soluções. Escalamos a solução rapidamente e, em apenas três meses, tínhamos toda a operação instalada e funcionando, identificando incidentes no ambiente e criando regras específicas."

Rodrigo Godoi
CISO
Grupo Guararapes

voices

CrowdStrike Customer Case Study



CrowdStrike implantado em 10 mil endpoints após piloto estendido

Como usuário experiente da CrowdStrike, Godoi queria fazer das soluções um dos principais pilares da nova infraestrutura de segurança da empresa. Mas primeiro era importante entender se as soluções faziam sentido para as operações mistas do grupo, entre varejo, manufatura e finanças. O primeiro passo foi avaliar vários produtos do mercado para ver se poderiam suportar 10 mil terminais. Depois de três dias, o Guararapes já trabalhava com a CrowdStrike para montar o piloto de uma prova de conceito. "Foi quando vimos a simplicidade, a facilidade de operação e a funcionalidade da CrowdStrike", ele disse.

O piloto deveria durar 15 dias, mas teve tanto sucesso que durou 60 dias e se tornou parte do projeto final. "A CrowdStrike realmente se destacou contra outras soluções", disse Godoi. "Escalamos a solução rapidamente e, em apenas três meses, tínhamos toda a operação instalada e funcionando, identificando incidentes no ambiente e criando regras específicas."

O grupo Guararapes agora usa a CrowdStrike para proteger 10 mil terminais em toda a sua operação comercial, de dispositivos dos pontos de venda a computadores das fábricas. Godoi criou um centro de operações de segurança (SOC) com operação 24 horas por dia, 7 dias por semana, integrado ao CrowdStrike Falcon® Complete, serviço gerenciado de detecção e resposta da CrowdStrike.

Em parceria com a CrowdStrike, a empresa está usando a solução para desenvolver casos de uso (por exemplo, se um incidente ocorre e há um alerta) apoiados por um manual de ação para lidar com incidentes semelhantes no futuro. Se uma máquina apresenta sinais de comportamento anormal, ela gera um alerta no SOC para que possa ser isolada da rede sem causar nenhum dano. "Isso nos ajudou muito", disse Godoi. "E é um grande ganho em nosso processo de resposta a incidentes."

Equipe de segurança livre do enorme peso do trabalho de suporte

A CrowdStrike aliviou a equipe de segurança de uma enorme carga de manutenção e suporte. "Com a CrowdStrike, não preciso mais de uma equipe focada em segurança de endpoints, em examinar a integridade dos servidores e sistemas para ver se estão funcionando, porque é isso que a CrowdStrike faz", disse Godoi. "Essas responsabilidades não são mais um fardo para o meu time."

Ao contrário da solução antivírus anterior, a CrowdStrike teve pouco ou nenhum impacto no desempenho dos endpoints. A integração com outros sistemas de negócios, como o DevOps, também foi fácil. "Quando você tem uma solução antivírus tradicional, ela torna os servidores e aplicativos mais lentos", disse Godoi. "Às vezes, um antivírus está configurado incorretamente ou tem uma distribuição de assinatura de tempo inadequada que causa problemas. Com a CrowdStrike, não tivemos nada disso."

Um dos principais desafios anteriores à CrowdStrike era a visibilidade do que estava acontecendo no ambiente do grupo Guararapes.

"Minha maior dificuldade era ter visibilidade dos ataques em tempo real", disse Godoi. "E como a CrowdStrike não precisa de atualização constante, consegue detectar novos malwares e vírus automaticamente. Antes, essas ameaças poderiam ficar quietas em uma máquina só esperando para atacar. Maior visibilidade significa que podemos responder mais rapidamente a essas tentativas e incidentes maliciosos."

RESULTADOS

Elevou a postura de segurança para uma proteção de classe financeira

Implantou a solução de forma rápida, simples e sem falhas

Construiu uma parceria forte, colaborativa e baseada em confiança

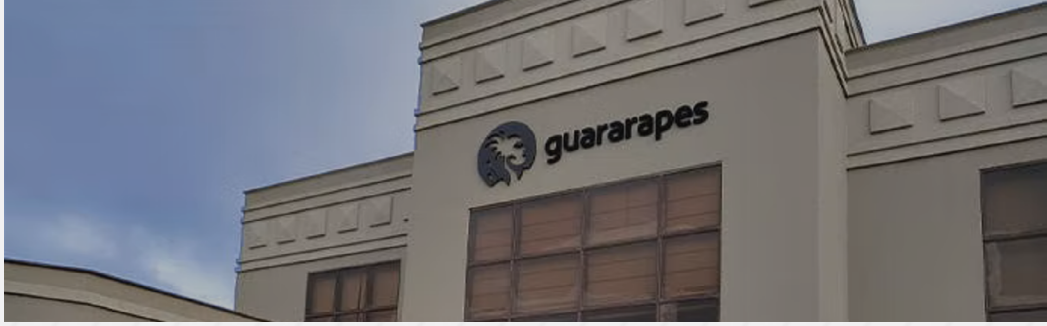
ENDPOINTS

CROWDSTRIKE PRODUCTS

- Falcon® Complete managed detection and response
- Falcon® Discover security hygiene
- Falcon® Intelligence
- Falcon OverWatch™ managed threat hunting
- Falcon® Insight XDR endpoint detection and response
- Falcon® Prevent next-generation antivirus
- Falcon® Spotlight vulnerability management

voices

CrowdStrike Customer Case Study



A análise inteligente de ameaças melhora a produtividade

O Guararapes utiliza a CrowdStrike para análise inteligente de ameaças, identificando novos incidentes e cenários, documentando e desenvolvendo ações corretivas. Godoi acrescentou que a CrowdStrike possui painéis para monitorar e visualizar a atividade por meio de um mapa de calor em tempo real. A solução ainda ajuda sua equipe a monitorar se um dispositivo está executando os aplicativos corretos. Antes, isso levaria meses até ser resolvido.

Essas melhorias na visibilidade, monitoramento em tempo real e automação, além da arquitetura nativa em nuvem da solução CrowdStrike, melhoraram significativamente a produtividade. “Um dos maiores benefícios da CrowdStrike foi o tempo que tive para executar o projeto”, disse Godoi. “Foi tudo muito rápido porque não precisávamos ir máquina a máquina ou usar a equipe de infraestrutura em projetos longos e demorados que levariam um ano até mostrar resultados.” Para a equipe técnica, a CrowdStrike melhorou a produtividade em 70%, permitindo que a equipe gaste tempo em funções e serviços mais valiosos.

Parceria com CrowdStrike: chave para o sucesso

A parceria que a Guararapes estabeleceu com a CrowdStrike foi fundamental para o sucesso da solução. “Temos uma parceria real com a CrowdStrike, não uma relação entre cliente e fornecedor”, disse Godoi. “Seja lá o que precisamos, a CrowdStrike nos atende. Quando vários concorrentes sofreram ataques, a CrowdStrike trabalhou conosco e compartilhou conhecimento para identificar o que aconteceu, se aqueles incidentes poderiam nos impactare como poderíamos nos proteger. Esse tem sido um ótimo aspecto do relacionamento com a CrowdStrike, que continua a crescer.”

SOBRE A CROWDSTRIKE

A CrowdStrike Holdings, Inc. (Nasdaq: CRWD), líder global em segurança cibernética, redefiniu a segurança moderna com a plataforma nativa em nuvem mais avançada do mundo para proteger áreas críticas de risco empresarial – endpoints e cargas de trabalho, identidade e dados na nuvem. Alimentada pela CrowdStrike Security Cloud e IA de classe mundial, a plataforma CrowdStrike Falcon® utiliza indicadores de ataque em tempo real, inteligência de ameaças, entendimento de ameaças adversárias e telemetria enriquecida de toda a empresa para fornecer detecções precisas, proteção e remediação automatizadas, caça a ameaças e observabilidade priorizada de vulnerabilidades.

CrowdStrike: **We stop breaches.**