DELL Technologies

Aprimore a maturidade de resiliência e segurança cibernética

A maturidade em segurança cibernética é uma alavanca estratégica para todas as empresas modernas

O atual cenário de ameaças cibernéticas está mais dinâmico e implacável do que nunca, com ataques baseados em IA aumentando em frequência, velocidade e sofisticação. As organizações não podem mais depender de defesas improvisadas ou atualizações incrementais.

Como líder de negócios, você precisa operar como se as violações fossem inevitáveis ou até estivessem prestes a acontecer. Na Dell Technologies, ajudamos os clientes a aumentar a maturidade de segurança e o nível de confiança das operações de negócios diante do risco cibernético. Fazemos isso promovendo uma abordagem abrangente e em camadas de segurança cibernética e resiliência, construída em torno de três áreas de prática fundamentais.

As empresas precisam ter recursos para:

- **Reduzir a superfície de ataque**
- **Detectar e responder a ameaças cibernéticas**
- **Recuperar-se de ataques cibernéticos**

Uma segurança cibernética eficaz começa com uma avaliação honesta da sua atual postura de segurança e maturidade. Essa clareza permite priorizar as melhorias certas e investir em um futuro mais seguro.

Reduza a superfície de ataque

A superfície de ataque de uma organização é dinâmica e está em rápida evolução, com a IA introduzindo novos vetores de ataque. Juntamente com o trabalho remoto e os sistemas legados, eles ampliam a superfície de ataque, criando mais pontos de entrada para agentes mal-intencionados. Isso torna a redução da superfície de ataque uma necessidade estratégica para reduzir os riscos, cumprir as obrigações de conformidade, proteger a resiliência organizacional e criar confiança na linha de base.

Aprimore a maturidade de resiliência e segurança cibernética

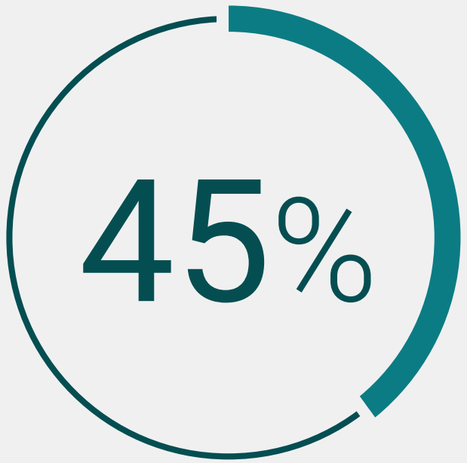
Reduzir a superfície de ataque ajuda a diminuir o risco geral, minimizando os pontos de entrada que os invasores podem explorar. Isso fortalece sua maturidade em segurança e agiliza os esforços de conformidade. O resultado é uma maior resiliência, redução de custos ao evitar incidentes e a capacidade de avançar mais rapidamente, inovar com mais liberdade e entrar em novos mercados com a confiança de que a segurança está incorporada desde o início. Começa com a adoção dos princípios Zero Trust (nunca confiar, sempre verificar) e a aplicação do menor privilégio entre usuários, dispositivos e aplicativos.

Na Dell Technologies, nós adotamos uma mentalidade de "segurança por padrão". A segurança cibernética está integrada em tudo o que fazemos, começando pela nossa cadeia de suprimentos global segura e estendendo-se às proteções incorporadas nos nossos principais produtos. Essas proteções começam no nível do hardware para ajudar a garantir que os dispositivos iniciem e executem apenas software confiável. Alinhamos nossas soluções aos princípios Zero Trust, ajudando você a eliminar vulnerabilidades antes que os invasores possam explorá-las. Os PCs com IA comerciais mais seguros do mundo[1], por exemplo, fornecem defesas fundamentais para o espaço de trabalho moderno.

A redução da superfície de ataque aumenta sua maturidade de segurança eliminando incertezas — menos incógnitas, menos pontos de entrada e menos surpresas.

Principais resultados para os clientes:

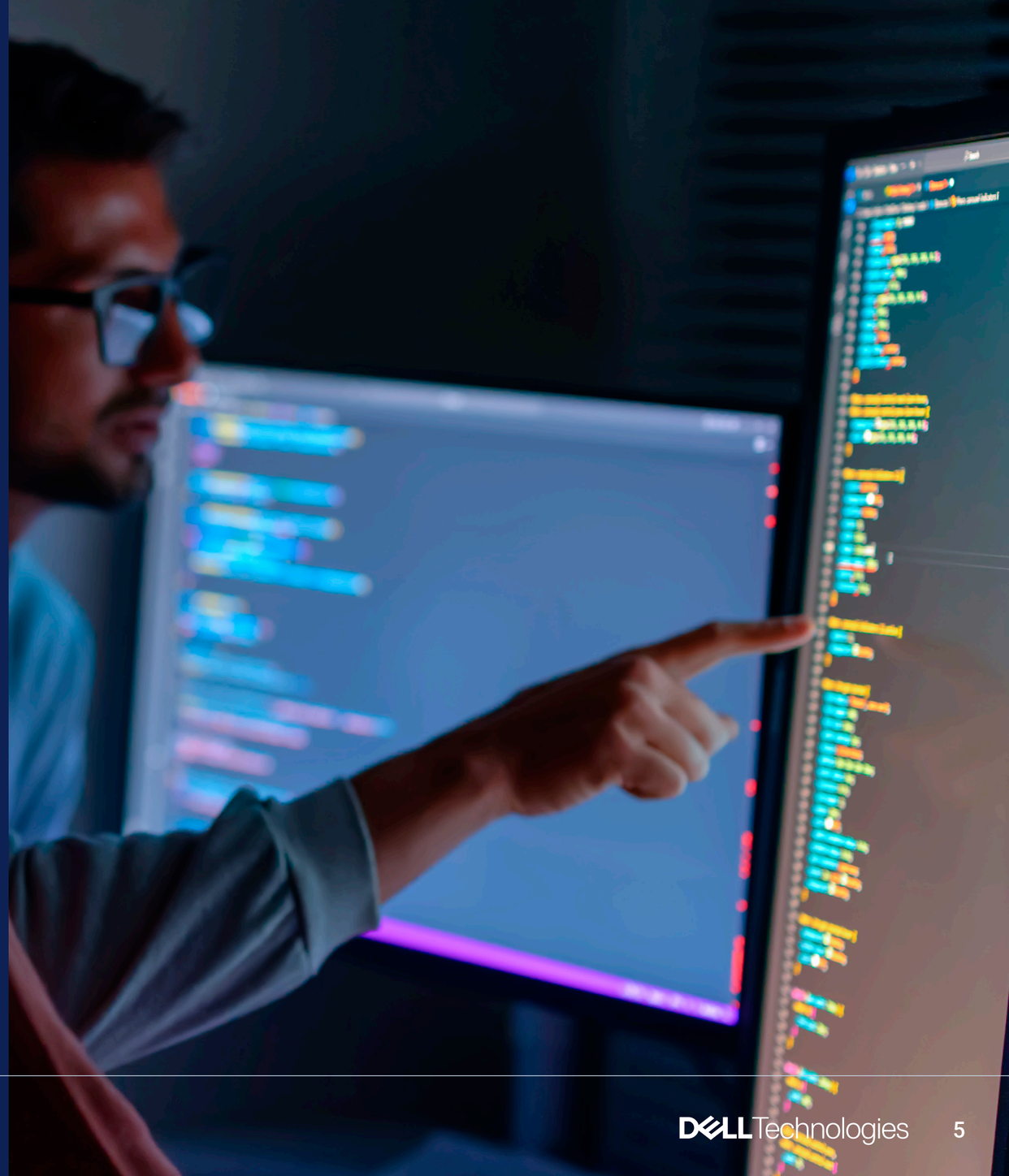
- **Minimização de vulnerabilidades:** Ao reforçar proativamente os endpoints, a infraestrutura e os aplicativos, você pode reduzir drasticamente as oportunidades para os invasores.
- **Gerenciamento de segurança simplificado:** Menos ativos expostos significam menos controles para gerenciar, resultando em uma postura de segurança mais otimizada e eficiente.
- **Base mais sólida para a inovação:** Com endpoints confiáveis e dados protegidos, você pode adotar novas tecnologias, como computação de borda e IA, com mais confiança.



Organizações que se concentram em reduzir sua superfície de ataque alcançam uma redução de 45% no risco de violação cibernética ao gerenciar exposições externas.[2]

Detecte e responda a ameaças cibernéticas

Na arena da segurança cibernética, a velocidade e a inteligência andam lado a lado. A detecção e a resposta eficazes permitem identificar e conter ameaças rapidamente, reduzindo o tempo de espera e limitando os danos de um ataque. O resultado é a redução de custos, menos tempo de inatividade e maior confiança operacional de que sua empresa pode operar com segurança mesmo sob ameaça constante.



Aprimore a maturidade de resiliência e segurança cibernética

No entanto, muitas organizações enfrentam dificuldades com a visibilidade limitada em ambientes híbridos e volume excessivo de alertas. Agora, os invasores permanecem dentro das redes por uma média de 11 dias antes da detecção. Para combater isso, você precisa de visibilidade em tempo real em endpoints, redes e sistemas por meio de monitoramento contínuo, inteligência contra ameaças e automação.

Os parceiros certos de segurança oferecem o conhecimento especializado em Threat Intelligence e resposta a incidentes. A Dell combina lógica analítica avançada, detecção de ameaças orientada por IA/ML e serviços gerenciados 24x7 com uma base de hardware segura para identificar e conter ameaças antes que causem interrupções. Serviços opcionais como nossa Managed Detection and Response (MDR) fornecem conhecimento especializado em segurança para ampliar a visibilidade e responder e mitigar ameaças rapidamente.

Fortes capacidades de detecção e resposta aumentam a maturidade da segurança, reduzindo o tempo de permanência e fornecendo às equipes a confiança necessária para agir decisivamente quando surgirem ameaças.

Principais resultados para os clientes:

- **Detecção mais rápida e menor tempo de espera:** O serviço Managed Detection and Response (MDR) pode reduzir o tempo médio de detecção e resposta em 25% a 49%, diminuindo a probabilidade de um ataque se tornar mais grave.
- **Redução da carga operacional:** A parceria com especialistas para a busca proativa de ameaças e monitoramento contínuo transfere a carga das equipes internas, liberando-as para o trabalho estratégico.
- **Resiliência aprimorada:** Recursos maduros de detecção e resposta resultam em menos incidentes de segurança e ajudam a evitar custos mais elevados relacionados a violações.

US$ **4,44** milhões

O custo médio de uma violação de dados atingiu US$ 4,44 milhões em 2025.[3]

Recupere-se de um ataque cibernético

Quando o pior cenário ocorrer, o objetivo principal é retornar às operações normais o mais rápido possível, com o mínimo de interrupção. A recuperação após um ataque cibernético garante a restauração rápida de dados e sistemas limpos, reduzindo danos à reputação e proporcionando a confiança de que a recuperação é confiável e livre de reinfecções.

Aprimore a maturidade de resiliência e segurança cibernética

Além de construir as defesas mais fortes possíveis, você precisa se planejar como se um ataque estivesse prestes a acontecer a qualquer momento. É crucial ter um plano em vigor e recursos de recuperação implementados. Isso inclui manter backups limpos e imutáveis dos dados essenciais em um cofre de recuperação isolado e usar ambientes de sala limpa, a fim de validar se os sistemas restaurados estão livres de malware antes de colocá-los on-line novamente.

A Dell integra recursos de recuperação às ofertas de produtos — e nossa maior prioridade é fazer com que as empresas retornem às operações após incidentes. Soluções como o nosso cofre do PowerProtect Cyber Recovery isolam e protegem cópias limpas de dados críticos para uma recuperação rápida, limitando perdas e reduzindo o poder de alavancagem de atacantes de ransomware. Essa arquitetura permite colocar rapidamente as cargas de trabalho essenciais on-line novamente, para que você se sinta confiante.

A recuperação é frequentemente o momento em que a maturidade em segurança é verdadeiramente testada, quando a confiança depende da rapidez e da eficiência com que a empresa consegue retornar às operações normais.

Principais resultados para os clientes:

- **Redução do impacto nos negócios:** Organizações com um plano de resposta a incidentes bem ensaiado podem reduzir os custos de violações em aproximadamente 61%.
- **Retomada mais rápida das operações:** Priorizar um rápido retorno aos negócios, não apenas a remoção de ameaças, ajuda a restaurar as operações com o mínimo de interrupção e custo.
- **Integridade de dados aprimorada:** Isolar dados essenciais, usar cópias imutáveis e validar a integridade antes de uma restauração aumenta a confiança no processo de recuperação.

das organizações admitem que teriam dificuldades para se recuperar de um ataque cibernético e, ao mesmo tempo, cumprir os acordos de nível de serviço.[4]

Aprimore a maturidade de resiliência e segurança cibernética

Fortaleça sua postura de segurança por meio de parcerias estratégicas

Os parceiros experientes são essenciais para navegar no cenário de segurança cibernética atual, dinâmico e complexo. As ameaças cibernéticas estão se tornando mais sofisticadas e frequentes, tornando praticamente impossível para uma única organização manter o conhecimento especializado, os recursos e a tecnologia necessários para se manter à frente. Ao colaborar com líderes de segurança como a Dell, as empresas obtêm acesso a habilidades especializadas, tecnologias de ponta e uma rede de parceiros confiáveis. Essas parcerias fornecem o suporte e o conhecimento especializado necessários para detectar, prevenir e responder a ameaças de forma eficaz, garantindo que as empresas permaneçam protegidas em um ambiente digital em constante evolução.

Com a abordagem correta nessas três áreas de atuação, as organizações aumentam sua maturidade em segurança, construindo a confiança para operar, inovar e crescer apesar da constante pressão cibernética. A Dell reúne infraestrutura confiável, espaço de trabalho confiável, serviços avançados e uma rede de parceiros para ajudar sua organização a se manter segura, adaptável e resiliente, pronta para o futuro.

Explore soluções de segurança

Perguntas frequentes

1. Por que a segurança cibernética deve ser a principal prioridade da minha empresa?
A segurança cibernética é mais do que apenas proteção; é a base que permite a uma empresa inovar e crescer, resistindo ao perigoso cenário de segurança cibernética. Uma postura de segurança robusta não se resume apenas à defesa, trata-se de capacitação. Empresas com estruturas maduras de segurança cibernética podem se mover mais rapidamente, inovar com mais liberdade e entrar em novos mercados com confiança. Eles estão mais bem equipados para lidar com mudanças das normas, demandas de clientes e pressões da concorrência.

2. Como podemos equilibrar a necessidade de segurança rigorosa com a liberdade de inovar?
Você não deveria ter que escolher entre segurança e inovação. Acreditamos que a segurança robusta realmente impulsiona a inovação. Quando você tem uma base "segura por padrão", em que a segurança é integrada aos dispositivos, à infraestrutura e aos dados desde o início, suas equipes podem adotar novas tecnologias, como a computação de borda e a IA, com confiança.

3. Por que a segurança da cadeia de suprimentos é tão crítica?
A verdadeira segurança começa muito antes de o botão liga/desliga ser pressionado. À medida que sua presença digital cresce, sua exposição também aumenta, e a confiança se torna sua primeira linha de defesa. Cada elo da cadeia de suprimentos deve ser protegido, pois um único componente comprometido pode prejudicar até mesmo o software mais avançado. É por isso que criamos a segurança desde a base, protegendo cada etapa, da produção à implementação. Do chão de fábrica à sua porta de entrada, sua tecnologia chega confiável, verificada e construída para funcionar com confiança.

4. Como a Dell contribui para a nossa recuperação após um ataque cibernético?
Minimizar o tempo de inatividade e as interrupções é fundamental quando ocorrem incidentes. A preparação é fundamental. Nosso cofre do PowerProtect Cyber Recovery isola uma cópia limpa e imutável dos seus dados mais críticos, mantendo-a separada com segurança do ambiente principal. Em caso de incidente, você pode restaurar as operações com rapidez e confiança, sem compromissos e sem pagar resgate.
A Dell oferece uma variedade de produtos e serviços projetados para ajudar você a implementar uma estratégia de recuperação abrangente. Isso inclui desde serviços de consultoria para criar um plano de recuperação e treinamento até recursos de proteção de dados que podem manter dados críticos seguros. A Dell adota uma abordagem centrada nas pessoas e na tecnologia, garantindo que tanto os funcionários quanto a tecnologia trabalhem juntos para ajudar você a se recuperar rapidamente.

5. A Dell auxilia na detecção de ameaças em tempo real?
Com certeza. A velocidade é tudo quando se trata de deter uma ameaça cibernética. Combinamos recursos de segurança integrados com serviços avançados, como Managed Detection and Response (MDR) para monitorar seu ambiente 24/7. Ao utilizar insights baseados em IA/ML e conhecimento especializado humano, ajudamos você a identificar anomalias e possíveis ameaças instantaneamente, permitindo que você responda e contenha problemas antes que eles afetem sua empresa.

Fontes

[1] Com base em uma análise interna da Dell de outubro de 2024 (Intel) e de março de 2025 (AMD). Aplicável a PCs com processadores Intel e AMD. Nem todos os recursos estão disponíveis em todos os PCs. Compra adicional necessária para alguns recursos. PCs com tecnologia Intel validados pela Principled Technologies, julho de 2025 Infográfico Anatomia de um dispositivo confiável
[2] Forrester Consulting, "The Total Economic Impact™ of BitSight: Cost Savings and Business Benefits Enabled by BitSight", outubro de 2024.
[3] IBM and Ponemon Institute, "Cost of a Data Breach Report 2025: The AI Oversight Gap", 2025.
[4] Dell Technologies, "A infraestrutura tecnológica é o propulsor de todas as empresas modernas", fevereiro de 2025.

Sobre a Dell Technologies

A Dell Technologies (NYSE: Dell) ajuda pessoas e organizações a construir um futuro digital e a transformar a forma como trabalham, vivem e se divertem. A empresa oferece aos clientes o mais amplo e inovador portfólio de tecnologias e serviços do setor na era da IA.

Copyright © 2026 Dell Inc. Todos os direitos reservados

Saiba mais em Dell.com