# Wie intrinsische Sicherheit vor Betriebsstörungen schützt

DELL Technologies

vmware

# Inhaltsverzeichnis



# Betriebsstörungen sind normal

Wenn es um die IT geht, sind Störungen ganz alltäglich. Von der Abwehr von Cyberangriffen bis hin zur Integration von Spitzentechnologien – in den Unternehmen von heute ist „Business as usual“ keine Selbstverständlichkeit mehr.

Doch selbst eine Abteilung, die auf Störungen eingestellt ist, war möglicherweise nicht auf alles vorbereitet, was sich in letzter Zeit in der Welt ereignet hat. Fast über Nacht mussten große und kleine Unternehmen Policies für das Arbeiten und Lernen von zu Hause aus einführen, ihre Business-Continuity-Strategien überdenken und ihre Betriebsmodelle neu erfinden, um ihr Geschäft am Laufen zu halten. Diese Unternehmen wandten sich an ihre IT-Teams, um all das zu ermöglichen.

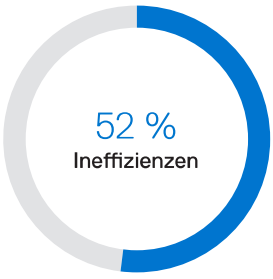
Millionen von Mitarbeitern arbeiten jetzt mobil, die es vorher nicht taten. Da ihre Desktop-PCs in einigen Fällen immer noch im Büro stehen, verwenden die Mitarbeiter möglicherweise auch ihre privaten Geräte, um eine Verbindung zum Unternehmensnetzwerk herzustellen und ihre Arbeit zu erledigen. Angesichts der zunehmenden Akzeptanz dieser „neuen Normalität“ werden viele dieser Mitarbeiter und ihre Unternehmen auch in Zukunft die Flexibilität des ortsunabhängigen Arbeitens bevorzugen.

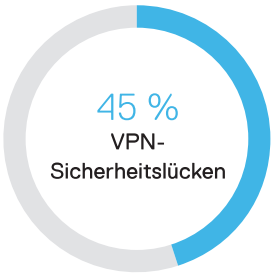
Doch wenn die Mitarbeiter nicht mehr unter dem wachsamen Auge der IT-Abteilung stehen, wird die Sicherheit eine noch größere Bedeutung erlangen. Im Jahr 2020 verzeichneten Unternehmen eine Zunahme von Cyberangriffen, die auf ahnungslose Mitarbeiter abzielten, die mit ungeschützten privaten Geräten arbeiten, wobei Ransomwareangriffe im März 2020 im Vergleich zum Februar 2020 um 148 % zunahmen.[1] Die IT-Teams waren auf den Ansturm von Mitarbeitern, die von zu Hause aus arbeiten, nicht vorbereitet, was ihre Fähigkeit, das Unternehmen zu schützen, beeinträchtigte. IT-Experten nannten Ineffizienz beim Remotezugriff (52 %), VPN-Sicherheitslücken (45 %) und Personalmangel (36 %) als ihre größten Endpoint-Security-Herausforderungen beim Umgang mit Cyberangriffen.[2]

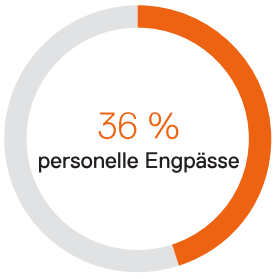
In einer Welt, in der bereits 7 Mio. Datensätze pro Tag kompromittiert werden, ist Sicherheit in einer ortsunabhängigen Arbeitswelt so wichtig wie nie.[3] Aber wenn der aktuelle Sicherheitsansatz nicht funktioniert, was dann?

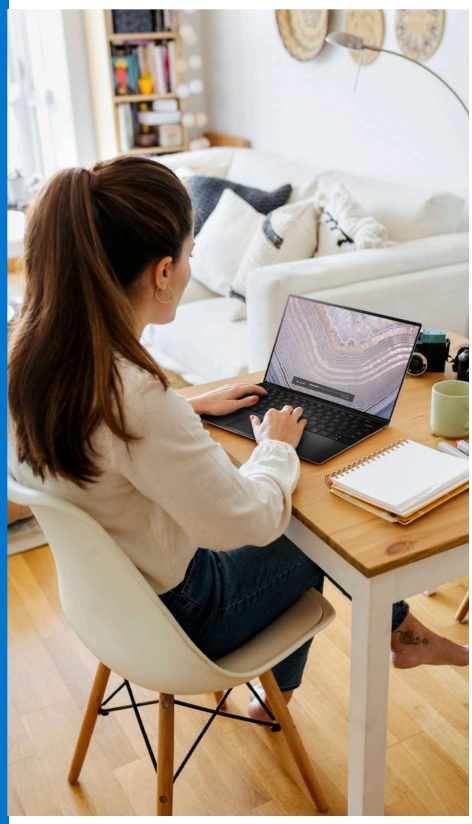
**CYBERANGRIFFE IN ZAHLEN**

148 %
Gesamtanstieg der Ransomwareangriffe im März 2020





# Intrinsische Sicherheit: Ein neuer Ansatz zur Verbesserung der Sicherheit

In der Vergangenheit wurde die Cybersicherheit nachträglich hinzugefügt, um bereits vorhandene Hardware und Software zu schützen. Aber das Hinzufügen immer neuer Sicherheitsschichten zu bestehender Technologie ist weder skalierbar noch verwaltbar. Dies gilt vor allem dann, wenn Trends wie mobiles Arbeiten, Bring Your Own Device, Cloud, künstliche Intelligenz, 5G und das Internet der Dinge die Anzahl potenzieller Datensicherheitslücken in jeder Facette des Unternehmens erhöhen.

Die Herausforderungen von heute und die Anforderungen an die Cybersicherheit von morgen lassen sich nicht mit dem Denken von gestern bewältigen. Es ist ein ganzheitlicher, integrierter Ansatz erforderlich, der intelligent und automatisiert ist, um sich schnell an alle unerwarteten Veränderungen anzupassen. Dell Technologies nennt diesen Ansatz „intrinsische Sicherheit".

Intrinsische Sicherheit ist kein Tool oder Produkt: Es ist eine Strategie zur Integration von Sicherheit in die grundlegende Ebene Ihrer Technologie – unterhalb des Betriebssystemlevels –, sodass Sicherheit der erste Schritt beim Aufbauen Ihrer Infrastruktur ist, nicht der letzte. Intrinsische Sicherheit berücksichtigt Nutzer, IDs, Geräte, Assets und Daten in Echtzeit über jede App oder Cloud hinweg, sodass Sie Risiken erkennen und Bedrohungen in der Größenordnung des heutigen digitalen Betriebs verhindern können.

Dadurch, dass Sie die Sicherheit tiefer in den Technologielösungen Ihres Unternehmens verankern, können Sie mit einem intrinsischen Sicherheitsansatz, beim Managen der Cybersicherheitsanforderungen Ihres Unternehmens proaktiv statt reaktiv agieren.

## Die Prinzipien der intrinsischen Sicherheit

Ein intrinsischer Sicherheitsansatz setzt sich aus 3 Grundprinzipien zusammen:

### Integriert

Ein intrinsischer Sicherheitsansatz baut Sicherheitskontrollen direkt in die Infrastruktur ein und ermöglicht es den Geschäftseinheiten, schnell zu skalieren, ohne dass die Sicherheitsanforderungen an letzter Stelle stehen.

### Einheitlich

Intrinsische Sicherheit beseitigt Silos zwischen IT- und Sicherheitsteams, indem sie es beiden Teams ermöglicht, dieselben Produkte und Tools zu verwenden. Dies erhöht die Zusammenarbeit, ermöglicht die effizientere Nutzung knapper Sicherheitsressourcen und sorgt für eine einheitlichere Reaktion auf neue Sicherheitslücken und aktive Bedrohungen.

### Kontextbezogen

Intrinsische Sicherheit liefert den Kontext, den Sie benötigen, um sowohl die Bedrohungen, denen Sie ausgesetzt sind, als auch die Endpunkte, Workloads, Netzwerke und Clouds, die Sie schützen, zu verstehen. Dieser Kontext ermöglicht es Ihnen, neuen Bedrohungen für Ihre wichtigsten Ressourcen auf intelligente Weise vorzubeugen und darauf zu reagieren, sodass Sie intelligentere Entscheidungen darüber treffen können, wie Sie Ihre Umgebung schützen.

# Der intrinsische Sicherheitsansatz von Dell Technologies

Der Bedarf an intrinsischer Sicherheit ist die Grundlage dafür, wie Dell Technologies Produkte herstellt, entwirft und liefert.

Er beginnt mit der Gewährleistung einer sicheren Lieferkette. Wenn ein böswilliger Akteur Komponenten manipuliert, Malware einbettet oder während des Herstellungsprozesses Sicherheitslücken in die Firmware einfügt, entstehen grundlegende Sicherheitslücken, die nicht erkannt werden können, bis es zu spät ist. Aus diesem Grund umfasst der Herstellungsprozess von Dell Technologies mehrere Kontrollschichten, um jegliche Risiken zu minimieren, die in die Lieferkette eingebracht werden könnten, wobei manipulationssichere Siegel sicherstellen, dass das Gerät in einem unverfälschten Zustand ankommt. Von sicheren Fabriken bis hin zu Logistik- und Versandsicherheitsprogrammen erfüllt das Programm für eine sichere Lieferkette von Dell Technologies die höchsten Standards für die Integrität der Lieferkette.

Darüber hinaus werden die Produkte von Dell Technologies unter Einsatz von Maßnahmen für einen sicheren Entwicklungslebenszyklus entwickelt, um die Sicherheit zu einem integralen Bestandteil des gesamten Designprozesses zu machen. Proaktive Sicherheitstests während der gesamten Entwicklung reduzieren die Möglichkeit, Malware oder Sicherheitslücken in die Software einzubetten, während Sicherheitstechniker in den Produktentwicklungsprozess von Dell Technologies integriert sind, um sicherzustellen, dass die Lösungen von Grund auf für eine intrinsische Sicherheit entwickelt wurden.

Als Hardwarehersteller ist Dell Technologies in der Lage, eine einzigartige Position in der Infrastrukturumgebung zu nutzen, um erweiterte Sicherheitsfunktionen zu entwickeln, die nicht von Software repliziert werden können. Gezielte Angriffe auf das BIOS eines PCs können es Hackern beispielsweise ermöglichen, alle Endpoint-Security-Funktionen eines Geräts zu kompromittieren. Die Lösungen von Dell Technologies helfen Ihnen, Ihr BIOS zu schützen, indem sie chipbasierte Sicherheit und kryptografische Root of Trust verwenden, um das Booten des Servers und Firmwareupdates zu authentifizieren und sicherzustellen, dass das BIOS nicht verändert oder manipuliert werden kann. Darüber hinaus bietet die Off-Host-Verifizierung die Gewissheit, dass die Systeme nicht kompromittiert wurden, während flexible Reimaging-Optionen es Ihnen ermöglichen, ein beschädigtes BIOS zu analysieren, um den Angriff besser zu verstehen und zu verhindern.

Ein weiteres Beispiel ist Dell SafeID, das zum Schutz Ihrer Abläufe beiträgt, indem es die Nutzerzugangsdaten vom Betriebssystem und dem Arbeitsspeicher isoliert. Stattdessen erfolgt die gesamte Speicherung und Verarbeitung von Zugangsdaten auf einem speziellen Sicherheitschip. Diese einzigartige, hardwarebasierte Sicherheitslösung schützt Endnutzerzugangsdaten wie Kennwörter, biometrische Vorlagen und Sicherheitscodes und hindert Angreifer daran, Nutzerzugangsdaten zu stehlen, die ihnen einen umfassenden Zugriff auf das Netzwerk ermöglichen würden.

# Verwenden der Lösungen von Dell Technologies für intrinsische Sicherheit

Lösungen von Dell Technologies enthalten fortschrittliche Sicherheitsfunktionen. Insbesondere in Zusammenarbeit mit VMware können diese Lösungen genutzt werden, um die allgemeine Sicherheitslage im gesamten Unternehmen zu verbessern. Hier finden Sie einige Beispiele:

**Netzwerklösungen von Dell EMC**
Das Dell EMC Netzwerkportfolio macht es noch einfacher, die Anforderungen moderner Workloads mit integrierten Hardware- und Softwarelösungen für virtualisierte Netzwerkfunktionen zu erfüllen. Die PowerSwitch-Switches sind beispielsweise so konzipiert, dass sie architektonische Flexibilität für den Betrieb von Rechenzentren mit Softwaredesign bieten, während die Dell EMC SD-WAN-Lösung mit Technologie von VMware zweckmäßige Netzwerk-Appliances mit führender SD-WAN-Software zu einer einfachen und dennoch leistungsstarken All-in-one-Lösung kombiniert. Gemeinsam bieten Hardware und Software von Dell Technologies eine höhere geschäftliche Flexibilität, eine höhere Produktivität durch Automatisierung und eine geringere Komplexität für IT-Teams.

**VMware Carbon Black Cloud**
Als Cloud-native Endgeräteverwaltungsplattform nutzt VMware Carbon Black Cloud Verhaltensanalysen, um Bedrohungen proaktiv zu erkennen und Verhaltensmuster von Angreifern aufzudecken. VMware Carbon Black Cloud analysiert täglich mehr als eine Billion Sicherheitsereignisse in der Kundenbasis von Dell Technologies. So können Sie gefährdete Nutzer, Endpunkte und Anwendungen identifizieren und isolieren, bevor ein Angriff die Gelegenheit hat, sich in Ihrem Netzwerk auszubreiten.

**VMware NSX**
Mit der Fähigkeit zur Mikrosegmentierung können IT-Teams mit VMware NSX granulären Schutz für die einzelne Workload bereitstellen. Mit diesem Ansatz können Sie bestimmte Firewallregeln auf bestimmte Workloads anwenden, statt alle Regeln auf den gesamten Datenverkehr anzuwenden, wodurch Ihr Sicherheitsansatz effizienter wird. Außerdem können Sie damit East-West Traffic sichern, um sich gegen die seitliche Ausbreitung von Malware zu schützen und gleichzeitig die Sichtbarkeit und die blinden Flecken der Sicherheit zu beseitigen. Diese Netzwerkvirtualisierungsplattform wird von Unternehmen eingesetzt, um Anwendungen über Rechenzentren, Multi-Cloud-, Bare-Metal- und Containerinfrastrukturen hinweg zu verbinden.

**Dell EMC PowerEdge-Serverportfolio**
PowerEdge-Server bieten hohe Performance für eine Vielzahl von Workloads vom Edge über die Cloud bis zum Core. Neben der Verwendung einer chipbasierten Sicherheit für Hardware zur Validierung der BIOS-Firmware automatisieren diese Server viele der manuellen Routineaufgaben, die zu Konfigurationsfehlern und Sicherheitslücken führen können. Die integrierte intelligente Automatisierung während des gesamten Serverlebenszyklus bietet eine tiefe Sicherheitsschicht und hilft IT-Teams, schnell und zuverlässig zu skalieren.

**VMware Workspace ONE**
Die intelligenzgesteuerte digitale Arbeitsplatzplattform von Dell Technologies integriert Zugriffskontrolle, Anwendungsmanagement und Multiplattformmanagement in einer einzigen Plattform. Dadurch erhält die IT-Abteilung vollständige Transparenz und konsolidiert gleichzeitig Managementsilos, um konsistente Prozesse und Policies zu erstellen und bereitzustellen, zusammen mit einem Over-the-Air-Management in Echtzeit für alle Geräte und Betriebssysteme. Mit der kontinuierlichen Überprüfung von Nutzern, Geräten und Anwendungen trägt Workspace ONE dazu bei, den Zero-Trust-Zugriff Realität werden zu lassen.

**Dell Technologies Unified Workspace**
Dieses Lösungsportfolio erleichtert die Bereitstellung, das Management und den Support von PCs auf sichere Weise, ganz gleich, wo die Mitarbeiter arbeiten. Anwendungen können mit VMware Workspace ONE werkseitig bereitgestellt werden, wodurch sichergestellt wird, dass die Geräte mit allen erforderlichen Sicherheitsprotokollen direkt an Remotemitarbeiter ausgeliefert werden. Bei der Skalierung von Remotemitarbeitern kann die IT-Abteilung mit Unified Workspace sicherstellen, dass die Mitarbeiter zu Hause mit vertrauenswürdigen Geräten arbeiten, ohne Zeit und Arbeit für das Auspacken, die Bereitstellung und den Versand von Geräten aufwenden zu müssen.

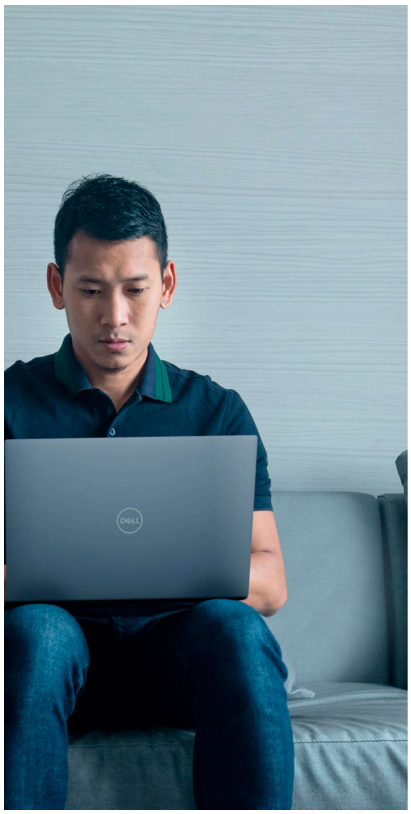
**Vertrauenswürdige Geräte von Dell für Endpoint Security**
Der umfassende Ansatz von Dell Technologies für Endpoint Security bietet integriertes Sicherheits- und Bedrohungsmanagement, um den sichersten PC der Branche bereitzustellen, durch:[4]

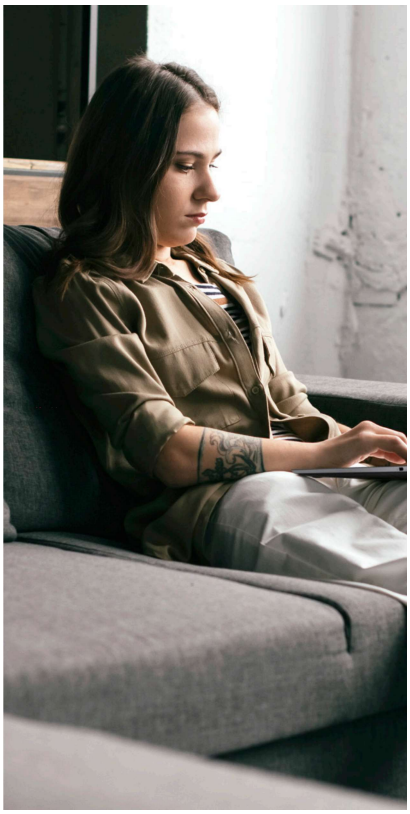
- Proaktive Erkennung und Blockierung von Endpunktangriffen und Bereitstellung von Sicherheitsexperten für die Suche nach und Beseitigung von Bedrohungen auf Endgeräten, im Netzwerk und in der Cloud
- Sichere Zusammenarbeit von Nutzern durch Verschlüsselung vertraulicher Daten auf Endgeräten und gleichzeitiger Sicherung von Informationen in der Cloud
- Bereitstellung einer Off-Host-BIOS-Verifizierung zur Minderung des Risikos von BIOS-Manipulationen auf Endgeräten
- Schutz vor Malwareangriffen durch einen exklusiven Sicherheitschip, der die Zugangsdaten für die Nutzerauthentifizierung von potenziellen Angreifern fernhält

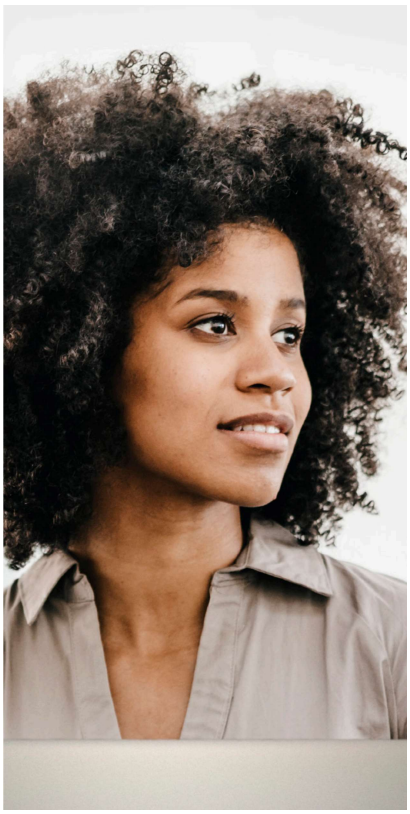
# Sicherheit auf ganz neuem Level

Mit einem intrinsischen Sicherheitsansatz können Sie die Sicherheit dort verankern, wo sie sein muss: an der Basis Ihres Unternehmens. Dell Technologies kann Sie dabei unterstützen, Ihre Infrastruktur zu nutzen, um Ihre Geräte, Apps und Nutzer von Schwachstellen in Schutzpunkte zu verwandeln.

Erfahren Sie, wie Dell Technologies einen digitalen Arbeitsplatz ermöglicht, damit Mitarbeiter von überall aus arbeiten und lernen können.







# Quellen

[1] Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted, Jim Treinen, VMware Carbon Black, 15. April 2020.

[2] Global Incident Response Threat Report, VMware Carbon Black, August 2020.

[3] The World in Data Breaches, Varonis, 2020.

[4] Basierend auf einer Analyse von Dell Technologies, Januar 2020.