DATENBLATT

WATCHGUARD FULL ENCRYPTION

Die erste Verteidigungslinie für einfachen und effektiven Schutz von Daten

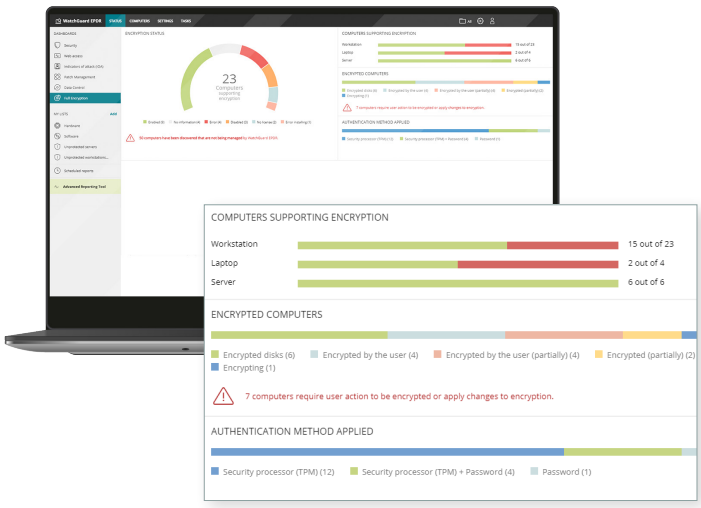
Gartner zufolge[1] wird alle 53 Sekunden ein Laptop gestohlen. Die ständig wachsenden, auf Endpoints gespeicherten Datenmengen haben das Interesse an diesen Daten und damit das Risiko für eine Datensicherheitsverletzung durch Verlust, Diebstahl oder unbefugten Zugriff auf Informationen deutlich erhöht.

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 arbeitet mit BitLocker, einer bewährten und stabilen Microsoft-Technologie, um Datenträger zu ver- und entschlüsseln, ohne Endanwender zu beeinträchtigen. Unternehmen bietet sie zudem den Mehrwert einer zentralen Steuerung und Verwaltung der auf der cloudbasierten Management-Plattform von WatchGuard gespeicherten Wiederherstellungsschlüssel.



Das 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.

- **WatchGuard Full Encryption** nutzt BitLocker, eine bewährte und häufig verwendete Windows-Technologie, für die zentrale Verwaltung.
- BitLocker ist im Lieferumfang der meisten Windows-Betriebssysteme enthalten. Mit der Webkonsole der Cloudplattform von WatchGuard können Sie Ihre Geräte zentral an einem Ort verwalten.
- Sie müssen keinen anderen Agent bereitstellen oder installieren. Alle WatchGuard Endpoint Security-Lösungen nutzen den gleichen ressourcensparenden Agent.
- Dank der zentralen Verwaltung von Wiederherstellungsschlüsseln über die Cloud müssen keine Server installiert bzw. gewartet werden.
- **WatchGuard Full Encryption** kann unmittelbar aktiviert werden und lässt sich einfach über die anwenderfreundliche Schnittstelle der WatchGuard Cloud verwalten.

Einhaltung regulatorischer Vorgaben, Berichte und zentrale Verwaltung

- **WatchGuard Full Encryption** ermöglicht eine einfache Einhaltung regulatorischer Vorgaben zum Datenschutz, indem die BitLocker-Aktivierung auf Windows-Geräten überwacht und erzwungen werden wird.
- Alle WatchGuard Endpoint Security-Lösungen bieten intuitive Dashboards, detaillierte Berichte und Änderungsaudits.
- Darüber hinaus ermöglicht die rollenbasierte Verwaltung Administratoren die Implementierung unterschiedlicher Autorisierungsstufen und Richtlinien für Gruppen und Geräte über eine einzelne zentrale Webkonsole.

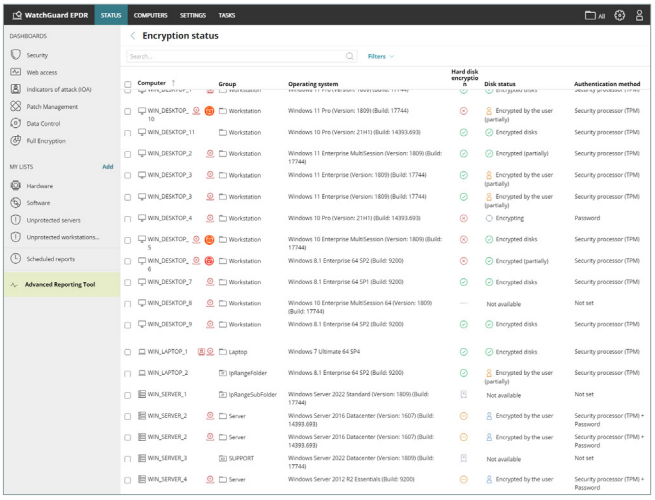
SICHERE USB-FLASHLAUFWERKE

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[4] betrafen 20 Prozent der Datensicherheitsverletzungen, die von globalen Sicherheitsentscheidungsträgern im Jahr 2020 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 nutzt BitLocker für die volle Verschlüsselung der Laufwerke Ihrer Laptops, Desktop-PCs, Server und Wechseldatenträger mit 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

Wenn der Zugriffsschlüssel vergessen wurde oder bei Änderungen der Startsequenz fordert BitLocker einen Wiederherstellungsschlüssel für den Start des betroffenen Systems an. Der Netzwerkadministrator kann bei Bedarf den Wiederherstellungsschlüssel über die Verwaltungskonsole abrufen und ihn an den Anwender senden.

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 Protection, 2021 – Forrester

Unterstützte Plattformen und Systemanforderungen von WatchGuard Full Encryption

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

Liste kompatibler Browser: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge und Opera.