DELL Technologies

# Melhorando as medidas protetivas de segurança sem aumentar o custo do quadro de funcionários

Para fortalecer significativamente sua segurança cibernética, um grande condado do sudoeste dos EUA recorreu ao Dell Managed Detection and Response.

Perfil do cliente

**Condado dos Estados Unidos**

Governo municipal e estadual | Estados Unidos

“Sabíamos que precisávamos melhorar nossa postura de segurança. O Dell Managed Detection and Response resolveu o problema sem aumentar o quadro de funcionários.”

**Diretor de sistemas de informação**
Grande condado do sudoeste dos EUA

## Necessidades dos negócios

Com a rápida ascensão do ransomware e de outras ameaças cibernéticas contra governos municipais e estaduais, um grande condado em expansão, localizado no sudoeste dos EUA, buscava fortalecer sua postura de segurança e aprimorar sua capacidade de detectar e responder a ameaças sem o custo e o esforço envolvidos na contratação e no treinamento de mais especialistas em segurança.

## Resumo geral das soluções

- Managed Detection and Response

## Resultados de negócios

- Melhora a postura de segurança do condado sem aumentar o quadro de funcionários.
- Complementa o conhecimento, as habilidades e a capacidade de ampliação da equipe de TI.
- Não sobrecarrega a equipe com o monitoramento e resposta a ameaças 24x7.
- Otimização da detecção e correção rápida em caso de violação do servidor.
- Oferece especialistas experientes com os quais o estado pode contar.

Um grande condado em rápida expansão, localizado no sudoeste dos Estados Unidos, atende a centenas de milhares de residentes e é conhecido por sua base diversificada de empresas, que variam de vibrantes empresas médicas, de biotecnologia e de produção a operações agrícolas e agropecuárias essenciais.

Nos últimos anos, as ameaças à segurança cibernética contra governos municipais e estaduais aumentaram drasticamente. Em 2020, nos EUA, 79 ataques de ransomware (que resultaram em quase US$ 19 bilhões em tempo de inatividade e custos de recuperação) foram iniciados contra entidades governamentais de todos os níveis no país.[1]

Após uma experiência decepcionante com a oferta de outro fornecedor, o condado do sudoeste dos EUA escolheu o Dell Managed Detection and Response, com a tecnologia do software de lógica analítica de segurança Secureworks® Taegis™ XDR. A solução é um serviço gerenciado e abrangente, que monitora, detecta, investiga e responde a ameaças em todo o ambiente de TI do condado 24x7.

"Sabíamos que precisávamos melhorar nossa postura de segurança", diz o diretor de sistemas de informações do condado. "O Dell Managed Detection and Response resolveu o problema sem aumentar o quadro de funcionários."

## Combinando dois recursos principais

A solução reúne os dois componentes mais essenciais a uma postura de segurança formidável:

- O conhecimento especializado dos analistas de segurança da Dell Technologies para complementar a equipe enxuta do condado, que consiste em um único analista de segurança, além de um administrador e engenheiro de sistemas
- Os recursos abrangentes do Secureworks Taegis XDR , uma plataforma de lógica analítica de segurança nativa da nuvem projetada para detectar as ameaças mais avançadas, permitindo que os analistas de MDR otimizem e colaborem com o condado nas investigações e, por fim, os ajudem a tomar as medidas certas para reduzir quaisquer impactos

"Quando solicitamos a ajuda de especialistas da Dell Technologies, eles praticamente ficaram em contato por uma semana ou dez dias e sabíamos que estávamos em boas mãos."

**Diretor de sistemas de informação**
Grande condado do sudoeste dos EUA

[1] Bischoff, Paul, "Ransomware attacks on US government organizations cost $18.9bn in 2020," Comparitech, 17 de março de 2021. https://www.comparitech.com/blog/information-security/government-ransomware-attacks/

“Eles nos ajudaram a instalar agentes de software em todos os servidores e workstations, com acionadores selecionados para interromper serviços ou desligar uma máquina ou conta e nos notificar caso uma ameaça seja detectada”, explica o diretor de sistemas de informações. “Os especialistas da Dell Technologies nos forneceram conselhos valiosos e priorizaram as etapas que precisávamos executar nos 90 dias em que implementamos tudo.”

## Mitigando rapidamente uma tentativa de violação

A solução também inclui até 40 horas trimestrais de orientação detalhada por escrito para responder e corrigir ameaças até mesmo nas situações mais complexas, além de mais 40 horas anuais para investigar atividades e iniciar a recuperação de incidentes de segurança graves, se necessário.

“Nós finalmente nos rendemos à solução quando experimentamos uma tentativa de violação real”, relembra o diretor de sistemas de informações do condado. “Um grupo de hackers detectou um exploit no servidor de e-mail do Microsoft Exchange. Após sermos notificados pela Microsoft e pela agência de segurança cibernética do nosso estado, descobrimos que um de nossos três servidores estava comprometido. A equipe da Dell Technologies foi muito minuciosa ao investigar a violação e nos ajudar a restaurar nosso servidor.”

Ele continua: “Minha recomendação para qualquer CIO do condado seria usar uma solução de segurança de classe empresarial, como Dell Managed Detection and Response, em vez da oferta de um fornecedor de software de proteção contra vírus. Quando solicitamos a ajuda de especialistas da Dell Technologies, eles praticamente ficaram em contato por uma semana ou dez dias e sabíamos que estávamos em boas mãos. Trabalhamos de maneira mais inteligente juntos, e houve muita sinergia entre nossas equipes.”