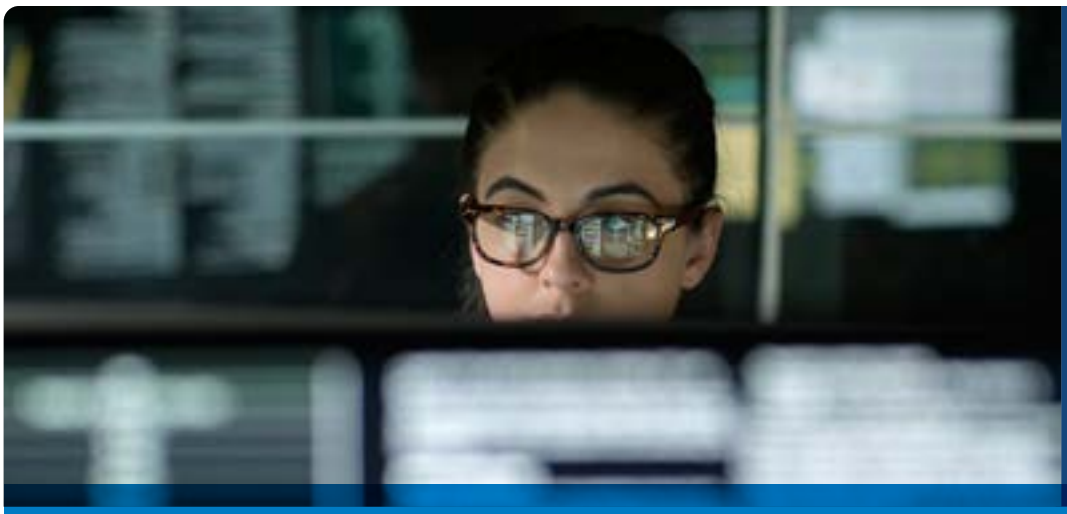
Impeça e responda a ameaças em todo o ambiente de TI



Identifique vulnerabilidades e priorize a resolução imediata

Managed Detection and Response Pro

Combinando gerenciamento de vulnerabilidades, detecção e resposta gerenciadas em uma única solução para ajudar a proteger seu ambiente de TI

O custo médio de uma violação de dados em 2022 foi de US$ 4,35 milhões. [1] Na verdade, quase 22.000 novas vulnerabilidades foram publicadas em 2021, e esse número continua aumentando. [2] As organizações devem encontrar uma forma de proteger seu ambiente contra o volume crescente de ameaças à segurança e as implicações associadas a uma violação.

Proteger seu ambiente de TI exige lidar com vulnerabilidades, investigar ameaças e responder com eficiência. As organizações também enfrentam o desafio de encontrar e reter profissionais qualificados de segurança, e as organizações de TI são consumidas com demandas críticas e operações diárias de negócios.

É por isso que criamos o Managed Detection and Response Pro. O MDR Pro é uma solução totalmente gerenciada que oferece identificação e priorização de vulnerabilidades, bem como detecção e resposta a ameaças 24x7. Nossos especialistas trabalham com sua equipe de segurança interna para proteger seu ambiente de TI, melhorar constantemente sua postura de segurança e ajudá-lo a estar sempre preparado.

Identificar e priorizar vulnerabilidades em toda a superfície de ataque

Os especialistas da Dell usam tecnologia líder para examinar seu ambiente de TI em intervalos periódicos, fornecendo uma visão completa das vulnerabilidades em seus endpoints, sua infraestrutura de rede e ativos de nuvem. Os especialistas da Dell aplicam o aprendizado de máquina para identificar vulnerabilidades que estão sendo exploradas ativamente de modo livre e são mais propensas a serem alvo em um futuro próximo. Isso ajuda você a priorizar os esforços de aplicação de patches em suas vulnerabilidades de mais alto risco e ativos críticos.

Principais benefícios:

- Manter as defesas em dia com gerenciamento e análises de vulnerabilidades recorrentes
- Dar uma visão completa de suas vulnerabilidades nos endpoints, na infraestrutura de rede e na nuvem
- Priorizar vulnerabilidades críticas a serem corrigidas antes de serem exploradas
- Unificar detecção e resposta em todo o ecossistema
- Detectar novos tipos de ataque com um banco de dados de ameaças continuamente atualizado
- Correlacionar eventos e rastrear a atividade completa do invasor
- Aproveitar a experiência e o conhecimento especializado da equipe de segurança da Dell

Detectar e responder aos invasores antes que ocorram danos

O Managed Detection and Response é um serviço totalmente gerenciado, completo e 24x7 que monitora, detecta, investiga e responde a ameaças em todo o ambiente de TI. Organizações com 50 endpoints ou mais podem melhorar de forma rápida e significativa sua postura de segurança e, ao mesmo tempo, reduzir a carga sobre a TI.

O serviço utiliza dois recursos principais:

- O conhecimento especializado dos analistas de segurança da Dell Technologies, obtido ao longo de anos de experiência ajudando organizações de todo o mundo a aumentar a proteção dos negócios
- O software de lógica analítica de segurança XDR, que se baseia em mais de 20 know-how em SecOps, pesquisa e inteligência de ameaças reais, além de experiência para detectar e responder a ameaças avançadas

Principais recursos

Detecção e investigação de ameaças

- A Dell trabalha em parceria com você para compreender seu ambiente e ajudar a implementar o agente de software nos endpoints aplicáveis, sem nenhuma taxa adicional
- Utilização de dados sobre invasores coletados de mais de 1.400 interações de resposta a incidentes no ano passado
- instruções passo a passo para conter a ameaça, mesmo em situações complexas
- Até 40 horas de orientação para remediação remota incluídas por trimestre
- Até 40 horas de resposta remota a incidentes anualmente permitem que as atividades de investigação comecem rapidamente

Identificação e priorização de vulnerabilidades

- Análises mensais de vulnerabilidades, com verificações adicionais conforme determinado entre a equipe da Dell e o cliente
- Inventário de ativos que é comparado com bancos de dados de vulnerabilidades conhecidas em busca de pontos fracos e atualizações necessárias
- Feedback para o cliente sobre a priorização de vulnerabilidades de maior risco a serem resolvidas e orientações para a aplicação de patches
- Análises realizadas por meio de uma plataforma avançada baseada em ML
- Análises trimestrais para informar o cliente sobre as tendências de vulnerabilidade em seu ambiente e no setor

Proteja seu ambiente ainda hoje com a Dell

À medida que a frequência e o custo das violações continuam aumentando, o Managed Detection and Response Pro ajudará a proteger seu ambiente de TI e a proteger seus ativos mais críticos contra agentes mal-intencionados, tudo isso enquanto melhora a postura de segurança de sua organização.

Entre em contato hoje mesmo com um representante de vendas.

[1] IBM. (2022). Relatório do Custo de uma Violação de Dados, 2022. Retirado em 20 de setembro de 2022, de https://www.ibm.com/downloads/cas/3R8N1DZJ

[2] Tenable (2021) Tenable's 2021 Threat Landscape Retrospective. Retirado em agosto de 2022, de https://www.tenable.com/cyber-exposure/2021-threat-landscape-retrospective