DELL Technologies

WHITE PAPER

DELL MANAGED DETECTION AND RESPONSE

A solução completa de segurança gerenciada para organizações de médio e pequeno porte.

SUMÁRIO EXECUTIVO

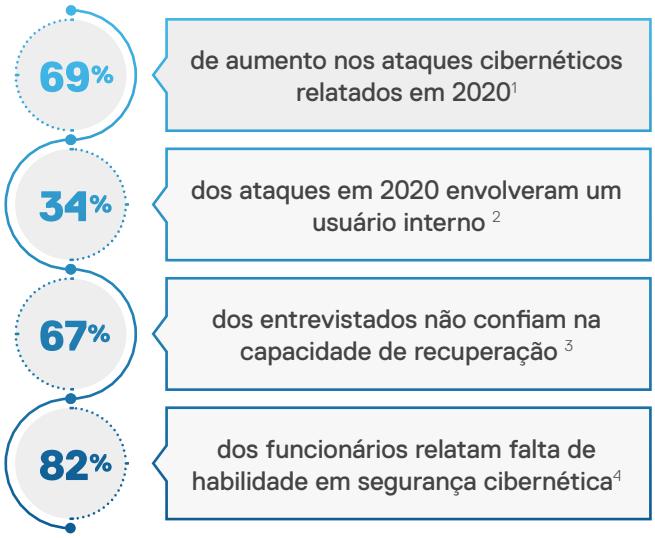
Os ataques cibernéticos às empresas estão em ascensão. Os relatórios do Centro de reclamações sobre crimes na Internet do FBI observaram em 2021 um aumento de 69% em relação ao ano passado e um total de US$ 4,2 bilhões em perdas.[1] Os ataques contra grandes corporações são títulos de primeira página, mas, na realidade, empresas de todos os portes estão vulneráveis. As pequenas empresas, que não têm os amplos recursos de grandes corporações, estão particularmente em risco.

A segurança cibernética é essencial para proteger os ativos de dados, as operações e a continuidade dos negócios. Muitas vezes, grandes corporações têm equipes de segurança dedicadas com a tecnologia, os métodos e a inteligência mais recentes. No entanto, empresas de médio e pequeno porte só podem ter um ou dois especialistas em segurança que precisam gerenciar e conduzir arrays cada vez mais complexos de equipamentos de segurança e ferramentas de software.

Um desafio crescente à TI

A carga de ataques em endpoints, servidores, aplicativos, redes e nuvem gera imensos volumes de alerta que sobrecarregam rapidamente as equipes de TI e de segurança. Ao mesmo tempo, os agentes de ameaça continuam a desenvolver técnicas, eliminando com agilidade a defesa eficaz de ontem. Proteger adequadamente os ambientes de TI na década de 2020 exige monitoramento e resposta 24x7 de 365 dias por especialistas dedicados.

Os ataques cibernéticos representam uma ameaça maior do que nunca



Se os líderes de TI das empresas de médio e pequeno porte alocarem funcionários de TI e orçamento suficientes para a segurança cibernética, áreas importantes, como o desenvolvimento de aplicativos e as DevOps, serão afetadas. O fato é que a proteção contra os atuais agentes de ameaças exige um investimento em talentos, ferramentas e operações com o qual muitas organizações simplesmente não podem arcar.

O Managed Detection and Response oferece respostas

Consequentemente, mais empresas estão considerando as soluções MDR (Managed Detection and Response) de provedores de serviços externos. Como os responsáveis pelas decisões de TI identificam um parceiro MDR excepcional?

Um Solution Provider de MDR viável deve implementar uma tecnologia que detecte tipos de ameaça conhecidos, minimize falsos positivos, correlacione eventos, rastreie a sequência de atividades de um invasor e automatize ações de contenção e prevenção. O provedor exige uma equipe de profissionais de segurança altamente qualificados e experientes para analisar alertas e corrigir ameaças 24x7x365, bem como procurar novos tipos de ameaça.

Maiores motivos para as empresas usarem soluções MDR (Managed Detection and Response)

- **Acesso a especialistas em segurança cibernética difíceis de encontrar**
- **Monitoramento, detecção e cobertura de resposta abrangentes**
- **Redução da carga sobre a equipe de TI, permitindo o foco nas DevOps**

Oferecendo chamadas de serviços de MDR para criar operações de segurança, estabelecer e refinar processos. Além disso, os analistas precisam de ferramentas de compartilhamento de conhecimento e treinamento regular para se manterem atualizados sobre as ameaças e técnicas mais recentes.

Embora muitos provedores de serviços anunciem serviços MDR, apenas alguns têm a capacidade e os recursos necessários para oferecer excelência.

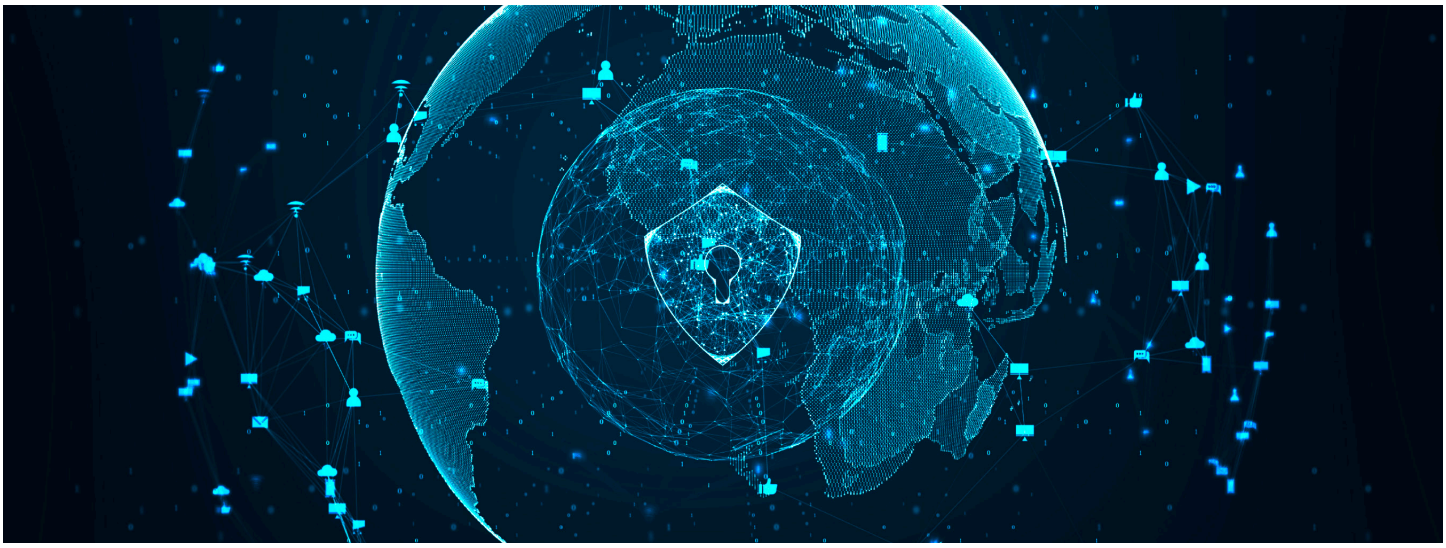
O Dell Managed Detection and Response é uma solução 24x7 completa e totalmente gerenciada que monitora, detecta, investiga e responde a ameaças em todo o ambiente de TI de uma organização. Não importa se uma empresa consiste em 50 endpoints ou milhares, o Dell MDR aprimora de modo rápido e significativo a postura de segurança da empresa e, ao mesmo tempo, diminui a carga sobre a equipe de TI. O Dell MDR aproveita a capacidade da Dell de investir em pessoas, processos e ferramentas para oferecer às empresas de médio e pequeno porte monitoramento e resposta de segurança cibernética em escala empresarial.

ATUAL AMBIENTE DE AMEAÇAS

Os agentes de ameaças modernos são metódicos, investindo semanas ou meses para pensar em como terão acesso a aplicativos e dados valiosos. Depois que identificam uma oportunidade, eles podem explorar uma abertura ou enviar e-mails de phishing para atrair os usuários a abrir um anexo mal-intencionado. A detecção e a resposta são elementos essenciais de um programa abrangente de segurança cibernética, junto com treinamento de funcionários, avaliações de segurança cibernética, testes de vulnerabilidade e de penetração, planejamento de resiliência e de recuperação e muito mais.

Caso o invasor tenha acesso, ele primeiro quer estabelecer uma base e a partir da qual ampliar o escopo do ataque. Mais uma vez, ele usa tempo para consolidar as posições dele na infraestrutura da empresa. Por exemplo, além de atacar sistemas empresariais, os ataques de ransomware geralmente visam manter off-line os sistemas de backup de uma empresa e bloquear o acesso aos backups. Isso pode eliminar a capacidade de uma empresa de se recuperar, deixando o pagamento do resgate como a única opção para recolocá-la em funcionamento.

Figura 1. Estratégia do agente de ameaças



Recursos sofisticados e constantemente atualizados de detecção e resposta são vitais para reconhecer ataques e outras pistas. O aviso antecipado dá à organização a oportunidade de reduzir os danos causados pelo ataque antes que ele se espalhe ainda mais.

As organizações vêm implementando uma ampla variedade de ferramentas de segurança cibernética, como as de auditoria de senhas, testes de rede, análise de vulnerabilidades, criptografia, monitoramento e detecção de ameaças. Os alertas vêm para a TI de todas essas ferramentas — o grande volume de alertas é desafiador, ainda mais quando se considera a dificuldade de correlacionar eventos entre as ferramentas. Além disso, manter a proficiência em todas essas tecnologias é um compromisso de tempo significativo para a equipe de segurança de TI.

O lado humano da equação de MDR exige um grupo de profissionais com anos de experiência e habilidades em segurança cibernética, como administração de sistemas, perícia forense cibernética, investigações de ameaças e testes de penetração. Esses profissionais são difíceis de encontrar, são caros de contratar e são constantemente recrutados por organizações mais proeminentes e com mais gastos. A pesquisa State of the CIO de 2021 identificou os cargos de segurança cibernética como os mais difíceis de preencher.[5] Reter analistas de segurança e preencher as vagas dos que saem é uma batalha interminável para os líderes de TI.

Mesmo depois de adquirir as ferramentas e os talentos essenciais, as empresas devem desenvolver operações e instalações de segurança 24x7.

Por que usar o Dell Technologies Managed Detection and Response

Pessoal

- **Especialistas experientes em segurança cibernética**
- **Analistas certificados pelo Taegis XDR**
- **As certificações também incluem CEH, GIAC SANS, CISSP e CompTIA**

Tecnologia

- **Plataforma de lógica analítica de segurança do Secureworks Taegis XDR, líder do setor**
- **Monitoramento contínuo e completo de ameaças utilizando telemetria de uma ampla variedade de endpoints, rede e nuvem**

Processo

- **Menos tempo de resolução**
- **Cobertura 24x7/365**
- **Assistência à implementação de agentes incluída**
- **40 horas por trimestre de orientação de correção remota**
- **40 horas por ano de iniciação da resposta a incidentes**

Parceiro de confiança

- **Confiável em todo o mundo para suporte a dispositivos e infraestrutura**
- **Mais de 20 anos de inovação em resiliência dos negócios**
- **Investindo continuamente em pessoas, processos e ferramentas**

Figura 2. Threat Intelligence

Os serviços Dell Managed Detection and Response dão acesso a recursos de primeira linha

Não surpreende que empresas de médio e pequeno porte geralmente se esforcem para se defender corretamente. O ambiente de segurança cibernética se tornou um caleidoscópio cada vez mais dinâmico de ameaças. A inundação de atividades ampliou os requisitos de pessoal, e a complexidade dos ataques eleva o nível de talento necessário.

O Dell Managed Detection and Response amplia sua equipe de segurança com especialistas em segurança cibernética, ferramentas e recursos operacionais comparáveis aos das maiores empresas globais. O Dell MDR reduz a carga da sua equipe de TI, diminui os riscos e aprimora significativamente a postura de segurança da sua empresa para que você possa se concentrar nas prioridades dos negócios.

O Dell Managed Detection and Response é uma combinação totalmente integrada de tecnologia, conhecimento especializado e operações. O serviço se baseia no conhecimento dos analistas de segurança da Dell Technologies que têm passado anos ajudando empresas de todo o mundo a proteger melhor as operações delas. O Dell MDR usa o poder do Secureworks® Taegis™ XDR — uma plataforma avançada de software de lógica analítica de segurança que é o produto de mais de 20 anos de conhecimento comprovado, pesquisa e Threat Intelligence reais e experiência em detectar e responder a ameaças sofisticadas.

Secureworks Taegis XDR

O Secureworks Taegis XDR é uma plataforma de segurança cibernética de uso específico que traz uma solução em escala de Big Data para as preocupações com a segurança. Uma plataforma nativa da nuvem, o Taegis XDR inclui avaliações contínuas orientadas por máquina e aprendizagem profunda de telemetria e eventos de diferentes vetores de ataque, reforçadas com informações completas sobre ameaças.

A única maneira de identificar e responder a ataques sofisticados é primeiro entender como os agentes mal-intencionados funcionam e o que os motiva. Todos os anos, a equipe do Secureworks por trás do XDR realiza aproximadamente 1.000 engajamentos de resposta a incidentes. Isso oferece a eles uma vantagem distinta de ver como as estratégias, as técnicas e os processos do agente de ameaças que efetivamente penetram as empresas dos clientes mudam regularmente.

O Taegis XDR analisa os dados relevantes à segurança coletados em endpoints, redes, sistemas de nuvem e sistemas de negócios no local para detectar ameaças. O XDR é uma plataforma totalmente aberta que complementa a infraestrutura de segurança existente, garantindo cobertura abrangente e protegendo investimentos anteriores.

O XDR oferece resposta, correção e informações automatizadas para aumentar a eficiência das operações de segurança e dar às equipes de resposta a visibilidade necessária para agir quando confrontadas com uma ameaça. Os clientes do Dell MDR se beneficiam da Threat Intelligence desenvolvida usando centenas de milhares de pontos de dados compilados entre clientes e serviços de inteligência compartilhados em todo o mundo.

Coloque os principais especialistas em segurança para trabalhar por você

Uma equipe global de analistas de segurança altamente treinados está sempre em busca de problemas nos seus sistemas. Os especialistas qualificados em segurança cibernética da Dell são experientes em todas as fases de detecção e redução de ameaças, inclusive investigações de ameaças, busca por ameaças, segurança de endpoint e resposta e recuperação de incidentes. Os analistas da Dell têm certificação XDR e têm uma variedade de outras certificações governamentais e reconhecidas pelo setor, inclusive CEH, GIAC SANS, CISSP e CompTIA. O centro de operações de segurança distribuído "Siga o sol" do Dell MDR funciona 24x7/365 dias por ano.

A equipe do Dell MDR conhece as operações e a infraestrutura de TI de uma empresa. Eles usam aprendizado de máquina e informações confiáveis sobre ameaças a milhares de ambientes de TI, fornecidas por meio do XDR para monitorar seu ambiente. A equipe do Dell MDR entra em ação instantaneamente quando uma advertência é exibida, investigando os dados de alerta para detectar conexões e padrões que apenas analistas de segurança treinados e experientes reconheceriam. Em seguida, eles aconselham os membros da equipe de resposta de uma organização sobre o melhor curso de ação.

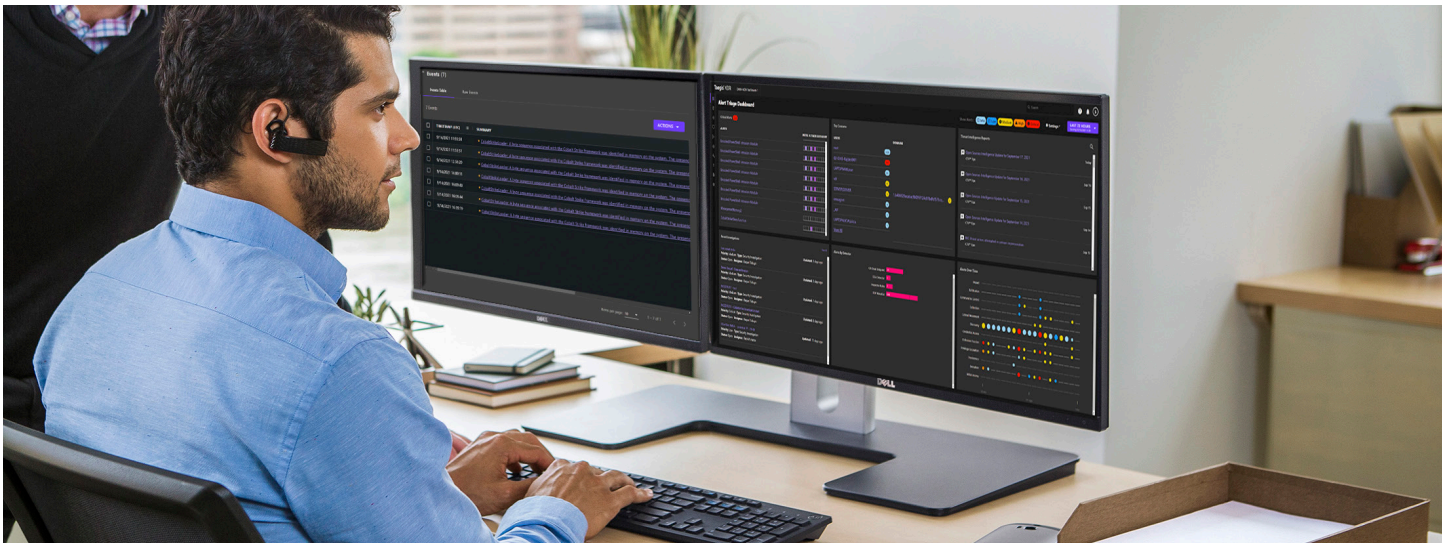
O Dell MDR faz parte do esforço de várias décadas da Dell para desenvolver uma organização de serviços de TI de classe mundial. Isso significa que os especialistas em segurança cibernética do Dell MDR não apenas fornecerão uma orientação excepcional para corrigir ameaças, mas também terão as habilidades e o conhecimento necessário para gerenciá-las em qualquer organização.

Busca por ameaças — identificando ameaças que podem escapar dos sistemas automatizados

Os agentes de ameaças estão cientes dos sistemas de detecção automatizada, portanto, trabalham para desenvolver novos tipos ou variações de ataque com base nos tipos existentes para passar por esses sistemas. Com um sistema como o Taegis XDR, isso não é fácil, mas é possível.

Os analistas de segurança utilizam a busca por ameaças para identificar essas ameaças "escondidas". Essa busca procura indicadores de comprometimento, o que pode ser uma série de logins malsucedidos em uma conta seguidos por um login bem-sucedido, ou tentativas de login anormais, como fora do horário comercial regular ou alterações repetidas em um arquivo em um curto período de tempo.

A busca eficaz por ameaças é um produto de tecnologia e de pessoas. A plataforma Taegis XDR oferece uma enorme quantidade de detalhes sobre a atividade de um invasor. Os analistas do Dell MDR exploram esses detalhes para reconhecer atividades até mesmo as bem escondidas.



CONHEÇA O DELL MDR

As mídias de notícias têm relatado as dificuldades de governos e corporações globais para conter ameaças à segurança cibernética. As empresas de médio e pequeno porte não precisam mais enfrentar esse desafio sozinhas. Com o Dell MDR, sua organização pode se beneficiar de especialistas em segurança altamente qualificados e dedicados a protegê-la, além de uma plataforma de segurança líder do setor, o Secureworks Taegis XDR. Sua organização aproveita a capacidade da Dell de investir em pessoas, processos e ferramentas para criar um serviço de segurança gerenciado adaptado às necessidades dela. O Dell Managed Detection and Response é um serviço de segurança cibernética de classe mundial que é acessível a todos.

Saiba mais sobre o Dell MDR

Entre em contato com um dos nossos especialistas em MDR

1. Aumento de 69% nos ataques segundo o FBI: https://blog.isc2.org/isc2_blog/2021/03/fbi-cybercrime-shot-up-in-2020-amidst-pandemic.html
2. 34% são internos: https://www.verizon.com/business/resources/reports/dbir/
3. 67% não confiam na capacidade de recuperação após um ataque cibernético destrutivo: www.delltechnologies.com/gdpi
4. 82% dos funcionários relatam uma falta de habilidade com segurança cibernética: https://www.csis.org/analysis/cybersecurity-workforce-gap
5. 13 cargos de TI mais difíceis de preencher: https://www.cio.com/article/221772/10-most-difficult-it-jobs-for-employers-to-fill.html

DELL Technologies