DELL Technologies

Zero Trust

Der Weg zu besserer Cybersicherheit

Machen Sie sich mit einem erfahrenen Technologie- und Sicherheitspartner auf den Weg zu Zero Trust

Unternehmen, die an der Verbesserung ihres Cybersicherheitsreifegrads arbeiten, entwickeln hierfür eine umsetzbaren Roadmap, in der Wege zur Reduzierung ihrer Angriffsfläche, zur Erkennung und Reaktion auf Cyberbedrohungen sowie zur Implementierung von Methoden zur Recovery nach Cyberangriffen identifiziert werden – all dies unter Verwendung von Zero-Trust-Funktionen.

Um den immer ausgefeilteren Cyberbedrohungen zu begegnen, nutzt Dell die in unsere Lösungen und die unserer Partner integrierten Sicherheitsfunktionen, um Kunden bei der Umsetzung von Zero Trust im Einklang mit ihren Geschäftszielen zu unterstützen.

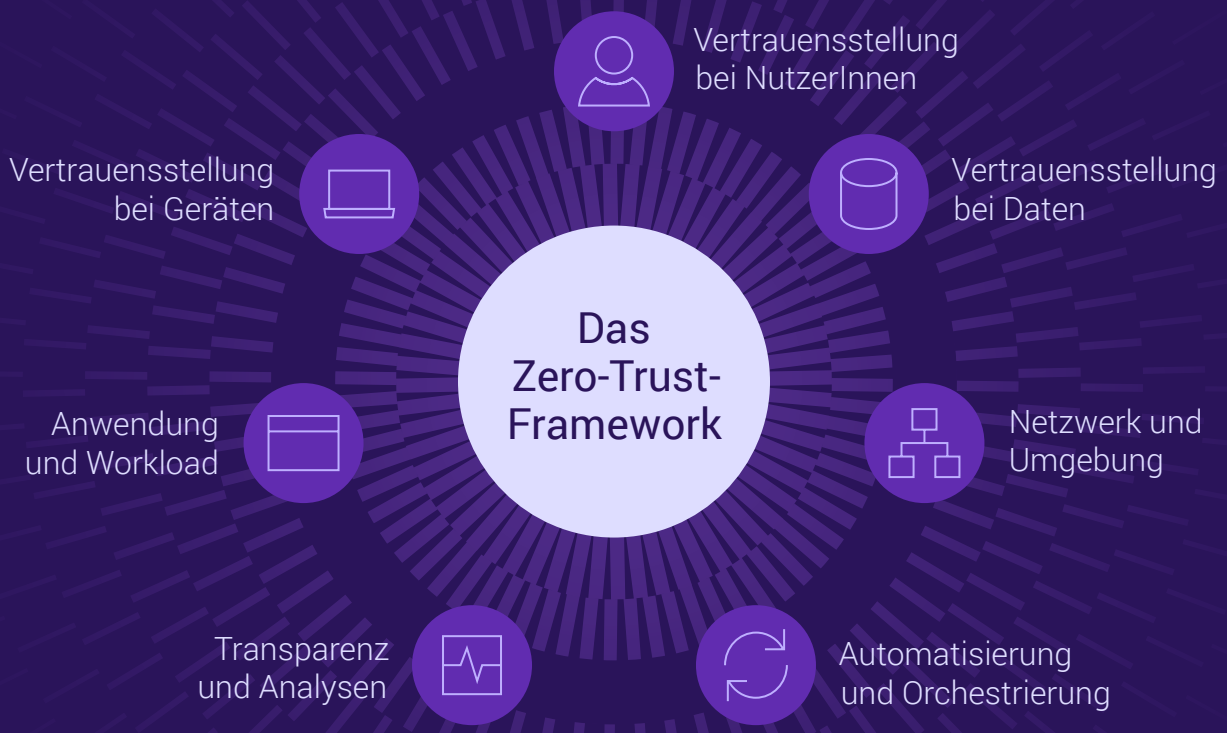
Was ist Zero Trust?

Stellen Sie sich Ihr Netzwerk als eine Burg vor. Sobald die Brücke heruntergelassen wurde und jemand die Burg betritt, kann die Person sich frei bewegen. Es ist an der Zeit, das Sicherheitsmodell der perimeterbasierten Abwehr gegen das modernere und sicherere Zero-Trust-Framework auszutauschen.

Bei Zero Trust handelt es sich um einen architektonischen Sicherheitsansatz im Gegensatz zu einem Produkt, das Sie kaufen. Der Name ist Programm: Bei Zero Trust wird niemals vertraut und immer überprüft, ob ein legitimer Geschäftszweck vorliegt, bevor Zugriff auf Ressourcen gewährt wird.
Das bedeutet, dass NutzerInnen und Geräte nicht standardmäßig als vertrauenswürdig eingestuft werden, selbst wenn sie mit einem autorisierten Netzwerk verbunden sind und bereits zuvor verifiziert wurden.

„Niemals vertrauen, immer verifizieren“

Grundlagen für ein sicheres IT-Setup



Das Zero-Trust-Framework, gemäß der Definition des US-amerikanischen National Institute of Standards and Technologies (NIST), wurde vom US-Verteidigungsministerium übernommen und in eine Architektur integriert.

Es basiert auf sieben miteinander verbundenen Säulen, die Dell Technologies in allen Sicherheitsbereichen als Orientierung dienen. Zusammen ermöglichen diese Säulen eine vielseitige, integrierte Architektur für einen umfassenden Sicherheitsansatz, der die Daten und Infrastruktur Ihres Unternehmens schützt.

Die Einführung von Zero Trust hat sich jedoch aufgrund der Komplexität, die die Integration unterschiedlicher Sicherheitsfunktionen und die Navigation durch die fragmentierten Lösungsoptionen verschiedener Sicherheitsanbieter mit sich bringen, bisher schwierig gestaltet.

NIST

U.S. Department *of* Defense

DELL Technologies

Optimieren Sie Ihren Zero-Trust-Reifegrad

Ganz gleich, wo Sie sich gerade auf Ihrem Weg befinden – Dell unterstützt Sie mit den passenden Lösungen

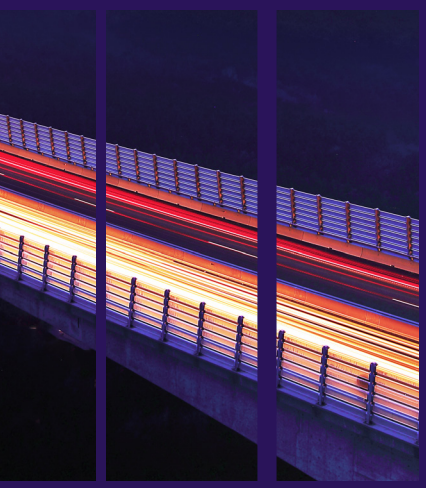
Dell Technologies eröffnet Ihrem Unternehmen Auswahlmöglichkeiten und Flexibilität. Für die Verbesserung Ihrer Cybersicherheitsreife bieten wir Ihnen Sicherheitslösungen mit Zero-Trust-Funktionen, mit denen Sie Ihre Unternehmenssicherheit verstärken und bösartige Cyberaktivitäten besser erkennen, abwehren und eine Recovery durchführen können.

Implementierung von Zero-Trust-Prinzipien

Auswahlmöglichkeiten und Flexibilität zur Verbesserung Ihrer Cybersicherheitsreife

Dell Technologies bietet Sicherheitslösungen und Zero-Trust-Funktionen, mit denen Sie Ihre Unternehmenssicherheit verstärken und bösartige Cyberaktivitäten besser erkennen, abwehren und eine Recovery durchführen können, u. a. durch:

- Integrierte Schutzmaßnahmen zur Verbesserung von Automatisierung, Threat Intelligence, Authentifizierung, Transparenz uvm.
- Services für die Entwicklung einer Roadmap, Integration wichtiger Technologien und proaktives Management zur Unterstützung von Zero Trust
- Professionelle Managed Services und Sicherheitsberatungsservices
- Ein umfangreiches Partnernetzwerk



Deutlich vereinfachte Einführung von Zero Trust

Eine vollständig integrierte Architektur für alle Bereiche

Da es sich bei Zero Trust um einen architektonischen Sicherheitsansatz und nicht um ein einzelnes Produkt handelt, ist eine sorgfältig geplante Lösungszusammenstellung erforderlich. Dell nimmt Ihnen die schwierigen Aufgaben der Zero-Trust-Integration ab. Und zwar so:

- Dell erstellt die erste und einzige vollständig integrierte Zero-Trust-Architektur, die vom US-Verteidigungsministerium entwickelt, getestet und validiert wurde.

DELL Technologies

Implementierung von Zero-Trust-Prinzipien

Erreichen Sie Zero Trust, aufbauend auf Ihrem spezifischen Sicherheits-Setup

Dell unterstützt Unternehmen bei der Verbesserung ihres Cybersicherheitsreifegrads mit Zero-Trust-Strategien, die dazu beitragen, Angriffsfläche zu reduzieren, die Erkennung zu verbessern und die Recovery nach Cyberbedrohungen zu beschleunigen.

Jede der dargestellten Zero-Trust-Säulen umfasst Technologien, Prozesse und MitarbeiterInnen für die kritischen Bereiche, in denen Sicherheits- und Geschäfts-Policys zum Schutz Ihres Unternehmens erforderlich sind. Dell Security Services unterstützen Sie in folgenden Bereichen:

- Sicherheitsreife, Zero Trust und Risikobewertungen
- Entwicklung von Strategien und Roadmaps
- Managed Services für wichtige Zero-Trust-Funktionen

DELL Technologies

Grundlagen von Zero Trust

Wir bieten moderne, integrierte Sicherheitslösungen, die Ihnen schneller den Weg zu Zero Trust ebnen

Dell Data Protection

Cyber-Recovery-Vault | PowerProtect Data Manager | CyberSense – Transparent Snapshots | Cloud IQ | Systemsperre | Abweichungserkennung | Sicheres Enterprise-Key-Management | TLS 1.3 | IPv6 | Multi-Faktor-Authentifizierung | Single Sign-On | Rollenbasierter Zugriff | Cloud IQ

Dell PowerEdge-Server

Softwarestückliste | Sichere Komponentenüberprüfung | Chipbasierte Sicherheit (Silicon Root of Trust) | Systemsperre | Abweichungserkennung | Sicheres Enterprise-Key-Management | TLS 1.3 | IPv6 | Multi-Faktor-Authentifizierung | Single Sign-On | Rollenbasierter Zugriff | Cloud IQ

Dell Storage-Plattformen

Datenisolierung | Datenunveränderlichkeit | Bedrohungserkennung | Zugriffskontrolle/ Authentifizierung | Datenverschlüsselung | STIG-Sicherheitsverstärkung | HW Root of Trust | Secure Boot | Digital signierte Firmware | Rollenbasierter Zugriff | Sichere Snapshots

Dell HCI/CI

HW Root of Trust | Vertrauenskette für Secure Boot | Digital signierte Updates | Key-Management | Sichere Protokollierung | Verteilte virtuelle Switches | VM-Isolierung | Authentifizierung und Autorisierung | Ökosystemkonnektoren | Kontinuierlich validierte Zustände | Integrität des Softwarecodes | Matrix für elektronische Kompatibilität

Dell PCs

BIOS-/Firmwaresicherheit | Hardwaresicherheit | Lieferkettensicherheit | Bedrohungsmanagementsoftware (EDR, XDR, VDR) | Data-Protection-Software für Netzwerk und Cloud

Dell Edge-Lösungen

HW/SW/VM-Bestätigung | Sicheres Onboarding | Vertrauenskette | Sichere BS-/ Anwendungsbereitstellung | Data Rights Management

Dell Network Switches

SmartFabric | Cloud IQ | SD-WAN | VLAN-Segmentierung | Enterprise-SONiC | Zugriffskontrolllisten | RADIUS | TACACS+ | Kryptografie | Verstärkter Switch-Schutz | Mikrosegmentierung | Virtuelles Routen und Weiterleiten

DELL Technologies

Unser beschleunigter Ansatz

Projekt Fort Zero ermöglicht die schnelle und gründliche ganzheitliche Integration von Zero Trust in Ihr Unternehmen.

Projekt Fort Zero bietet eine validierte Methode für die sofortige Verbesserung des Zero-Trust-Reifegrads, wodurch die Einführungszeit verkürzt, Unterbrechungen reduziert und Kosten unter Kontrolle gehalten werden.

Aufgrund unseres Fachwissens und unserer Reichweite in der Branche hat das US-Verteidigungsministerium Dell Technologies gebeten, die Einführung von Zero Trust zu beschleunigen. Um Unternehmen aus dem privaten und öffentlichen Sektor die Einführung zu erleichtern und sie bei der globalen Skalierung ihrer Zero-Trust-Architektur zu unterstützen, arbeitet Dell am Aufbau eines Ökosystems und an der Integration von mehr als 30 führenden Technologie- und Sicherheitsunternehmen. Wir sind führend in der Entwicklung und globalen Skalierung der Zero-Trust-Architektur für private und öffentliche Unternehmen weltweit. Dies zeigt das Engagement von Dell, die Ziele des US-Verteidigungsministeriums zur Erreichung von Zero Trust, umzusetzen.

On-Premise

In Rechenzentren für Unternehmen, in denen Datensicherheit und Compliance von größter Wichtigkeit sind

Remote oder lokal

An Standorten wie Einzelhandelsgeschäften, wo die sichere Echtzeitanalyse von Kundendaten Wettbewerbsvorteile bieten kann

Edge

An Orten wie Flugzeugen oder Fahrzeugen mit unregelmäßiger Konnektivität, wo die zeitweilige Implementierung für die Betriebskontinuität erforderlich ist

DELL Technologies

Wir unterstützen Sie bei der schnelleren Einführung von Zero Trust, indem wir alle **152** vom US-Verteidigungsministerium definierten Aktivitäten für eine erweiterte Zero-Trust-Ebene bereitstellen.

Optionen zur Umsetzung

Grundsätze | Organisation | Schulung | Material | Führung und Weiterbildung | Belegschaft | Einrichtungen | Policy

Zero-Trust-Zielebene

Vertrauensstellung bei NutzerInnen	Vertrauensstellung bei Geräten	Anwendung und Workload	Vertrauensstellung bei Daten	Netzwerk und Umgebung	Automatisierung und Orchestrierung	Transparenz und Analysen
Nutzerbestand	Gap-Analyse mit Geräteintegritäts-Tool	Anwendungs-/ Codeidentifizierung	Datenanalyse	Festlegung fein abgestimmter Zugriffsregeln und -Policys, Teil 1	Policy-Bestandsaufnahme und -Entwicklung	Skalierungsaspekte
App-basierte Berechtigung	Integration von AV-Tools der nächsten Generation mit C2C	Ressourcenautorisierung, Teil 1	Protokollierung und Analyse von DLP-Durchsetzungspunkten	Festlegung von SDN-APIs	Analyse der Aufgabenautomatisierung	Protokollanalysen
Regelbasierter dynamischer Zugriff, Teil 1	Gemanagtes NPE/ PKI-Gerät	Entwicklung einer DevSecOps Software Factory, Teil 1	Protokollierung und Analyse von DRM-Durchsetzungspunkten	Festlegung fein abgestimmter Zugriffsregeln und -Policys, Teil 2	Analyse der Reaktionsautomatisierung	Bestands-ID- und Warnmeldungskorrelation
Abteilungs-MFA/IDP	Gerät durch Standard-Policy ablehnen	Genehmigte(r) Binärdateien/Code	Festlegung von Daten-Tagging-Standards	Implementierung SDN-programmierbarer Infrastruktur	Analyse der Tool-Compliance	Bedrohungswarnmeldungen, Teil 1
Systemimplementierung und Managen von Nutzerberechtigungen, Teil 1	Implementierung von UEDM oder gleichwertigen Tools	Programm für Sicherheitslückenmanagement, Teil 1	Implementierung von Daten-Tagging- und -klassifizierungs-Tools	Rechenzentrum-Makrosegmentierung	Abteilungszugriffsprofil	Implementierung von Analyse-Tools
Lebenszyklusmanagement von Abteilungsidentitäten	Enterprise-Gerätemanagement, Teil 1	SDC-Ressourcenautorisierung, Teil 1	Monitoring von Dateiaktivitäten, Teil 1	Implementierung von Mikrosegmentierung	Implementierung von SOAR-Tools	Programm zur Cyber Threat Intelligence, Teil 1
NutzerInnen durch Standard-Policy ablehnen	Implementierung von EDR-Tools und Integration mit C2C	Ressourcenautorisierung, Teil 2	Implementierung von DRM- und Schutz-Tools, Teil 1	Segmentierung von Abläufen in Kontrollmanagement- und Datenebenen	Standardisierte API-Aufrufe und -Schemata, Teil 1	Konfigurationsprotokolle
Einzelauthentifizierung	Implementierung von Tools für Bestands-, Sicherheitslücken- und Patchmanagement	Entwicklung einer DevSecOps Software Factory, Teil 2	Implementierung von Durchsetzungspunkten	B/C/P/S-Makrosegmentierung	Workflow-Anreicherung, Teil 1	Bedrohungswarnmeldungen, Teil 2
Systemimplementierung und Managen von Nutzerberechtigungen, Teil 2	Enterprise-IDP, Teil 1	Automatisierung von Anwendungssicherheit und Codekorrekturen, Teil 1	Interoperabilitätsstandards	Mikrosegmentierung für Anwendungen und Geräte	Unternehmenssicherheitsprofil, Teil 1	Nutzer/Geräte-Baselines
Lebenszyklusmanagement von Unternehmensidentitäten, Teil 1	Implementierung von C2C/ Compliance-basierter Netzwerkautorisierung, Teil 1	Programm für Sicherheitslückenmanagement, Teil 2	Entwicklung einer SDS-Policy	Schutz von Daten während der Übertragung	Unternehmensintegration und Workflow-Bereitstellung, Teil 1	Festlegung des Nutzer-Baseline-Verhaltens
Implementierung von UEBA-Tools	Implementierung von Anwendungssteuerungs- und FIM-Tools	Kontinuierliche Validierung	Manuelles Daten-Tagging, Teil 1		Implementierung von Daten-Tagging- und -klassifizierungs-ML-Tools	Baseline und Profilerstellung, Teil 1
Regelmäßige Authentifizierung	Gemanagte und eingeschränkte BYOD- und IoT-Unterstützung	SDC-Ressourcenautorisierung, Teil 2	Monitoring von Dateiaktivitäten, Teil 2		Standardisierte API-Aufrufe und -Schemata, Teil 2	Programm zur Cyber Threat Intelligence, Teil 2
Enterprise-PKI/IDP, Teil 1	Enterprise-Gerätemanagement, Teil 2		Implementierung von DRM-und Schutz-Tools, Teil 2		Workflow-Anreicherung, Teil 2	
	Implementierung von XDR-Tools und Integration mit C2C, Teil 1		DLP-Durchsetzung durch Daten-Tags und -analysen, Teil 1			
			Integration von DAAS-Zugriff mit SDS-Policy, Teil 1			
			DRM-Durchsetzung durch Daten-Tags und -analysen, Teil 1			
			Integration von SDS-Lösung(en) und -Policys mit Enterprise-IDP, Teil 1			

Zielaktivitäten insgesamt: 91

Quelle: Zero-Trust-Strategie des US-Verteidigungsministeriums, 7. November 2022

DELL Technologies

Erweiterter Zero Trust

Vertrauensstellung bei NutzerInnen	Vertrauensstellung bei Geräten	Anwendung und Workload	Vertrauensstellung bei Daten	Netzwerk und Umgebung	Automatisierung und Orchestrierung	Transparenz und Analysen
Regelbasierter dynamischer Zugriff, Teil 2	Enterprise-IDP, Teil 2	Anreicherung von Attributen für Ressourcenautorisierung, Teil 1	Manuelles Daten-Tagging, Teil 2	Erkennung und Optimierung von Netzwerkbeständen	Unternehmenssicherheitsprofil, Teil 2	Bedrohungswarnmeldungen, Teil 3
Unternehmensrollen und -berechtigungen, Teil 1	Implementierung von C2C/Compliance-basierter Netzwerkautorisierung, Teil 2	Anreicherung von Attributen für Ressourcenautorisierung, Teil 2	Monitoring von Datenbankaktivitäten	Zugriffsentscheidungen in Echtzeit	Unternehmensintegration und Workflow-Bereitstellung, Teil 2	Baseline und Profilerstellung, Teil 2
Alternative, flexible MFA, Teil 1	Monitoring von Entitätenaktivitäten, Teil 1	ATO (Continuous Authorization to Operate), Teil 1	Automatisiertes Daten-Tagging und Support, Teil 1	Mikrosegmentierung von Prozessen	Implementierung von KI-Automatisierungs-Tool	UEBA-Baseline-Unterstützung, Teil 1
Echtzeit-genehmigungen und JIT/JEA-Analysen, Teil 1	Vollständige Integration von Gerätesicherheits-Slack mit C2C	Automatisierung von Anwendungssicherheit und Codekorrekturen, Teil 2	DRM-Durchsetzung durch Daten-Tags und -analysen, Teil 2		Workflow-Anreicherung, Teil 3	UEBA-Baseline-Unterstützung, Teil 2
Lebenszyklusmanagement von Unternehmensidentitäten, Teil 2	Enterprise-PKI, Teil 1	REST-API-Mikrosegmente	DLP-Durchsetzung durch Daten-Tags und -analysen, Teil 2		Analysegesteuerte KI entscheidet über A&O-Änderungen	KI-unterstützter Netzwerkzugriff
Monitoring von Nutzeraktivitäten, Teil 1	Gemanagte und vollständige BYOD- und IoT-Unterstützung, Teil 1	ATO (Continuous Authorization to Operate), Teil 2	Integration von DAAS-Zugriff mit SDS-Policy, Teil 2		Implementierung von Playbooks	KI-unterstützte dynamische Zugriffskontrolle
Kontinuierliche Authentifizierung, Teil 1	Implementierung von XDR-Tools und Integration mit C2C, Teil 2		Integration von SDS-Lösung(en) und -Policys mit Enterprise-IDP, Teil 2		Automatisierte Workflows	
Kontinuierliche Authentifizierung, Teil 2	Monitoring von Entitätenaktivitäten, Teil 2		Integration von SDS-Tool und/oder Integration mit DRM-Tool, Teil 1			
Enterprise-PKI/IDP, Teil 3	Enterprise-PKI, Teil 2		Automatisiertes Daten-Tagging und Support, Teil 2			
Unternehmensrollen und -berechtigungen, Teil 2	Gemanagte und vollständige BYOD- und IoT-Unterstützung, Teil 2		Umfassendes Monitoring von Datenaktivitäten			
Alternative, flexible MFA, Teil 2			DRM-Durchsetzung durch Daten-Tags und -analysen, Teil 3			
Echtzeit-genehmigungen und JIT/JEA-Analysen, Teil 2			DLP-Durchsetzung durch Daten-Tags und -analysen, Teil 3			
Lebenszyklusmanagement von Unternehmensidentitäten, Teil 3			Integration von DAAS-Zugriff mit SDS-Policy, Teil 3			
Monitoring von Nutzeraktivitäten, Teil 2			Integration von SDS-Tool und/oder Integration mit DRM-Tool, Teil 2			
Enterprise-PKI/IDP, Teil 2						

Erweiterte Aktivitäten insgesamt: 61

Dell Technologies vereinfacht die komplexen Abläufe zum schnellen Erreichen eines Zero-Trust-Reifegrads.

Quelle: Zero-Trust-Strategie des US-Verteidigungsministeriums, 7. November 2022

DELL Technologies

Die passenden Lösungen für alle Unternehmensanforderungen

Optimieren Sie Ihren Zero-Trust-Reifegrad

Zero Trust ist ein definiertes Framework mit einer Reihe von Prinzipien, die als Leitlinien für Sicherheitsansätze dienen und mit einer Vielzahl von Funktionen implementiert werden können. Unabhängig davon, ob Sie sich auf ein umfassendes Zero-Trust-Modell oder auf gezielte Verbesserungen auf Basis der Zero-Trust-Prinzipien konzentrieren – Dell ist Ihr erfahrener Sicherheitspartner, der Sie bei der Weiterentwicklung Ihrer Sicherheitsstrategie unterstützt.

Chemieindustrie	Informations-technologie	Kommunikation	Rettungsdienste
Lebensmittel und Landwirtschaft	Verteidigung	Gesundheitswesen und öffentliche Gesundheit	Fertigung
Finanzielles	Kernreaktoren	Commercial	Behörden
Energie	Transportwesen	Wasser und Abwasser	Dämme

DELL Technologies

DELL Technologies

Ein erfahrener Technologie- und Sicherheitspartner, der Ihr Unternehmen auf dem Weg zu Zero Trust unterstützt und begleitet

Verbessern Sie mit Zero Trust Ihre langfristige Cybersicherheit.

Dell Security Services bieten:

- Bewertung des Sicherheitsreifegrads und des Gesamtrisikos durch Experten
- Entwicklung einer Zero-Trust-Roadmap
- Laufendes Management von Sicherheitsaktivitäten

DELL Technologies

Dell.com/SecuritySolutions

Rückruf anfordern

Mit unseren SicherheitsberaterInnen chatten

Telefon: 1-800-433-2393