DELL Technologies

Cyberbeveiliging en veerkracht verbeteren

De volwassenheid van cyberbeveiliging is een strategische hefboom voor elk modern bedrijf

Het huidige landschap van cyberdreigingen is dynamischer en onvergeeflijker dan ooit, met AI-gestuurde aanvallen die steeds vaker voorkomen en sneller en verfijnder worden. Organisaties kunnen niet langer vertrouwen op fragmentarische beveiligingsmaatregelen of incrementele updates.

Als bedrijfsleider moet u handelen alsof een inbreuk onvermijdelijk, zelfs op handen is. Bij Dell Technologies helpen we klanten met het vergroten van de volwassenheid van hun beveiliging en het vertrouwen dat ze hebben in het runnen van hun bedrijf in het licht van cyberrisico's. We doen dit door een uitgebreide, gelaagde aanpak voor cyberbeveiliging en veerkracht te bevorderen die is opgebouwd rond drie cruciale punten.

Bedrijven moeten beschikken over de capaciteiten om:

- **Hun aanvalsoppervlak te verkleinen**
- **Cyberbedreigingen te detecteren en erop te reageren**
- **Te herstellen van cyberaanvallen**

Effectieve cyberbeveiliging begint met een eerlijke beoordeling van uw huidige beveiligingsmentaliteit en -volwassenheid. Gewapend met die kennis kunt u prioriteit geven aan de juiste verbeteringen en investeren in een veiligere toekomst.

Het aanvalsoppervlak beperken

Het aanvalsoppervlak van een organisatie is dynamisch en evolueert snel nu AI nieuwe aanvalsvectoren introduceert. Samen met werken op afstand en verouderde systemen vergroten ze het aanvalsoppervlak, waardoor er meer access points voor bedreigers ontstaan. Daarom is beperking van het aanvalsoppervlak een strategische noodzaak om risico's te verminderen, te voldoen aan nalevingsverplichtingen, de veerkracht van de organisatie te beschermen en basisvertrouwen op te bouwen.

Cyberbeveiliging en veerkracht verbeteren

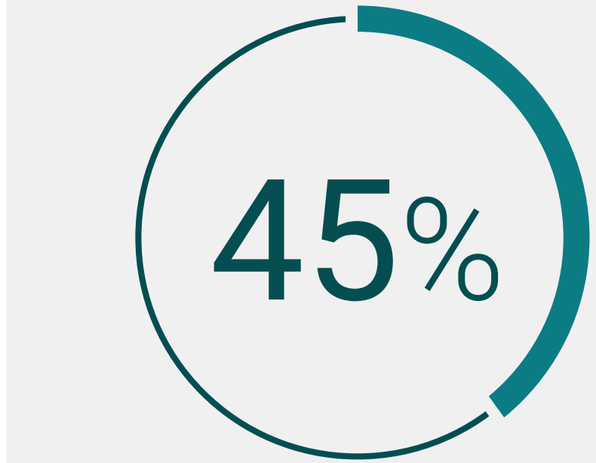
Door het aanvalsoppervlak te verkleinen, verlaagt u het algehele risico, u beperkt immers de access points die aanvallers kunnen misbruiken tot een minimum. Dit versterkt de volwassenheid van uw beveiliging en stroomlijnt de nalevingsactiviteiten. Het resultaat is meer veerkracht, lagere kosten doordat incidenten worden voorkomen en de mogelijkheid om sneller te bewegen, vrijer te innoveren en vol vertrouwen nieuwe markten te betreden in de wetenschap dat beveiliging vanaf het begin is ingebouwd. Het begint met het toepassen van Zero Trust-principes - nooit vertrouwen, altijd controleren - en het afdwingen van minimale rechten voor alle gebruikers, apparaten en applicaties.

Bij Dell Technologies hanteren we een 'secure-by-design'-mentaliteit. Cyberbeveiliging is een integraal onderdeel van alles wat we doen, van onze veilige wereldwijde leveringsketen tot en met ingebouwde beveiligingsmaatregelen in onze belangrijkste producten. Deze beveiliging begint op hardwareniveau om ervoor te zorgen dat apparaten opstarten en alleen vertrouwde software uitvoeren. We stemmen onze oplossingen af op Zero Trust-principes, zodat u beveiligingslekken kunt elimineren voordat aanvallers deze kunnen misbruiken. Onze veiligste zakelijke AI PC's ter wereld [1]bieden bijvoorbeeld fundamentele verdediging voor de moderne werkruimte.

Door het aanvalsoppervlak te beperken, verhoogt u de volwassenheid van uw beveiliging door een einde te maken aan onzekerheid: minder onbekende factoren, minder access points en minder verrassingen.

Belangrijkste resultaten voor klanten:

- **Beveiligingslekken minimaliseren:** door eindpunten, infrastructuur en applicaties proactief te versterken, kunt u de kansen voor aanvallers drastisch verminderen.
- **Vereenvoudigd beveiligingsbeheer:** minder blootgestelde assets betekent minder controles, wat leidt tot een meer gestroomlijnde en efficiënte beveiligingsmentaliteit.
- **Sterkere basis voor innovatie:** met vertrouwde eindpunten en beschermde data kunt u nieuwe technologieën zoals AI en edge computing met meer vertrouwen implementeren.



Organisaties die zich richten op beperking van hun aanvalsoppervlak, lopen een 45% lager risico op cyberinbreuk wat betreft het beheren van blootstelling aan externe bedreigingen.[2]

Cyberbedreigingen detecteren en erop reageren

Op het gebied van cyberbeveiliging gaan snelheid en intelligentie hand in hand. Met effectieve detectie en respons kunt u bedreigingen snel identificeren en beheersen, waardoor de verblijfstijd wordt verkort en de schade van een aanval wordt beperkt. Het resultaat is lagere kosten, minder downtime en meer operationeel vertrouwen dat uw bedrijf veilig kan werken, zelfs als er constant sprake is van bedreigingen.

Cyberbeveiliging en veerkracht verbeteren

Veel organisaties worstelen echter met beperkte zichtbaarheid in hybride omgevingen en een overweldigend volume aan waarschuwingen. Aanvallers verblijven nu gemiddeld 11 dagen in netwerken voordat ze worden ontdekt. Om dit tegen te gaan, hebt u realtime inzicht nodig in eindpunten, netwerken en systemen door middel van continue bewaking, Threat Intelligence en automatisering.

De juiste beveiligingspartners bieden gespecialiseerde expertise op het gebied van Threat Intelligence en incidentrespons. Dell combineert geavanceerde analyses, AI/ML-gestuurde bedreigingsdetectie en 24x7 beheerde services met een veilige hardwarebasis om dreigingen te identificeren en in te dammen voordat ze voor verstoring zorgen. Optionele services zoals onze Managed Detection and Response (MDR) bieden beveiligingsexpertise om de zichtbaarheid te vergroten en snel te reageren op bedreigingen en deze te beperken.

Sterke detectie- en responsmogelijkheden verhogen de volwassenheid van uw beveiliging door de verblijfstijd te verkorten en teams het vertrouwen te geven dat ze daadkrachtig kunnen optreden wanneer er bedreigingen opduiken.

Belangrijkste resultaten voor klanten:

- **Snellere detectie en kortere verblijfstijd:** Managed detection and response (MDR) kan de gemiddelde tijd om een aanval te detecteren en erop te reageren met 25-49% verkorten en zo de kans verkleinen dat een aanval ernstiger wordt.
- **Verlichting van operationele last:** door samen te werken met experts voor proactieve dreigingsdetectie en continue monitoring, worden interne teams minder belast en kunnen ze zich richten op strategische taken.
- **Verbeterde veerkracht:** geavanceerde detectie- en responsmogelijkheden leiden tot minder beveiligingsincidenten. Zo worden hoge aan beveiligingsincidenten gerelateerde kosten vermeden.

4,44 **miljoen** dollar

De gemiddelde kosten van een datalek bedroegen in 2025 4,4 miljoen dollar.[3]

Herstel na een cyberaanval

Wanneer het ergste scenario zich voordoet, is het primaire doel om zo snel mogelijk en met minimale verstoring terug te keren naar de normale bedrijfsvoering. Herstel na een cyberaanval zorgt ervoor dat u schone data en systemen snel kunt herstellen, zodat u minder reputatieschade lijdt en erop kunt vertrouwen dat uw herstel betrouwbaar is zonder risico op herinfectie.

Cyberbeveiliging en veerkracht verbeteren

Ook al bouwt u de sterkst mogelijke verdedigingswerken, u moet plannen alsof een aanval onvermijdelijk is. Het is van cruciaal belang om over een volledig herstelplan en de nodige capaciteiten te beschikken. Dit omvat het onderhouden van schone, onveranderlijke back-ups van kritieke data in een geïsoleerde herstelkluis en het gebruik van cleanroom-omgevingen om te controleren of herstelde systemen vrij zijn van malware voordat ze weer online worden gezet.

Dell bouwt herstelmogelijkheden in het productaanbod in en wanneer zich incidenten voordoen, is het onze eerste prioriteit om bedrijven weer operationeel te krijgen. Oplossingen zoals onze PowerProtect Cyber Recovery Vault isoleren en beveiligen schone kopieën van kritieke data voor snel herstel. Zo worden de verliezen beperkt en kunnen ransomware-aanvallers minder schade aanrichten. Deze architectuur helpt u om kritieke workloads snel weer online te krijgen, zodat u zich geen zorgen hoeft te maken.

Herstel is vaak het punt waar de volwassenheid van de beveiliging echt wordt getest, wanneer vertrouwen afhankelijk is van hoe snel en schoon de normale bedrijfsvoering kan worden hersteld.

Belangrijkste resultaten voor klanten:

- **Minder impact op het bedrijf:** organisaties met een goed doordacht incidentresponsplan kunnen de kosten van inbreuken met ongeveer 61% verlagen.
- **Snellere hervatting van activiteiten:** door de nadruk te leggen op een snel herstel van activiteiten, niet alleen op het verwijderen van bedreigingen, kan de bedrijfsvoering met minimale verstoring en kosten worden hersteld.
- **Verbeterde data-integriteit:** door kritieke data te isoleren, onveranderlijke kopieën te gebruiken en de integriteit te valideren voordat een herstel plaatsvindt, neemt het vertrouwen in het herstelproces toe.

van de organisaties gaf toe dat ze moeite zouden hebben om te herstellen van een cyberaanval en tegelijkertijd aan hun Service Level Agreements te blijven voldoen.[4]

De volwassenheid van uw beveiliging versterken via strategische partnerschappen

Ervaren partners zijn essentieel om het hoofd te kunnen bieden aan het huidige snel veranderende en complexe landschap van cyberbeveiliging. Cyberdreigingen worden steeds geavanceerder en frequenter, waardoor het bijna onmogelijk is voor één organisatie om de expertise, resources en technologie te behouden die nodig zijn om voorop te blijven lopen. Door samen te werken met leiders op het gebied van beveiliging zoals Dell, krijgen bedrijven toegang tot gespecialiseerde vaardigheden, geavanceerde technologieën en een netwerk van vertrouwde partners. Deze partnerschappen bieden de support en expertise die nodig zijn om bedreigingen effectief te detecteren, te voorkomen en erop te reageren, zodat bedrijven beschermd blijven in een steeds veranderende digitale omgeving.

Met de juiste aanpak op deze drie gebieden vergroten organisaties de volwassenheid van hun beveiliging en bouwen ze het vertrouwen op om te werken, te innoveren en te groeien ondanks constante cyberdruk. Dell combineert een vertrouwde infrastructuur, een vertrouwde werkruimte, geavanceerde services en een partner ecosysteem om uw organisatie te helpen veilig, flexibel en veerkrachtig te blijven, klaar voor de toekomst.

Ontdek beveiligingsoplossingen

Veelgestelde vragen

1. Waarom moet cyberbeveiliging een topprioriteit zijn voor mijn bedrijf?
Cyberbeveiliging is meer dan alleen bescherming, het is de basis waarop een bedrijf kan innoveren en groeien terwijl het zijn mannetje staat in het gevaarlijke landschap van cyberbeveiliging. Een sterke beveiligingsmentaliteit draait niet alleen om verdediging, maar ook om facilitering. Bedrijven met volledig ontwikkelde frameworks voor cyberbeveiliging kunnen sneller bewegen, vrijer innoveren en vol vertrouwen nieuwe markten betreden. Ze zijn beter uitgerust om te voldoen aan veranderingen in de regelgeving, eisen van klanten en concurrentiedruk.

2. Hoe kunnen we de noodzaak van strikte veiligheid in evenwicht brengen met de vrijheid om te innoveren?
U hoeft niet te kiezen tussen veilig zijn en innovatief zijn. Wij geloven juist dat robuuste beveiliging innovatie mogelijk maakt. Wanneer u beschikt over een 'secure-by-design'-basis, waarbij beveiliging vanaf het begin is ingebouwd in uw apparaten, infrastructuur en data, kunnen uw teams met vertrouwen nieuwe technologieën zoals AI en edge computing toepassen.

3. Waarom is de beveiliging van de leveringsketen zo belangrijk?
Echte beveiliging begint lang voordat de aan/uit-knop wordt ingedrukt. Naarmate uw digitale voetafdruk groter wordt, neemt ook uw blootstelling toe en wordt vertrouwen uw eerste verdedigingslinie. Elke schakel in de leveringsketen moet worden beschermd, omdat één gecompromitteerd onderdeel zelfs de meest geavanceerde software kan ondermijnen. Daarom bouwen we beveiliging vanaf de basis op, waardoor elke stap van productie tot implementatie wordt beschermd. Van de fabrieksvloer tot aan uw voordeur: u ontvangt vertrouwde technologie die gecontroleerd is en gebouwd om betrouwbaar te presteren.

4. Hoe helpt Dell ons bij het herstel na een cyberaanval?
Het minimaliseren van downtime en onderbrekingen is van cruciaal belang wanneer er incidenten optreden. Voorbereiding is essentieel. Onze PowerProtect Cyber Recovery Vault isoleert een schone, onveranderlijke kopie van uw meest kritieke data, veilig gescheiden van uw primaire omgeving. In het geval van een incident kunt u de bedrijfsvoering snel en vol vertrouwen herstellen zonder compromissen en zonder losgeld te betalen.
Dell biedt verschillende producten en services die zijn ontworpen om u te helpen een alomvattende herstelstrategie te implementeren. Dit varieert van consultancyservices voor het opstellen van een herstel- en trainingsplan tot mogelijkheden voor databescherming die kritieke data veilig houden. Dell kiest voor een mens- en technologiegerichte aanpak, zodat zowel werknemers als technologie samenwerken om u te helpen snel te herstellen.

5. Kan Dell helpen bij het in real time detecteren van bedreigingen?
Jazeker. Snelheid is alles als het gaat om het stoppen van een cyberdreiging. We combineren geïntegreerde beveiligingsfuncties met geavanceerde services zoals Managed Detection and Response (MDR) om uw omgeving 24/7 te bewaken. Door gebruik te maken van AI/ML-gestuurde inzichten en menselijke expertise, helpen we u afwijkingen en potentiële bedreigingen onmiddellijk te detecteren, zodat u kunt reageren en grip kunt krijgen op problemen voordat ze gevolgen hebben voor uw bedrijf.

Bronnen

[1] Gebaseerd op interne analyse van Dell, oktober 2024 (Intel) en maart 2025 (AMD). Van toepassing op pc's met Intel en AMD-processors. Niet alle functies zijn beschikbaar voor alle pc's. Extra aankoop vereist voor sommige functies. Intel pc's gevalideerd door Principled Technologies, juli 2025 Anatomy of a Trusted Device Infographic

[2] Forrester Consulting, "The Total Economic Impact™ of BitSight: Cost Savings and Business Benefits Enabled by BitSight", oktober 2024.

[3] IBM en Ponemon Institute, "Cost of a Data Breach Report 2025: The AI Oversight Gap", 2025.

[4] Dell Technologies, "Advance Cybersecurity Maturity: Technology Infrastructure is the Heartbeat of Every Modern Business," februari 2025.

Over Dell Technologies

Dell Technologies (NYSE: DELL) helpt organisaties en particulieren hun digitale toekomst vorm te geven en te transformeren hoe ze werken, leven en spelen. Het bedrijf biedt klanten de breedste en meest innovatieve technologieën in de branche en serviceportfolio's voor het AI-tijdperk.

Meer informatie op Dell.com