DELL Technologies

Dell Trusted-Devices

Die branchenweit sichersten PCs[1]

Dell Technologies ist sich der Tatsache bewusst, dass zu den heutigen Sicherheitsherausforderungen auch das Management einer sich weiterentwickelnden Bedrohungslandschaft innerhalb einer modernen Arbeitsumgebung gehört. Cyberkriminelle nutzen ausgeklügelte Angriffe, die auf mehrere Sicherheitslücken abzielen. Eine effektive Endpoint Security-Strategie muss die gesamte Angriffsoberfläche schützen. Deshalb verfolgt Dell einen umfassenden Ansatz zur Sicherung von Geräten ober- und unterhalb des Betriebssystems, um eine optimale Ausfallsicherheit und vertrauenswürdige Geräte anbieten zu können.

Oberhalb des BS:
Integrierte Sicherheit ist Teil des Plans.

Unterhalb des BS:
Intrinsische Sicherheit ist im Design integriert.

Mit **Dell SafeGuard and Response** können Sie Cyberangriffe verhindern, erkennen und darauf reagieren.

Schützen Sie Daten auf dem Gerät und in der Cloud mit **Dell SafeData**.

Erkennen Sie BIOS-Manipulationen mit **Dell SafeBIOS**.

Vertrauen Sie darauf, dass die Hardware bei der Lieferung mit **Dell SafeSupply Chain** manipulationssicher ist.

Sichern Sie Nutzerzugangsdaten mit **Dell SafeID**.

Schützen Sie vertrauliche Informationen mit **Dell SafeScreen** und **Dell SafeShutter**.

Intelligentere und schnellere Erfahrungen durch unsichtbaren und nahtlosen Schutz

Dell Trusted-Devices bieten eine sichere Grundlage für die mobilen MitarbeiterInnen von heute. Unsere umfassende Produktreihe von Endpoint Security-Lösungen ist aufeinander abgestimmt, um die Geräte sowohl oberhalb als auch unterhalb des Betriebssystems zu schützen. Diese leistungsstarke Kombination sorgt für Datensicherheit und Produktivität der AnwenderInnen – und zwar standortunabhängig.

Oberhalb des BS

Vereiteln Sie ausgeklügelte Cyberangriffe mit Dell SafeGuard and Response.

Das Dell SafeGuard and Response-Portfolio, das von VMware® Carbon Black und Secureworks® unterstützt wird, bietet einen umfassenden Ansatz für das Bedrohungsmanagement im Zusammenhang mit Endpunkten. Künstliche Intelligenz und maschinelles Lernen erkennen und blockieren Endpunktangriffe proaktiv, während SicherheitsexpertInnen dabei helfen, identifizierte Bedrohungen am Endpunkt, im Netzwerk und in der Cloud aufzudecken und abzuwehren.

Schützen Sie Daten auf dem Gerät und in der Cloud mit Dell SafeData.

Unterstützen Sie NutzerInnen bei der standortunabhängigen, sicheren Zusammenarbeit. Dell Encryption bietet umfassende Sicherheitsfunktionen zur Verschlüsselung aller Daten auf der Festplatte, also von freigegebenen Daten mehrerer NutzerInnen und von individuellen Nutzerdaten mit mehreren Verschlüsselungsschlüsseln, die alle von einem einzelnen Dashboard verwaltet werden, um den Complianceanforderungen zu entsprechen. Netskope verfolgt einen datenzentrierten Ansatz für Cloud-Sicherheit und -Zugriff, der Daten und NutzerInnen überall schützt, während Absolute der IT Transparenz, Schutz und Persistenz außerhalb der Unternehmensfirewall bietet.

Unterhalb des BS

Erkennen Sie BIOS-Manipulationen mit Dell SafeBIOS.

BIOS-Angriffe sind bekanntermaßen schwierig zu identifizieren. Dell SafeBIOS warnt Sie vor BIOS-Manipulationen, damit Sie das Gerät schnell isolieren und untersuchen können. Mit der exklusiven, vom Host unabhängigen Verifizierung von Dell bleibt das Vergleichs-Image an einem geschützten und separaten Ort für forensische Untersuchungen nach dem Angriff erhalten.[1]

Vertrauen Sie darauf, dass die Hardware bei der Lieferung mit Dell SafeSupply Chain manipulationssicher ist.

In Dell Trusted-Devices sind branchenführende Lieferkettensicherheit sowie Integritätskontrollen integriert. Die manipulationssicheren Siegel sorgen dafür, dass das Gerät beim Eintreffen frei von Manipulationen ist. Bei hochwertigen Systemen können Sie die Festplatte auf die NIST-Spezifikationen zurücksetzen, um ein manipulationsfreies Image Ihres Unternehmens sicherzustellen.

Sichern Sie Nutzerzugangsdaten mit Dell SafeID.

Nur Dell sichert Nutzerzugangsdaten auf einem speziellen Sicherheitschip. So bleiben sie vor Malware geschützt, die darauf ausgelegt ist, Zugangsdaten zu stehlen.[1]

Schützen Sie vertrauliche Informationen mit Dell SafeScreen und Dell SafeShutter.

Unterstützen Sie NutzerInnen dabei, von überall aus zu arbeiten und ihre vertraulichen Informationen zu schützen.

Weitere Informationen finden Sie unter: Delltechnologies.com/endpointsecurity oder kontaktieren Sie Ihren Dell Endpoint Security Specialist noch heute unter endpointsecurity@dell.com.

[1] Basierend auf internen Analysen von Dell, Januar 2020.

Veröffentlicht in Deutschland 10/21 Lösungsübersicht