DATENBLATT

WatchGuard Full Encryption

Die erste Verteidigungslinie für einfachen und effektiven Schutz von Daten

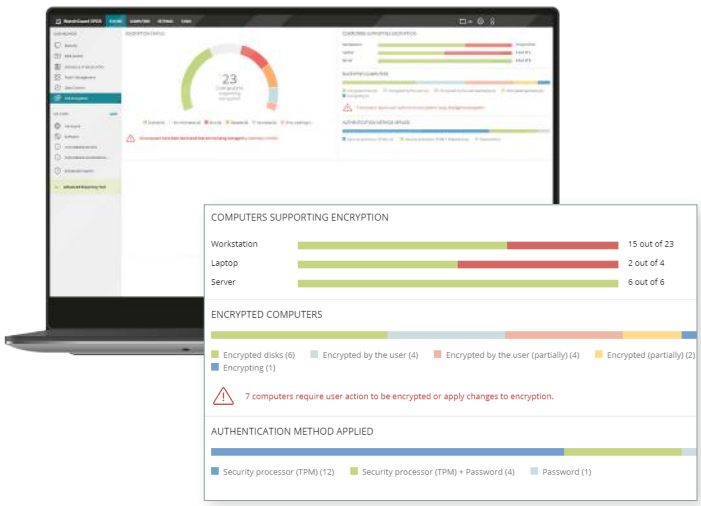
Gartner zufolge[1] wird alle 53 Sekunden ein Laptop gestohlen. Die ständig wachsenden, auf Endpoints gespeicherten Datenmengen haben das Interesse an diesen Daten und damit das Risiko für eine Datensicherheitsverletzung durch Verlust, Diebstahl oder unbefugten Zugriff auf Informationen deutlich erhöht.

Dies hat dazu geführt, dass die Einhaltung verschiedener Vorschriften, z. B. DSGVO (Datenschutz-Grundverordnung)[2] in der Europäischen Union und CCPA[3] in den USA, erhöhte Anstrengungen im Hinblick auf die Reduzierung eines zunehmend wahrscheinlichen Verlusts, Diebstahls oder unbefugten Zugriffs auf Daten und den damit verbundenen schwerwiegenden wirtschaftlichen Auswirkungen erfordert.

ZENTRALE ERHÖHUNG DES SCHUTZES VOR UNBEFUGTEM ZUGRIFF

Eine der effizientesten Methoden zur Minimierung des Datenrisikos ist die automatische Verschlüsselung der Festplatten von Desktops, Laptops und Servern. So wird gewährleistet, dass der Datenzugriff sicher und mit den implementierten Authentifizierungsmechanismen konform ist. Die Implementierung von Verschlüsselungsrichtlinien schafft eine zusätzliche Sicherheitsschicht und Kontrolle für Unternehmen. Sie kann jedoch bei Verlust des Schlüssels zu Datenkontrollen- und Wiederherstellungsproblemen führen.

WatchGuard Full Encryption schützt Windows- und macOS-Geräte mit vollständiger Festplattenverschlüsselung vor Datensicherheitsverletzungen und unbefugtem Zugriff. Die Lösung nutzt BitLocker unter Windows bzw. FileVault unter macOS, um Festplatten ohne Beeinträchtigungen für die Anwender zu verschlüsseln und zu entschlüsseln. Dies hat für Organisationen den Vorteil, dass die auf der WatchGuard Cloud-Management-Plattform gespeicherten Wiederherstellungsschlüssel zentral gesteuert und verwaltet werden.



WatchGuard Full Encryption-Dashboard der Webverwaltungskonsole von WatchGuard mit Schlüsselindikatoren zum Verschlüsselungsstatus von Endpoints im gesamten Unternehmen.

VORTEILE

Verhinderung des Verlusts, Diebstahls und unbefugten Zugriffs auf Daten, ohne Anwender zu beeinträchtigen

- Verschlüsselung der Datenträger und Schutz der Inhalte vor Diebstahl, versehentlichem Verlust und böswilligen Insidern Datenverschlüsselung, -entschlüsselung und -zugriff erfolgen für Anwender automatisch, unmittelbar und nahtlos.
- Wiederherstellungsschlüssel werden auf der Cloudplattform gespeichert und können bequem und sicher über diese oder die zugehörige Webkonsole wiederhergestellt werden.

Keine Bereitstellung oder Installation. Keine Server oder zusätzliche Kosten. Keine Probleme.

- BitLocker ist auf den meisten Windows-Betriebssystemen vorinstalliert, während FileVault auf den meisten macOS-Geräten zu finden ist. Mit WatchGuards Cloud-Plattform können Sie alle Ihre Geräte von einem zentralen Ort aus verwalten.
- Sie müssen keinen anderen Agent bereitstellen oder installieren. Alle WatchGuard Endpoint Security-Lösungen nutzen den gleichen ressourcensparenden Agent.
- **WatchGuard Full Encryption** kann direkt aktiviert werden und lässt sich einfach über die Cloud-Konsole verwalten.

Einhaltung regulatorischer Vorgaben, Berichte und zentrale Verwaltung

- WatchGuard Full Encryption ermöglicht durch Überwachung und Durchsetzung der Datenverschlüsselung eine einfache Compliance mit Datenschutzvorgaben.
- WatchGuard Full Encryption nutzt BitLocker oder FileVault, sodass Administratoren Verschlüsselungsrichtlinien festlegen und Wiederherstellungsschlüssel zentral über die Cloud verwalten können.
- Alle WatchGuard Endpoint-Sicherheitslösungen bieten intuitive Dashboards, detaillierte Berichte und Anwenderaktivitätsprotokolle für Audits.

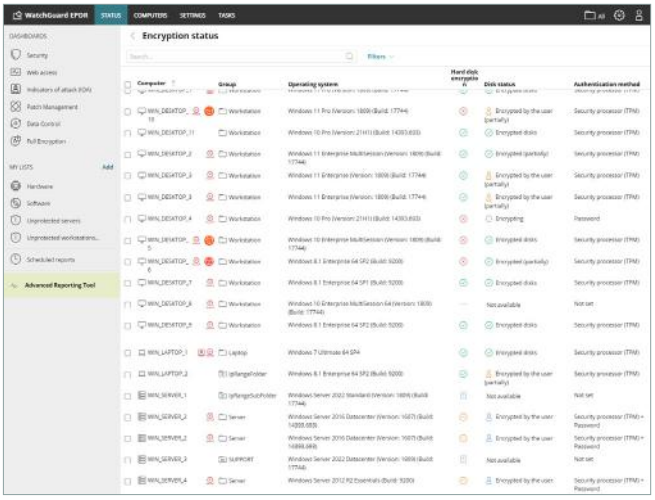
SICHERE USB-FLASHLAUFWERKE*

Im vergangenen Jahr hat die Nutzung von USB-Sticks weltweit, insbesondere in Industrieunternehmen, um 30 Prozent zugenommen. Cyberangreifer haben diesen Trend erkannt und nutzen USB-Laufwerke aus, um Zugriff auf ein System zu erhalten oder alle bzw. eine Komponente Ihres Netzwerks zu infizieren.

Daher sind Datensicherheitsverletzungen oder unbefugter Zugriff auf vertrauliche Daten für Unternehmen wahrscheinlicher. Laut einer Studie von Forrester betrafen 17 Prozent der Datensicherheitsverletzungen, die im Jahr 2023 gemeldet wurden, den Verlust oder Diebstahl von Vermögenswerten wie Laptops oder USB-Laufwerken.

Der erste Schritt bei der Minimierung des Bedrohungsrisikos sind strenge Richtlinien für die Nutzung von USB-Laufwerken im Unternehmen, Rollenebenen und auf Mitarbeiterprofilen basierenden Berechtigungen, sodass nur vom IT-Team oder MSP des Unternehmens bereitgestellte und verifizierte Geräte verwendet werden.

Diese Richtlinien reichen jedoch angesichts wachsender Cyberbedrohungen möglicherweise nicht aus. **WatchGuard Full Encryption** bietet maximalen Datenschutz für alle verschlüsselten Endpoints, indem eine Pre-Boot-Authentifizierung die Identität von Anwendern verifiziert, bevor das Betriebssystem geladen wird. Auf diese Weise werden Verlust und Diebstahl von Laptops sowie unbefugter Zugriff auf Daten verhindert.



Computerliste mit Verschlüsselungsstatus, Gruppen, den diese angehören, Betriebssystem und der verwendeten Authentifizierungsmethode

WICHTIGE FUNKTIONEN

Die Tendenz zu hybriden Arbeitsmodellen, entweder remote oder im Büro vor Ort zu arbeiten, macht die vollständige Festplattenverschlüsselung zur wichtigen ersten Verteidigungsmaßnahme für Geräte wie Laptops und USB-Laufwerke.

Bei WatchGuard Endpoint Security handelt es sich um ein zusätzliches Modul für WatchGuard Endpoint Security-Lösungen, das für eine zentrale Verwaltung der vollständigen Festplattenverschlüsselung konzipiert wurde und folgende Funktionen bietet:

Vollständige Festplattenverschlüsselung und -entschlüsselung

WatchGuard Full Encryption verschlüsselt die Laufwerke Ihrer Windows- und macOS-Laptops, -Desktop-PCs, -Server und Wechseldatenträger (nur Windows). **Das WatchGuard Full Encryption**-Dashboard bietet globale Einblicke in kompatible Netzwerk-Endpoints, deren Verschlüsselungsstatus und die verwendete Authentifizierungsmethode und ermöglicht es Administratoren, Verschlüsselungseinstellungen zuzuweisen und Verschlüsselungsberechtigungen einzuschränken.

Zentrale Verwaltung von Verschlüsselungsschlüsseln

If the access key is forgotten or there are changes in the boot sequence, BitLocker will ask for a recovery key to start up the affected system. For macOS, if the user password is forgotten, FileVault will also ask for a recovery key to start up the system. In both cases, if required, the network administrator can get the recovery keys through the management console and send them to the user.

Listen, Berichte, zentrale Richtlinienanwendung

In der Computerliste der Konsole können Administratoren mehrere Filter basierend auf dem Verschlüsselungsstatus anwenden. Diese Listen können für Datenanalysen mit externen Tools exportiert werden.

Definieren Sie Verschlüsselungsrichtlinien über die Konsole und zeigen Sie Richtlinienänderungen anhand von Auditberichten an, die Sie bei Bedarf Regulierungs- oder Aufsichtsbehörden vorlegen können.

[1] TechSpective

[2] DSGVO – Datenschutz-Grundverordnung: Zwingt Unternehmen, den Schutz personenbezogener Daten, die verarbeitet werden, zu gewährleisten. Die Nichteinhaltung kann hohe Geldstrafen und indirekte Schäden verursachen.

[3] CCPA – California Consumer Privacy Act von 2018: Dies ist das erste Gesetz in den USA, das auf der DSGVO der EU aufbaut. Es gilt für Unternehmen mit Sitz in Kalifornien und Unternehmen mit Sitz außerhalb des US-Bundesstaates.

[4] The State Of Privacy And Data Security, 2023 - Forrester

* Die Verschlüsselung und Entschlüsselung von externen und USB-Flash-Laufwerken wird nur unter Windows unterstützt.

Unterstützte Plattformen und Systemanforderungen von WatchGuard Full Encryption

Kompatibel mit WatchGuard EPDR, WatchGuard Advanced EPDR, WatchGuard EDR, und WatchGuard EPP Unterstützte Betriebssysteme: Windows and macOS.

Liste kompatibler Browser: : Google Chrome, Mozilla Firefox, Safari, and Microsoft Edge.