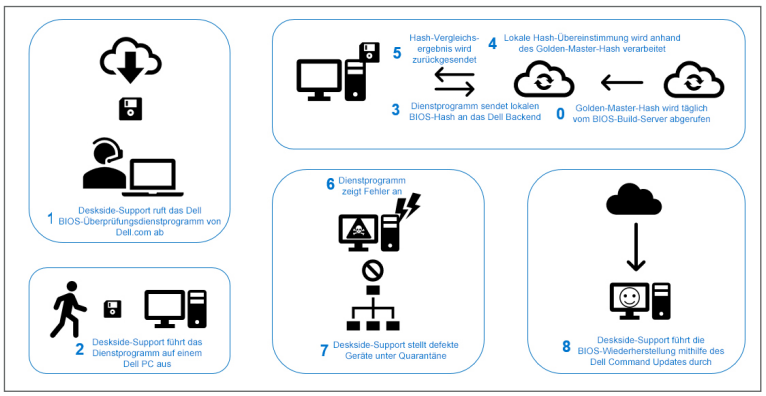
Dell SafeBIOS

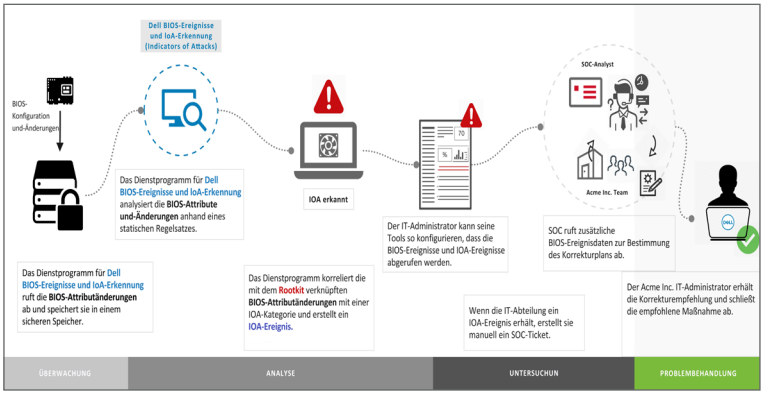
INTEGRIERTE SICHERHEIT AUF DEN BRANCHENWEIT SICHERSTEN PCS FÜR UNTERNEHMENSKUNDEN

DELL SAFEBIOS VERRINGERT DURCH INTEGRIERTE FIRMWARE-ANGRIFFSERKENNUNG DAS RISIKO VON BIOS-MANIPULATIONEN

Verbesserte BIOS-Manipulationswarnung
Das Schützen von Unternehmensdaten ist grundlegend für die Datensicherheit, unabhängig davon, ob es sich dabei um geistiges Eigentum oder um persönliche Daten des Kunden handelt. Da alltägliche Bedrohungen immer häufiger vereitelt werden, suchen Cyberkriminelle nach fortgeschritteneren Wegen, um an diese wichtigen Informationen zu kommen, und werden dabei immer raffinierter. Dank immer ausgefeilteren Endpoint-Security-Lösungen wie Virenschutz der nächsten Generation und Managed Endpoint Detection and Response nimmt die Zahl der Angriffsvektoren ab und Hacker sind gezwungen, nach alternativen Angriffspunkten zu suchen.



Der Schutz des BIOS ist entscheidend für die Sicherheitsstrategie eines Unternehmens.
Gängige Endpoint-Security-Lösungen konzentrieren sich hauptsächlich auf das lokale Betriebssystem und die darüber liegenden Anwendungen. Dadurch bleibt die unterste Stufe des PC-Stacks, das BIOS, anfällig für böswillige Angriffe, die das gesamte System außer Kraft setzen können. Wenn sich Malware die Kontrolle über das BIOS verschafft, kontrolliert sie auch den PC und seinen Netzwerkzugang. Ist das BIOS befallen, sind die Auswirkungen häufig gravierend, da sich der Eindringling in der grundlegenden Integritätsbasis für den PC festsetzt. Wenn ein Angreifer Zugriff auf das BIOS erlangt, kann er die Endpoint-Security-Funktionen dieses Geräts sowie das gesamte Netzwerk des Unternehmens gefährden.



Ein solcher Angriff ist technisch sehr anspruchsvoll und hat ein enormes Schadpotenzial. Diese klaffende Sicherheitslücke wird zu einem zunehmend gravierenden Problem, da die Angreifer nach neuen Angriffsvektoren suchen.

Dell SafeBIOS reagiert auf diesen Paradigmenwechsel in Sachen Sicherheit.
Angesichts der zunehmenden Häufigkeit von BIOS-spezifischen Angriffen und neuen Malwarevarianten, die fähig sind, sich im BIOS neu zu installieren, benötigen Unternehmen eine ausgefeiltere Möglichkeit, um nicht nur ihre Systeme zu schützen, sondern um gleichzeitig sicherzustellen, dass ihre Systeme nicht bereits infiziert sind.

Dell integriert Post-Boot-Verifizierung in seine kommerziellen PCs und gibt der IT dadurch die Gewissheit, dass das BIOS der Mitarbeiter nicht modifiziert wurde. Anstatt BIOS-Informationen auf der für Angriffe anfälligen Hardware selbst zu speichern, bietet Dell SafeBIOS eine Off-Host-BIOS-Verifizierungsfunktion. SafeBIOS verwendet eine sichere Cloud-Umgebung, um ein einzelnes BIOS-Image mit den im BIOS-Labor gespeicherten offiziellen Messdaten abzugleichen.

Dell SafeBIOS

Darüber hinaus automatisiert Dell die Früherkennung von BIOS Events, Angriffsindikatoren und risikoreichen Konfigurationen, indem die BIOS-Konfigurationshistorie sichtbar gemacht wird. Durch die kontinuierliche Extraktion und Analyse von BIOS-Konfigurationen und -Ereignissen werden gefährdete Endpunkte sichtbar und die IT wird bei erhöhtem Risiko benachrichtigt, damit sie Maßnahmen zur Eindämmung einleiten kann.

Sollte das BIOS beschädigt oder manipuliert werden, bietet Dell seinen Kunden flexible Reimage-Optionen. Durch die Analyse des kontaminierten BIOS wird die Art des Angriffs klar. Dies ermöglicht den Kunden, die BIOS-Integrität mithilfe des Off-Host-Prozesses zu überprüfen, ohne den Startvorgang zu unterbrechen. SafeBIOS sorgt für mehr Transparenz bei BIOS-Änderungen und bietet zusätzliche Sicherheit, um Bedrohungen fernzuhalten.

Sollte ein BIOS infiziert sein, wird das BIOS-Image automatisch für die Analyse und Korrektur erfasst, nachdem der BIOS-Recovery-Prozess durchlaufen wurde.

Partnerintegration
Diese Funktionen bieten in Kombination die Möglichkeit, potenzielle Risiken schneller zu erkennen und zu beheben. Die Standalone-Funktion ist derzeit über den Dell Support verfügbar.

VMware Workspace One bietet dem IT-Management neuartige Einblicke in den BIOS-Status für eine einheitliche Endgeräteverwaltung (Unified Endpoint Management, UEM). Durch die Integration mit VMware Workspace One kann die IT automatisierte Workflows einrichten, um automatische Over-the-Air-Updates bereitzustellen und die Geräte-Compliance sicherzustellen.

Die kombinierte Leistung von VMware Carbon Black Audit and Remediation und Dell SafeBIOS bietet modernste Sicherheit sowohl oberhalb als auch unterhalb der BS-Ebene und ermöglicht Telemetriefunktionen anhand des vom Host unabhängigen BIOS-Verifizierungsstatus für Dell PCs. Mit der integrierten Lösung können Sicherheits- und IT-Teams das Reporting des Verifizierungsstatus automatisieren und so Maßnahmen ergreifen, um durch BIOS-Manipulationen entstandene Schäden zu korrigieren. Diese Partnerschaft verstärkt die Position von Dell als Anbieter der sichersten PCs der Branche.

Dell SafeBIOS ist Teil des Dell Trusted Devices-Portfolios für Endpoint Security mit Lösungen, die Endpunkte sowohl oberhalb als auch unterhalb der Betriebssystemebene unterstützen und dadurch einen umfassenden Data-Protection-Ansatz liefern, einschließlich:

- SafeBIOS: Erhalten Sie Einblick in versteckte und drohende Angriffe mit BIOS-Manipulationsalarm – über die exklusive Dell Off-Host BIOS-Verifizierung[1], BIOS Image Capture, BIOS Events und IoA.
- SafeID: Nur Dell sichert Endnutzerzugangsdaten in einem speziellen Sicherheitschip. So bleiben sie vor Malware verborgen, die dafür ausgelegt ist, Zugangsdaten zu stehlen.
- SafeScreen: Endnutzer können überall arbeiten, und vertrauliche Daten bleiben dank einem integrierten digitalen Blickschutzfilter auch wirklich vertraulich.
- SafeData: Schützen Sie sensible Daten auf dem Gerät, um Compliance-Bestimmungen zu erfüllen, und sichern Sie Informationen in der Cloud. So sorgen Sie dafür, dass Ihre Endnutzer jederzeit sicher zusammenarbeiten können.
- SafeGuard and Response (von VMware Carbon Black und SecureWorks): Vorbeugung, Erkennung und Reaktion auf fortgeschrittene Malware- und Cyber-Angriffe, damit Sie produktiv weiterarbeiten können – frei von den Unterbrechungen und Abwanderungen, die ein Angriff verursachen kann.

Wenden Sie sich noch heute an Ihren Dell Endpoint Security Specialist unter endpointsecurity@dell.com. Gerne besprechen wir mit Ihnen, wie wir Sie dabei unterstützen können, Ihre Sicherheitsstrategie zu verbessern.

[1] Basierend auf interner Analyse.