DELL Technologies

Ihr Fundament für echte Innovationen

Ausfallsicherheit bei Cyberangriffen
für das moderne Rechenzentrum

Legen Sie das Fundament für das moderne Rechenzentrum

Das Tempo der technologischen Transformation war vielleicht nie so hoch wie aktuell. Unternehmen stehen vor einem wachsenden Druck, die Einführung von KI zu beschleunigen und innovative Technologien zu entwickeln, während sie gleichzeitig kritische Daten schützen und die Geschäftskontinuität sicherstellen müssen. Eine starke Cybersicherheit und Ausfallsicherheit sind die entscheidenden Bausteine für die Entwicklung und Durchsetzung mutiger Ideen.

Wir bei Dell sind davon überzeugt, dass die Förderung von Innovationen ein Bekenntnis zu den drei Säulen der Ausfallsicherheit bei Cyberangriffen erfordert:

- **Verkleinerung der Angriffsfläche**
- **Erkennung von und Reaktion auf Cyberbedrohungen**
- **Wiederherstellung nach einem Cyberangriff**

Ausfallsicherheit bei Cyberangriffen zur Erfüllung der Innovationsanforderungen

Unternehmen können neue Produkte, Services und Geschäftsmodelle schneller als je zuvor entwickeln. Angesichts der beschleunigten Innovationsrate stehen Geschäfts- und IT-Führungskräfte vor einer zunehmenden Komplexität durch KI-gesteuerte Technologien, verteilte Infrastruktur und immer ausgefeiltere KI-gesteuerte Cyberbedrohungen.

Führungskräfte aus Unternehmen und IT erkennen an, dass sie sich zwischen der Notwendigkeit von Innovationen und der Notwendigkeit von Ausfallsicherheit bei Cyberangriffen hin- und hergerissen fühlen:

79 %
sagen, dass die Balance zwischen Sicherheit und Innovation eine Herausforderung in ihrem Unternehmen darstellt*

89 %
geben an, dass Sicherheit bei der Entwicklung neuer Innovationen eine entscheidende Rolle spielt*

67 %
der Befragten befürchten, dass Innovationen ihre Angriffsfläche vergrößern könnten.*

* Quelle: Umfrage von Dell Technologies unter 750 Geschäfts- und IT-EntscheiderInnen aus den USA, UK, DE, FR und JP, alle Segmente, Februar 2025.

Es gibt drei Ziele für das moderne Rechenzentrum, die die Spannung zwischen der Notwendigkeit von Innovationen und der Notwendigkeit von Ausfallsicherheit bei Cyberangriffen reduzieren:

1. **Minimieren Sie Sicherheitslücken** angesichts der rasanten Entwicklung von Cyberbedrohungen, insbesondere mit KI. Dies gibt Ihnen die Zuversicht Innovationen umzusetzen, ohne befürchten zu müssen, kritische Ressourcen unnötigen Risiken auszusetzen.

2. **Gehen Sie von Sicherheitsverletzungen aus**, um sich entwickelnde Bedrohungen schnell zu erkennen und darauf zu reagieren. Auf diese Weise können sich Teams auf Innovationen konzentrieren, statt kontinuierlich auf Bedrohungen zu reagieren.

3. **Schnelle Recovery und Rückkehr zur Business Continuity** nach einem Cyberangriff. Durch häufige Tests der Systeme und praxisorientierte Pläne können Unternehmen die Auswirkungen von Bedrohungen eindämmen und das Vertrauen von Kunden und Investoren in den Geschäftsbetrieb und Innovationspläne aufrechterhalten.

Dell liefert die Grundlage für Ausfallsicherheit bei Cyberangriffen für Innovationen

Die Vorgehensweise bei Dell zu Erzielung von Ausfallsicherheit bei Cyberangriffen basiert auf drei Säulen, um einen Sicherheitsstatus zu schaffen, der Innovationen ermöglicht. Jede Säule erfüllt ein wichtiges Ziel des modernen Rechenzentrums und sorgt gleichzeitig für die nötige Agilität und Flexibilität für echte Innovationen.

Verkleinerung der Angriffsfläche

Erkennung von und Reaktion auf Cyberbedrohungen

Recovery nach einem Cyberangriff

Verkleinerung der Angriffsfläche

Unternehmen können Innovationsinitiativen schnell und flexibel umsetzen, wenn die Teams davon überzeugt sind, dass es weniger Einstiegspunkte gibt, die AngreiferInnen ausnutzen können. Mit der End-to-End-Transparenz und dem integrierten Schutz von Dell können Sie Schwachstellen identifizieren und minimieren, Sicherheitslücken schließen und Richtlinien für den Zugriff auf Geräte, Systeme und Daten mit möglichst geringen Berechtigungen durchsetzen.

Konzipieren Sie eine sichere Infrastruktur von Grund auf mit der sicheren Lieferkette und der sicheren Komponentenverifizierung (Secured Component Verification, SVC) von Dell. Schützen Sie ganzen Prozess von der validierten Komponentenbeschaffung über die Fertigung bis zur Lieferung, um böswillige oder gefälschte Komponenten in Ihrer Bereitstellung zu verhindern.

Implementieren Sie Zero-Trust-Prinzipien mit den integrierten Sicherheitsfunktionen für die Identitäts- und Zugriffskontrolle von Dell, wie z. B. Multi-Faktor-Authentifizierung, biometrische Daten, rollenbasierte Zugriffskontrollen und duale Authentifizierung. Schaffen Sie eine Umgebung, in der neue Technologien, Remotezusammenarbeit und schnelle Experimente möglich sind, ohne dass dies die Sicherheit beeinträchtigt.

Entdecken Sie Sicherheitslücken vor einem Angriff mit den Sicherheitsbewertungsservices von Dell, einschließlich Penetrationstests und kontinuierlichem Sicherheitslückenmanagement. Proaktive Erkennung und Behebung von Sicherheitslücken Wenn ein Unternehmen nicht ständig damit beschäftigt ist, auf Bedrohungen zu reagieren, kann es sich auf das konzentrieren, was als Nächstes kommt.

Stellen Sie sicher, dass Geräte am Ende der Nutzungsdauer sicher mit den Asset Recovery Services (ARS) von Dell gemanagt werden. Neue Lösungen und Technologien können das Ende bestimmter Systeme und Hardware bedeuten. ARS sorgt dafür, dass Sie Systeme sicher und nachhaltig stilllegen.

Erkennung von und Reaktion auf Cyberbedrohungen

Wenn Organisationen Bedrohungen schnell erkennen und darauf reagieren können, werden keine Innovationsprojekte beeinträchtigt, was sich negativ auf das Vertrauen von Kunden, Partnern oder Investoren und somit auf das Geschäftswachstum auswirken könnte. Dell unterstützt Sie bei der Integration von Erkennungs und Reaktionsmechanismen in Ihre gesamte Infrastruktur, damit Sie sich weiterentwickelnde Bedrohungen stoppen können, bevor sie Ihre Geschäftsprozesse beeinträchtigen.

Beschleunigen Sie die Bedrohungserkennung und entlasten Sie gleichzeitig Ihre IT-Abteilung mit den Managed Detection and Response (MDR)-Services von Dell. Überwachen, erkennen und untersuchen Sie Bedrohungen in der gesamten IT-Umgebung kontinuierlich und reagieren Sie darauf, um Ihren Sicherheitsstatus schnell zu verbessern.

Mit der Threat Intelligence-Plattform von Dell **erhalten Sie Einblicke in Echtzeit in sich entwickelnde Sicherheitslücken.** Greifen Sie auf Threat Intelligence-Feeds, Bedrohungsanalysen und Incident-Response-Funktionen zu, um neue Bedrohungen proaktiv zu erkennen und darauf zu reagieren.

Reagieren Sie schnell mit fachkundiger Unterstützung, wenn Bedrohungen erkannt werden. Die CSIR-Services (Cybersecurity Incident Response) von Dell bieten Unterstützung durch ExpertInnen bei der Reaktion auf Incidents, einschließlich Analyse, Eindämmung und Beseitigung von Bedrohungen. Unser erfahrenes Team weiß, wie Sie Betriebsunterbrechungen minimieren und gleichzeitig Bedrohungen beseitigen können, damit Ihr Unternehmen Initiativen fördern kann, die einen echten Wettbewerbsvorteil bedeuten.

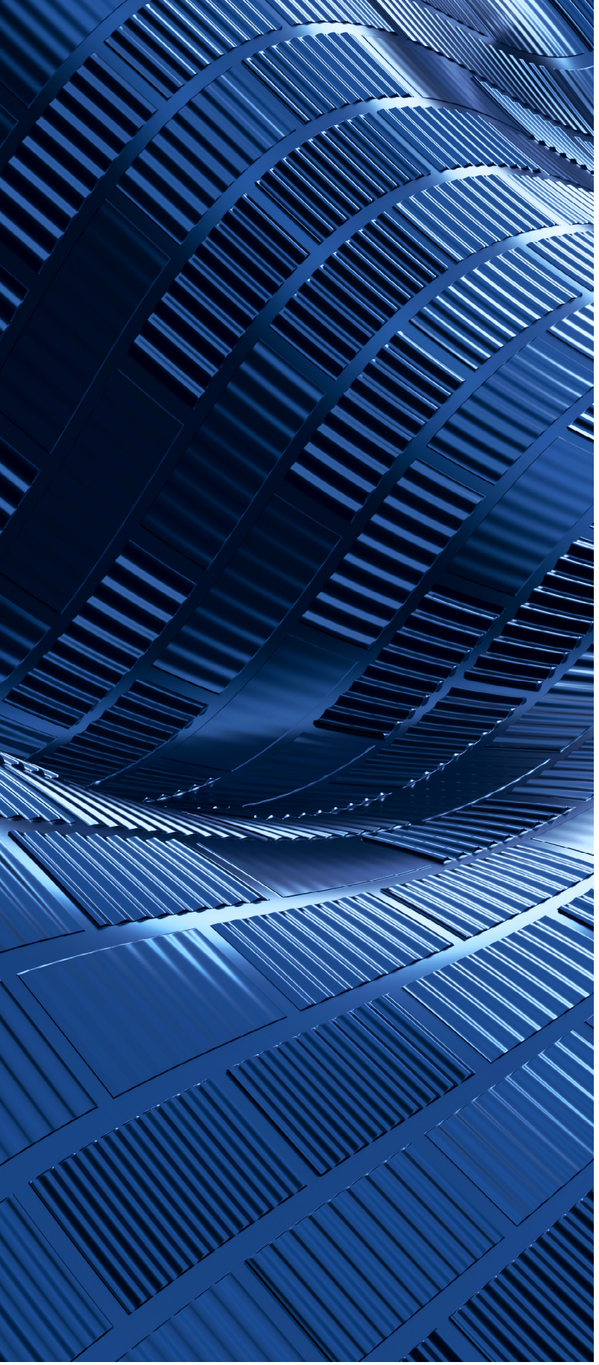
Recovery nach einem Cyberangriff

Unternehmen stärken das Vertrauen des Markts in ihre Innovationsfähigkeit, wenn sie demonstrieren, dass sie sich schnell von einem Angriff erholen, Betriebsabläufe wiederherstellen und Ausfallzeiten minimieren können. Effiziente Recovery-Funktionen, einschließlich der Wiederherstellung von Geräten, Systemen und Daten, sorgen dafür, dass selbst erfolgreiche Angriffe das Vertrauen der Kunden nicht dauerhaft beeinträchtigen. Eine schnelle Recovery ist von entscheidender Bedeutung für Branchen, die behördliche Auflagen einhalten und Audits durchführen müssen, um sicherzustellen, dass Angriffe sensible Daten oder Systeme nicht gefährdet haben.

Beschleunigen Sie die Server-Recovery mit Automated System Recovery (ASR) von Dell, die Server schnell auf ihren letzten bekannten, nicht kompromittierten Betriebszustand zurücksetzt.

Schützen Sie die Datenintegrität mit Dell Storage und Data Protection Solutions, die Isolations- und Unveränderbarkeitsfunktionen enthalten. Bewahren Sie Backups außerhalb der Reichweite von Cyberangriffen auf und verhindern Sie, dass Ransomware sie verschlüsselt oder zerstört, damit Sie den Geschäftsbetrieb mit nicht kompromittierten Daten wiederaufnehmen und finanzielle Auswirkungen möglichst gering halten können.

Reagieren Sie sofort auf Incidents und sorgen Sie für Business Continuity mit dem Incident Response and Recovery (IRR)-Serviceteam von Dell. Das Team ist rund um die Uhr verfügbar, um auf Bedrohungen zu reagieren. Es unterstützt und begleitet Unternehmen bei der Eindämmung, Abwehr und Wiederherstellung nach einem Angriff.



Cybersicherheit und Ausfallsicherheit für das moderne Rechenzentrum

Dell Storage

Sie können sich darauf verlassen, dass Ihre Daten sicher, geschützt und verfügbar sind.

Ist es möglich, sichere Storage-Lösungen mit umfassender Bedrohungserkennung und -reaktion zu kombinieren? Absolut! Unsere Lösungen überwinden die Komplexität der Sicherheit, indem sie Threat Intelligence aggregieren und vorgelagert zu den Sicherheitsplattformen kaskadieren.

Dell Server

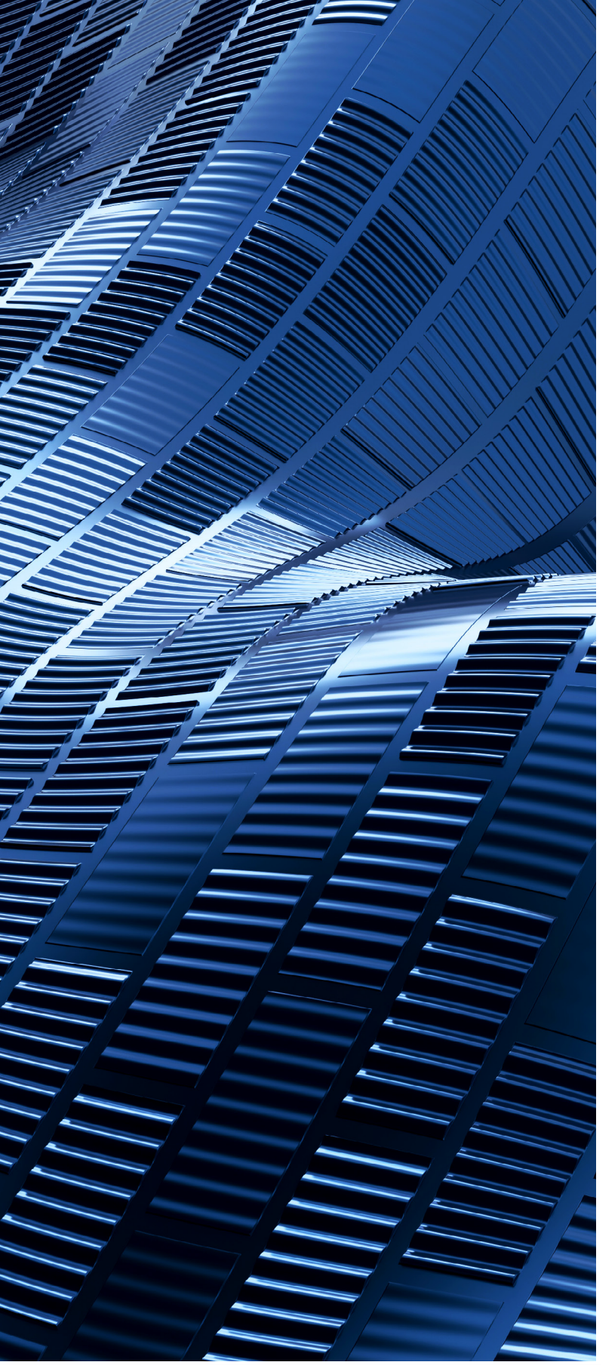
Begegnen Sie der heutigen Bedrohungslandschaft mit einer cybersicheren Architektur, die sich weiterentwickelnde Sicherheitskontrollen, -funktionen und -lösungen bereithält.

Anbieter wie AMD und Intel ermöglichen den Aufbau von Servern auf der Grundlage von Vertrauen auf Hardwareebene aufzubauen. Dies schützt Kundendaten, sorgt für Geräteintegrität von der Lieferkette über den gesamten Betriebslebenszyklus hinweg, stärkt die Ausfallsicherheit von Endpunkten und gibt Kunden die Gewissheit, dass ihre Infrastruktur vor den fortschrittlichsten Cyberbedrohungen geschützt ist.

Dell Networking

Erhöhen Sie die Sicherheit mit mehreren Verteidigungsebenen in Hardware und Software – am Edge und im Netzwerk.

Eine umfassende und anpassbare Sicherheitsstrategie ist der Schlüssel, um Vertrauen und Kontrolle in der dynamischen Unternehmenslandschaft von heute aufrechtzuerhalten. Durch die Kombination aus fortschrittlicher Architektur, strengen Sicherheitszertifizierungen, robusten Zugriffsprotokollen und nahtlosen Integrationen sorgt dieser Ansatz dafür, dass Ihr Netzwerk sicher bleibt und gleichzeitig mit höchster Leistung arbeitet.



Disaggregierte Architektur Von Dell

Profitieren Sie von der Flexibilität, Computing, Storage und Netzwerke separat zu skalieren. Dies führt zu einer besseren Ressourcenauslastung, niedrigeren Kosten und einfacheren Betriebsabläufen.

Skalieren Sie Computing-, Storage- und Netzwerkressourcen unabhängig voneinander, um mehr Effizienz zu erzielen und Kosten einzusparen und gleichzeitig eine breite Mischung von Workloads zu unterstützen. Verbessern Sie die Auslastung, optimieren Sie den Geschäftsbetrieb und das Lebenszyklusmanagement, steigern Sie die Verfügbarkeit und Ausfallsicherheit bei Cyberangriffen und sorgen Sie für zukunftssichere IT-Umgebungen, damit Unternehmen schnell auf neue Anforderungen reagieren und die Komplexität minimieren können.

Dell Cyberausfallsicherheit

Schaffen Sie eine sichere Infrastruktur mit KI-gestützter Ausfallsicherheit, damit sich Ihr Unternehmen nach destruktiven Cyberangriffen erholen kann.

Sorgen Sie für Ausfallsicherheit bei Cyberangriffen, indem Sie kritische Daten mit integrierter Unveränderlichkeit, schneller Recovery und intelligenter Bedrohungserkennung sichern. So können Sie Betriebsabläufe schnell wiederherstellen und Geschäftsunterbrechungen angesichts von Ransomware oder Cyberangriffen minimieren.

Dell AIOps

Schützen Sie Ihre Infrastruktur mit Cybersicherheitsbewertungen und schnellen Korrekturmaßnahmen.

Reagieren Sie schneller auf Sicherheitsmeldungen direkt in der Anwendung, die Administrator/innen zur Verwaltung des Zustands, der Kapazität und der Leistung der Infrastruktur verwenden. Überwachung und vorausschauende Analysen kombinieren menschliche und maschinelle Intelligenz, um Erkenntnisse zu liefern, die sicherstellen, dass Ihre IT-Infrastruktur den geschäftlichen Anforderungen entspricht.

Dell Professional Services

Vereinfachen Sie Sicherheitsabläufe durch eine automatisierte, integrierte und optimierte Erfahrung.

Erfahren Sie mehr darüber, wie Ihr Unternehmen einen ganzheitlicheren Ansatz für die Cybersicherheit verfolgen kann. Stärken Sie Ihre Umgebung mit IT-Lösungen für Ausfallsicherheit bei Cyberangriffen, indem Sie Daten und Systeme schützen, die Ausfallsicherheit bei Cyberangriffen verbessern und die Komplexität von Sicherheitseinstellungen überwinden. Mit modernen End-to-End-Lösungen von Dell Technologies erhalten Sie das Vertrauen, die Kontrolle und die Skalierbarkeit, die Sie benötigen, um Herausforderungen im Sicherheitsbereich zu bewältigen.

1 IDC Worldwide Quarterly Converged Systems Tracker, 1. Quartal 2022

Ausfallsicherheit bei Cyberangriffen zum Schutz von Innovationen

Bei Dell Technologies integrieren wir Sicherheitsvorkehrungen in alles, was wir entwickeln. Wir machen es zu unserer Aufgabe, damit dafür nicht ihre Zeit in Anspruch genommen wird.

Wir treiben den technologischen Fortschritt seit Jahrzehnten voran und wissen, was erforderlich ist, um eine Umgebung zu schaffen, in der bahnbrechende Erfolge entstehen können. Wir gehen bei der Gestaltung, Beschaffung, Herstellung, Lieferung und Verwaltung unserer Produkte gewissenhaft vor, damit Sie ihnen in Ihrer Umgebung vertrauen können – und darauf vertrauen können, dass sie ihre ambitioniertesten Initiativen unterstützen.

Wenn Sie sich für die Lösungen für Ausfallsicherheit bei Cyberangriffen von Dell entscheiden, schaffen Sie die Grundlage für Innovationen, die Ihnen einen echten Wettbewerbsvorteil bringen werden.

Aufbau einer sicheren Grundlage für Innovationen

Ausfallsicherheit bei Cyberangriffen zum Schutz der Zukunft

Weitere Informationen

DELL Technologies AMD intel