Verbessern der Sicherheitslage für Ihr Netzwerk mit Netzwerkzugangskontrolle

In einer Zeit sich schnell entwickelnder Cyber-Bedrohungen und einer sich immer weiter ausbreitenden digitalen Infrastruktur bleibt die Netzwerksicherheit für Unternehmen jeder Größe von größter Bedeutung. Der Verizon 2023 Data Breach Investigations Report zeigt, dass 38 % der Datensicherheitsverletzungen im Jahr 2022 auf kompromittierte Anmeldeinformationen zurückzuführen sind, selbst bei vorhandener Multifaktor-Authentifizierung. Da Unternehmen mit der Komplexität der Sicherung ihrer Netzwerke konfrontiert sind, erweist sich die Netzwerkzugangskontrolle (Network Access Enforcement) als eine leistungsstarke Lösung zum Schutz vor unbefugtem Zugriff, zur Verringerung des Risikos von Datensicherheitsverletzungen, zur Gewährleistung der Compliance und zur Optimierung der Netzwerkleistung.

Die Netzwerkzugangskontrolle in WatchGuard Cloud ermöglicht es Netzwerkadministratoren, eine Endpoint-Prüfung durchzuführen, um sicherzustellen, dass auf den Geräten eine angemessene Endpoint-Sicherheit verfügbar ist, bevor eine Verbindung mit dem Netzwerk hergestellt wird. Mit einer automatisierten Steuerung der Geräte, die eine Verbindung herstellen können, können Netzwerkadministratoren das Schutzniveau in Unternehmensnetzwerken über die herkömmliche Netzwerkzugriffssteuerung hinaus erhöhen.

Vorteile der Implementierung der Netzwerkzugangskontrolle

- **Erhöhte Sicherheit**
  Die Netzwerkzugangskontrolle (Network Access Enforcement) dient als zusätzliche Sicherheitsebene und schützt proaktiv vertrauliche Daten, geistiges Eigentum und wichtige Netzwerkressourcen, indem sie strenge Sicherheitsrichtlinien durchsetzt, um unbefugten Netzwerkzugriff zu verhindern.
- **Gewährleistung der Compliance**
  Die Netzwerkzugangskontrolle vereinfacht die Compliance, indem sie striktere Sicherheitsrichtlinien durchsetzt, eine problemlose Anpassung an gesetzliche Anforderungen in verschiedenen Branchen wie dem Gesundheits- und Finanzwesen gewährleistet und Unternehmen bei der ständigen Herausforderung unterstützt, branchenspezifische Vorschriften und Standards zu erfüllen.
- **Optimierte Netzwerkleistung**
  Die Netzwerkzugangskontrolle erhöht nicht nur die Sicherheit, sondern trägt auch entscheidend zur Optimierung der Netzwerkleistung bei, indem sie nicht autorisierten Geräten den Zugriff auf Netzwerkressourcen verwehrt, den Betrieb optimiert und so die Effizienz steigert und den problemlosen Zugriff für rechtmäßige Benutzer gewährleistet, während nicht autorisierte Geräte abgeschirmt werden.

Funktionsweise der Netzwerkzugangskontrolle

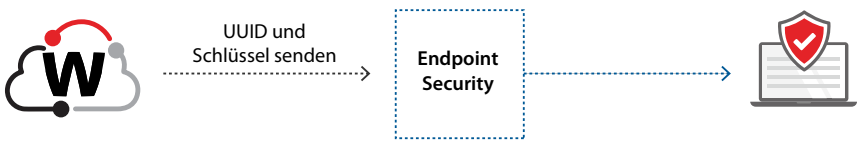

Abbildung 1. WatchGuard Cloud sendet die UUID und den Schlüssel an den Endpoint-Service, der sie an Clients mit WatchGuard Endpoint Security weiterleitet.

Die Netzwerkzugangskontrolle beginnt mit der Installation des WatchGuard Endpoint Security-Agenten auf einem Endpoint-Gerät. Dieser Agent registriert sich dann nahtlos bei der WatchGuard Cloud-Verwaltungskonsole, woraufhin Sie auf das jeweilige Gerät ausgerichtete Richtlinien für die Endpoint-Sicherheit konfigurieren und bereitstellen können.

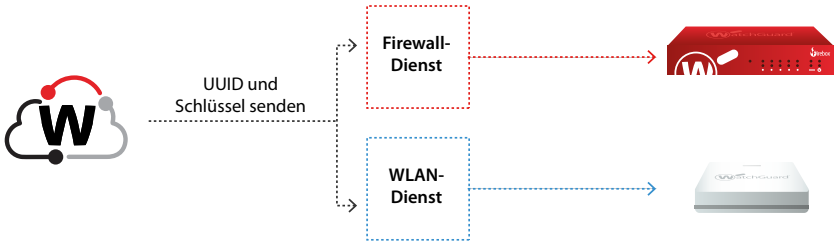

Abbildung 2: Wenn die Netzwerkzugangskontrolle aktiviert ist, sendet WatchGuard Cloud die UUID und den Schlüssel an die Firewall und die WLAN-Dienste und leitet sie an die WatchGuard Firebox- und Access Point-Instanzen weiter.

Die Netzwerkzugangskontrolle ist nicht standardmäßig aktiviert. In WatchGuard Cloud können Sie die Netzwerkzugangskontrolle auf Ihren WatchGuard Firebox-Firewalls und -Zugriffspunkten aktivieren. Sobald dies abgeschlossen ist, bestimmen diese Firebox-Instanzen und Zugriffspunkte, ob ein Endgerät auf das Netzwerk zugreifen kann.

Abbildung 3. Ein Client mit WatchGuard Endpoint Security stellt eine VPN-Verbindung mit dem Netzwerk her. Ein Client ohne WatchGuard Endpoint Security wird daran gehindert, eine Verbindung mit dem Netzwerk über VPN herzustellen.

Wenn der Client eine VPN-Verbindung mit aktivierter Endpoint-Durchsetzung initiiert, überprüft die Firebox-Instanz sofort die Anwesenheit des Endpoint-Agenten. Anschließend fordert er die UUID und den Schlüssel vom Client an und überprüft, ob diese Werte mit den erwarteten Werten übereinstimmen, wodurch dem Client nach erfolgreicher Validierung letztendlich Zugriff auf das VPN gewährt wird. Der VPN-Zugriff wird dem Client nicht gewährt, wenn die Validierung nicht den Erwartungen entspricht.

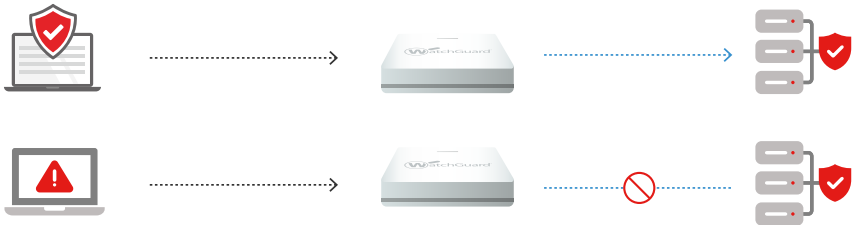

Abbildung 4. Ein Client mit WatchGuard Endpoint Security stellt eine Verbindung mit dem WLAN-Netzwerk her. Ein Client ohne WatchGuard Endpoint Security kann keine Verbindung mit dem WLAN-Netzwerk herstellen.

Wenn der Client eine Verbindung mit dem WatchGuard Access Point mit aktivierter Endpoint-Durchsetzung herstellt, führt der AP eine Reihe von Prüfungen durch. Zunächst wird überprüft, ob der Endpoint-Agent auf dem Client ausgeführt wird. Dann fordert der AP die UUID und den Schlüssel vom Client an und überprüft, ob diese Werte mit den erwarteten übereinstimmen. Der Client erhält Zugriff auf das Netzwerk, wenn die Validierung erfolgreich ist. Bei nicht erfolgreicher Validierung wird dem Client der Zugriff nicht gewährt.

Integration mit dem Sicherheitsökosystem von WatchGuard

In einer Zeit, in der Netzwerksicherheit nicht mehr wegzudenken ist, erweist sich die Netzwerkzugangskontrolle als wertvolles Instrument für Unternehmen beliebiger Größe. Es versetzt Unternehmen in die Lage, die Sicherheit, Compliance und Verwaltbarkeit ihrer kabelgebundenen und drahtlosen Netzwerke zu verbessern. Um eine zuverlässige Kontrolle des Netzwerkzugriffs und der Sicherheitsrichtlinien zu gewährleisten, ist die Netzwerkzugangskontrolle eng mit unserer Suite von Sicherheitslösungen, einschließlich der Endpoint-Sicherheit und Firewalls, integriert. Dieser einheitliche Ansatz vereinfacht die Durchsetzung von Richtlinien zur Endpoint-Sicherheit im gesamten Netzwerk und stellt sicher, dass die Sicherheitslage Ihres Unternehmens konsistent und umfassend bleibt.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB +1 206 613 0895 www.watchguard.de