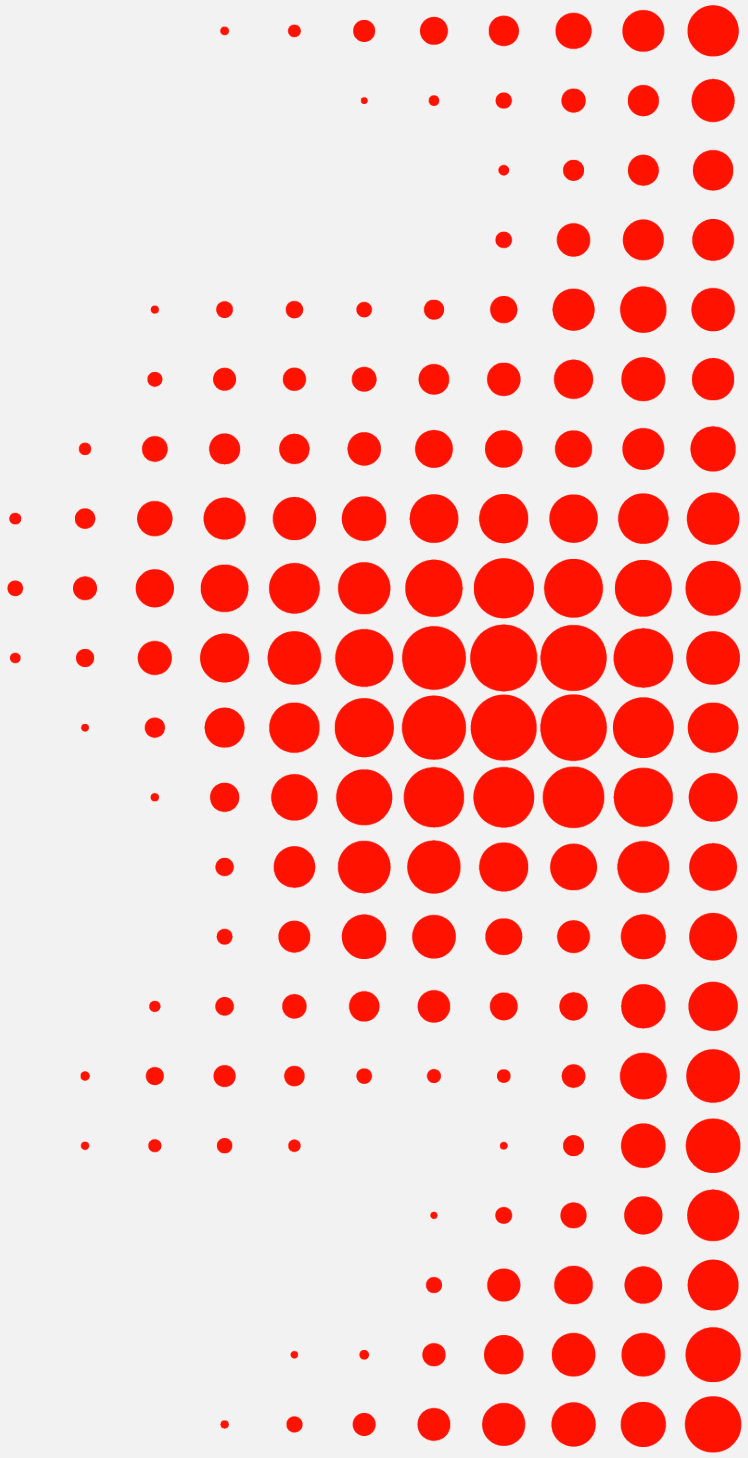
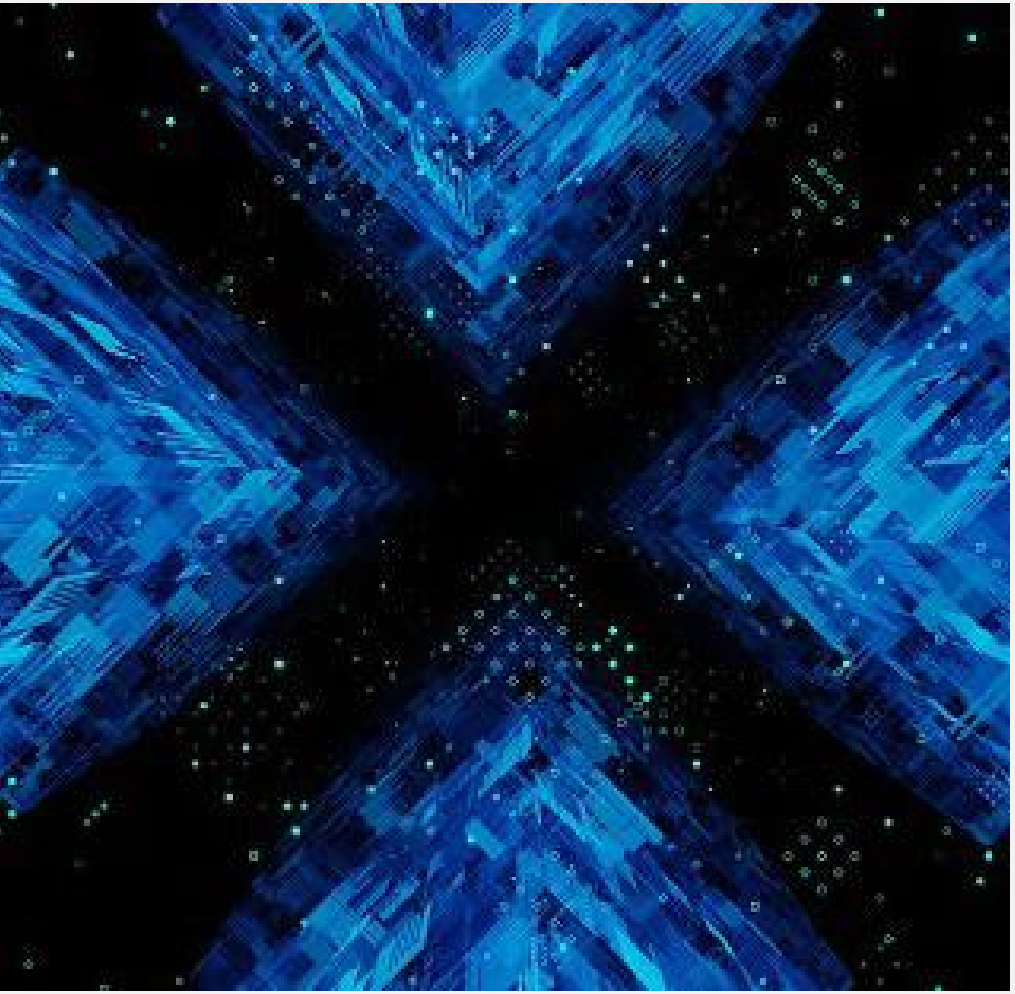
An der Peripherie: Netzwerkzugangskontrolle in der heutigen Ära

Leitfaden für erweiterte Netzwerkzugangskontrolle (Network Access Control, NAC) mit Netzwerkzugangserzwingung (Network Access Enforcement, NAE) unter Verwendung von WatchGuard Firebox, WLAN und Endpoint Security

Inhaltsverzeichnis

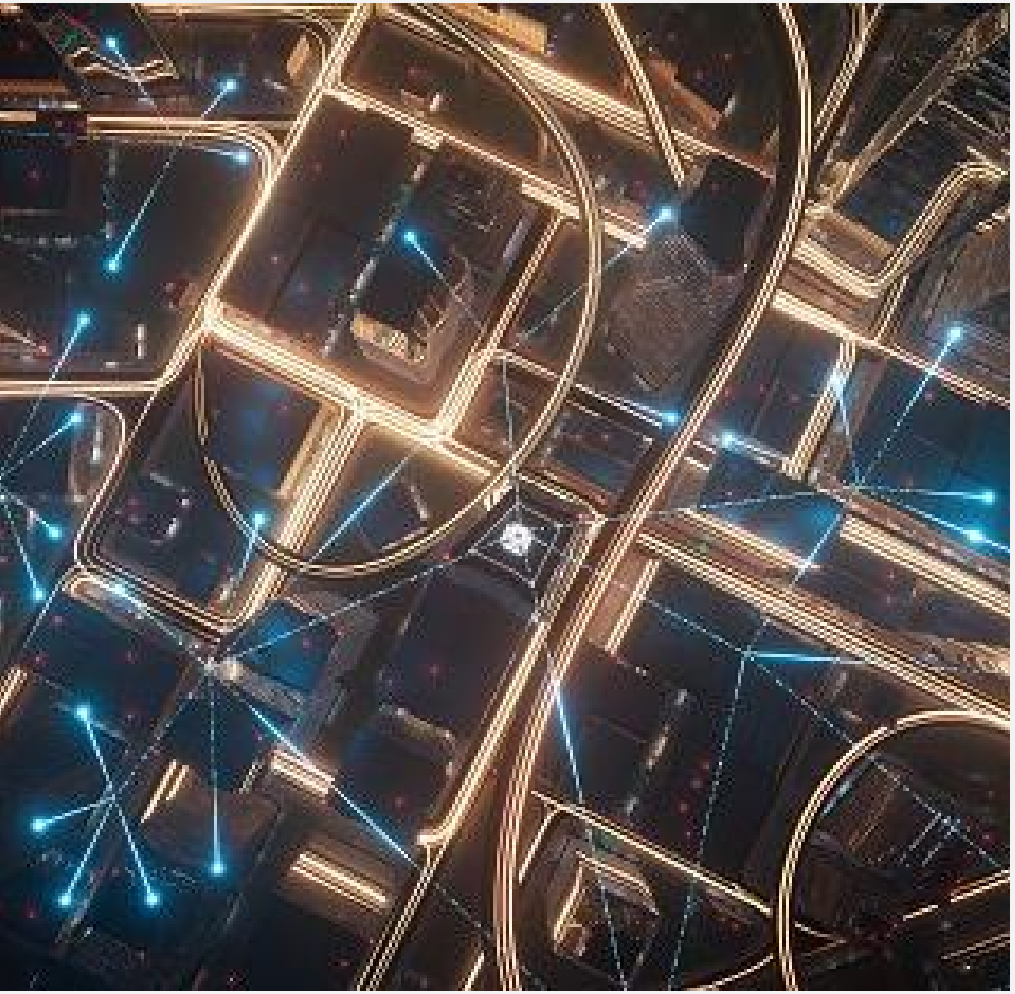




00 Die Bedeutung der Netzwerkzugangskontrolle

Mit der zunehmenden Abhängigkeit von vernetzten Systemen und Cloud-Diensten wird die Netzwerkzugangskontrolle (NAC) zu einer wichtigen Verteidigungslinie, die die Integrität und Sicherheit moderner digitaler Infrastrukturen schützt, indem sie sicherstellt, dass nur autorisierte Anwender und Geräte auf das Netzwerk zugreifen und nicht autorisierte oder gefährdete Entitäten ferngehalten werden.

In diesem E-Book erfahren Sie mehr über die Grundlagen von NAC und wie die Unified Security Platform® -Architektur von WatchGuard die Bereitstellung von NAC vereinfacht und die Sicherheit erhöht.



01 Grundlagen der Netzwerkzugangskontrolle

1.1 Definition von NAC und ihre Rolle in der Network Security

NAC wurde entwickelt, um den Zugriff auf Ihr Netzwerk durch Geräte und Anwender zu verwalten und zu regulieren. Ihre Hauptaufgabe besteht darin, als Gatekeeper zu fungieren, Sicherheitsrichtlinien durchzusetzen, Entitäten zu authentifizieren, die Zugang erhalten möchten, und die Gerätekonformität sowie den Gesundheitszustand von Geräten zu prüfen, bevor der Zugriff gewährt wird. Durch den Einsatz einer Kombination aus Authentifizierungs-, Autorisierungs- und Endpoint-Sicherheitsprüfungen hilft NAC Ihnen, das Risiko von unbefugtem Zugriff, Datensicherheitsverletzungen und der Verbreitung von Malware in Ihren Netzwerken zu verringern.

1.2 NAC-Bereitstellungsmodelle: Lokal, cloudbasiert und hybrid

Diese Bereitstellungsmodelle bieten Ihnen Flexibilität je nach Ihren spezifischen Anforderungen und Ihrer Infrastruktur.

- Bei lokalen NAC-Lösungen wird das System im lokalen Rechenzentrum oder Netzwerk Ihres Unternehmens installiert und verwaltet, sodass Sie direkte Kontrolle über Sicherheitsrichtlinien und Daten haben. Dieses Modell eignet sich für Unternehmen mit strengen Anforderungen an die Datensouveränität oder für Unternehmen, die die Implementierung ihrer Netzwerkzugangskontrolle völlig autonom gestalten möchten.
- Cloudbasierte NAC hingegen nutzt die Cloud-Infrastruktur zur Bereitstellung von Netzwerkzugangskontrolldiensten. Dieses Modell bietet Skalierbarkeit, einfaches Management und die Möglichkeit, sich an dynamische Netzwerkumgebungen anzupassen. Cloudbasierte NAC ist besonders vorteilhaft, wenn Ihr Unternehmen über dezentrale oder Remote-Mitarbeiter verfügt, da es eine zentrale Kontrolle ohne umfangreiche Hardware vor Ort ermöglicht.
- Hybride Bereitstellungen der Netzwerkzugangskontrolle kombinieren Elemente von lokalen und Cloud-basierten Modellen und bieten einen ausgewogenen Ansatz. Bei hybriden Setups können Sie so die Kontrolle über kritische Aspekte lokal behalten und gleichzeitig die Skalierbarkeit und Flexibilität der Cloud-Lösungen nutzen.

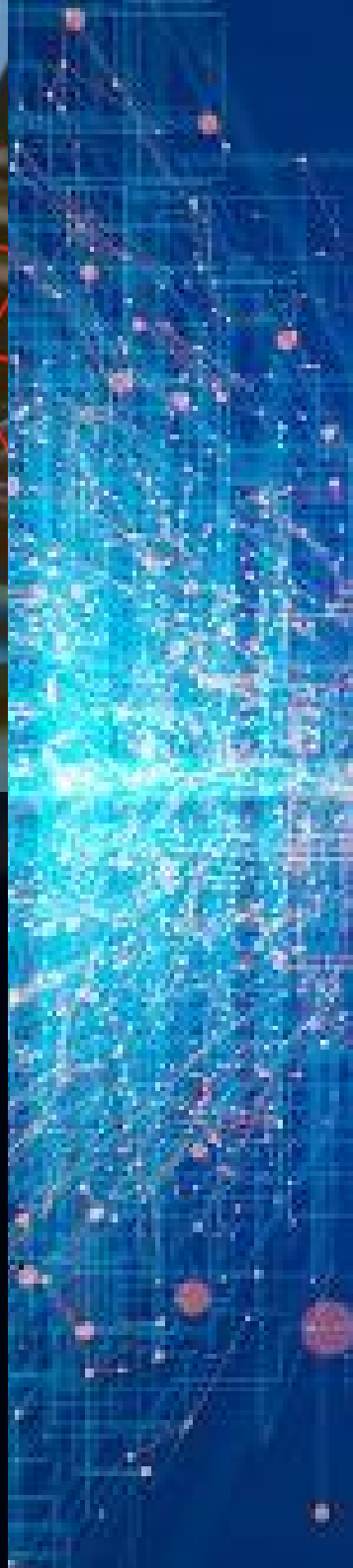
1.3 NAC-Komponenten: Authentifizierung und Autorisierung

Die Netzwerkzugangskontrolle umfasst mehrere kritische Komponenten, wobei Authentifizierung und Autorisierung eine entscheidende Rolle bei der Gewährleistung der Sicherheit und Integrität des Netzwerkzugangs spielen.

- Bei der Authentifizierung wird die Identität von Anwendern oder Geräten überprüft, die versuchen, eine Verbindung zum Netzwerk herzustellen. Dazu gehört die Überprüfung von Anmeldeinformationen wie Benutzernamen und Kennwörtern, digitalen Zertifikaten oder biometrischen Daten, um sicherzustellen, dass nur autorisierte Personen Zugang erhalten.
- Die Autorisierung bestimmt die Zugriffsrechte, die authentifizierten Anwendern oder Geräten auf der Grundlage von vordefinierten Sicherheitsrichtlinien gewährt wird. Bei diesem Prozess werden Anwendern bestimmte Berechtigungen und Privilegien zugewiesen, um sicherzustellen, dass sie nur auf Ressourcen und Dienste zugreifen, die für ihre Rolle geeignet sind.

1.4 Durchsetzung von NAC-Richtlinien: Zugang gewähren, einschränken und überwachen

Die Durchsetzung der NAC-Richtlinien ist entscheidend für die Sicherung des Zugangs zu Ihrem Netzwerk. Vordefinierte Sicherheitsrichtlinien stellen sicher, dass nur authentifizierte und autorisierte Anwender oder Geräte in das Netzwerk gelangen, wenn ihnen der Zugang gewährt wird. Mit diesen Richtlinien definieren Sie akzeptables Verhalten und Compliance-Kriterien, die zur Aufrechterhaltung der Integrität des Netzwerks beitragen. Umgekehrt zeichnet sich NAC durch die Beschränkung des Zugangs aus, indem nicht autorisierte oder nicht konforme Entitäten sofort identifiziert und isoliert werden.



02 NAC-Lösungen von WatchGuard

2.1 Übernehmen Sie die Kontrolle über den Netzwerkzugang mit WatchGuard

Eine Übersicht der WatchGuard-Lösungen für NAC.

Firebox

Die Firebox-Appliance von WatchGuard ist das Herzstück der NAC-Lösung von WatchGuard und bietet umfassende Sicherheitsfunktionen, um Ihre Netzwerke vor verschiedenen Bedrohungen zu schützen. Zu diesen Funktionen zählen:

- Firewall: Schützt Netzwerke vor unbefugtem Zugang und bösartigem Datenverkehr
- Intrusion Prevention: Erkennt und blockiert bekannte Angriffe
- Web-Filter: Blockiert den Zugang zu bösartigen Websites
- Anwendungskontrolle: Kontrolliert den Zugang zu Anwendungen basierend auf Identität und Rolle des Anwenders und der Tageszeit
- VPN: Ermöglicht sicheren Fernzugriff auf Netzwerke

Access Points

WatchGuard Access Points erweitern den Schutz der Firebox auf drahtlose Netzwerke und bieten die gleichen Funktionen wie Firebox-Appliances, plus:

- WLAN-Sicherheit: Unterstützt WPA2-Enterprise- und WPA3-Verschlüsselung zum Schutz des drahtlosen Datenverkehrs
- Captive Portal: Bietet Authentifizierung und Autorisierung für drahtlose Anwender
- Gast-Netzwerke: Ermöglicht Gästen den Zugang zum Netzwerk ohne Beeinträchtigung der Sicherheit

Endpoint Security

WatchGuard Endpoint Security schützt Endgeräte, einschließlich Laptops, Desktops und Mobilgeräte. Es bietet eine Vielzahl von Funktionen, darunter:

- Antivirus: Erkennt und blockiert Viren, Malware und andere Bedrohungen
- Endpoint Detection and Response (EDR) Untersucht komplexe Angriffe und reagiert auf sie
- Mobile Device Management (MDM): Sichert und verwaltet Mobilgeräte

Cloudbasierte Lösungen

WatchGuard Cloud vereinfacht die Bereitstellung und Verwaltung der NAC-Funktionen von WatchGuard. Sie bietet zentrale Sichtbarkeit und Kontrolle über alle Sicherheitsgeräte und Netzwerke und erleichtert Ihnen die Verwaltung Ihrer Sicherheitslage.

2.2 Endpoint Security Agent: Installation, Konfiguration und Reporting

Der Endpoint Security Agent von WatchGuard bietet mehrere Vorteile für die Netzwerkzugangskontrolle:

Optimierte Installation und Bereitstellung: Einfache Installation und Bereitstellung auf Desktops, Laptops und Mobilgeräten, um NAC-Richtlinien anzuwenden und die Sicherheit auf allen Endpoints in Ihrem Netzwerk zu verbessern.

Zentrale Konfiguration und Verwaltung: Zentrale Konfiguration und Verwaltung über WatchGuard Cloud. Dieser zentralisierte Ansatz ermöglicht Ihnen die einfache Verwaltung von Endpoint-Sicherheitsrichtlinien, die Anwendung von Updates und die Überwachung des Zustands aller Endpoints in Ihrem Netzwerk.

Umfassende Berichterstattung und Visualisierung: Sie erhalten umfassende Berichte und Einblicke in die Sicherheitslage Ihrer Endpoints, einschließlich detaillierter Informationen zum Sicherheitsstatus der Endpoints, erkannte Bedrohungen und ergriffene Abhilfemaßnahmen. Sie können diese Informationen nutzen, um potenzielle Schwachstellen zu identifizieren, die Wirksamkeit von NAC-Richtlinien zu verfolgen und die Einhaltung von Sicherheitsstandards nachzuweisen.

Verbesserte Network Security: Verbessern Sie die Netzwerksicherheit durch effektiven Schutz der Endpoints. Geschützte Endpoints sind weniger anfällig für Malware-Infektionen, Phishing-Angriffe und andere Bedrohungen, die Ihr Netzwerk gefährden könnten.

Verbesserte Compliance: Erfüllen Sie die Compliance-Anforderungen in Bezug auf die Endpoint-Sicherheit, indem Sie nachweisen, dass alle Endpoints geschützt sind und den Richtlinien für die Netzwerkzugangskontrolle entsprechen.

2.3 Netzwerkzugangserzwingung (Network Access Enforcement (NAE)): Richtlinienerstellung und -durchsetzung

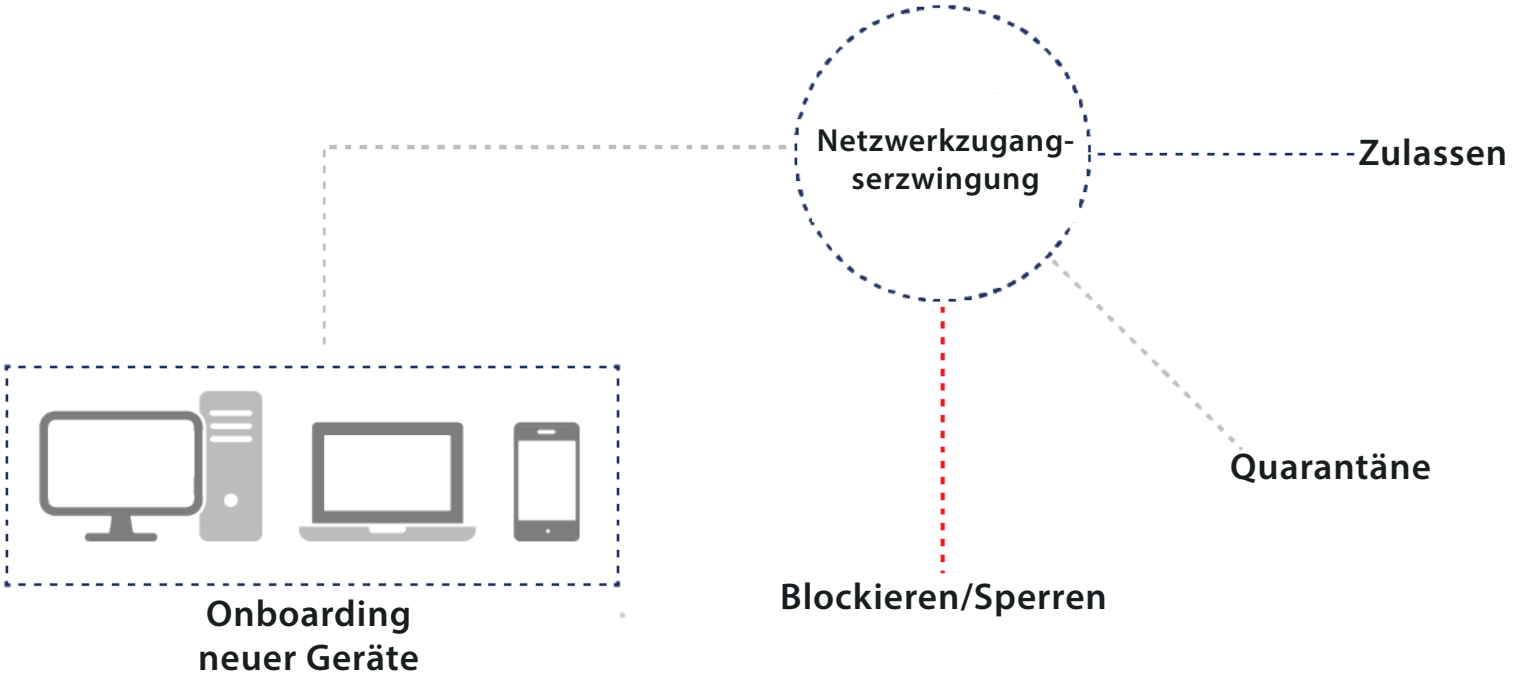
WatchGuard NAE ist eine stärkere, fortschrittlichere Version von NAC, mit der Sie steuern können, welche Geräte Zugang zu Ihren Netzwerken haben können, sei es kabelgebunden oder drahtlos. Außerdem können Sie den Zugriff auf VPNs und andere Fernzugriffsdienste steuern können, indem Sie Sicherheitsanforderungen für Endpoints durchsetzen, bevor diese eine Verbindung herstellen können. Durch die Aktivierung von NAE auf WatchGuard Access Points und den Einsatz einer WatchGuard Endpoint-Sicherheitslösung können Sie beispielsweise verlangen, dass auf den Endpoints aktuelle Sicherheitssoftware installiert ist, dass sie frei von Malware sind und dass ihre Konfigurationen den Unternehmensrichtlinien entsprechen, bevor sie eine Verbindung zu einem Access Point herstellen können.

Während sich die Wettbewerber weitgehend auf separate Endpoint- oder Netzwerksicherheitslösungen konzentrieren, lässt sich die NAE-Lösung von WatchGuard nahtlos in WatchGuard Firebox-, WLAN- und Endpoint-Sicherheitslösungen integrieren und ermöglicht so eine umfassende Netzwerkzugangskontrolle als Teil unserer Unified Security Platform-Architektur.

- Die Firebox ist die zentrale Stelle für die Durchsetzung von NAE-Richtlinien. Sie kommuniziert mit WatchGuard Endpoint Security-Agenten, die auf den Endpoints installiert sind, um deren Konformität mit den vordefinierten Sicherheitsanforderungen zu überprüfen.
- NAE kann auf WLAN-Netzwerke ausgeweitet werden, um sicherzustellen, dass sich nur autorisierte und konforme Geräte mit drahtlosen Access Points verbinden können.
- WatchGuard Endpoint Security-Agenten bieten Echtzeitüberwachung und -Berichterstattung des Gerätezustands, sodass die Firebox oder der Access Point fundierte Entscheidungen über die Gewährung oder Verweigerung des Netzwerkzugriffs treffen kann.

Die Vorteile von WatchGuard NAE:

- Verringerung des Risikos von Malware-Infektionen, indem Sie von den Endpoints verlangen, dass sie aktuelle Sicherheitssoftware installieren
- Schutz sensibler Daten, in dem der Zugriff nicht autorisierter Geräte auf das Netzwerk verhindert wird
- Einhaltung von Sicherheitsvorschriften durch automatisierte Durchsetzung von Sicherheitsrichtlinien
- Senkung der IT-Kosten durch Automatisierung der Durchsetzung von Sicherheitsrichtlinien und Entlastung der IT-Mitarbeiter, die sich so auf andere Aufgaben konzentrieren können.



2.4 Anwenderverwaltung und Integration von Gruppenrichtlinien

Die Integration der WatchGuard Anwenderverwaltung und Gruppenrichtlinien vereinfacht die Anwenderzugangskontrolle und schafft Sicherheit durch die Nutzung vorhandener Anwenderverzeichnisse und Gruppenrichtlinien. Auf diese Weise können Sie Anwenderkonten, Berechtigungen und Zugangskontrollregeln zentral verwalten, den Verwaltungsaufwand reduzieren und eine konsistente Durchsetzung der Sicherheit im gesamten Netzwerk gewährleisten.

Anwender-Authentifizierung und Autorisierung WatchGuard Lösungen lassen sich in verschiedene Anwenderverzeichnisse integrieren, darunter Active Directory-, LDAP- und RADIUS-Server, um Anwender zu authentifizieren und zu autorisieren. Versucht ein Anwender, auf eine Netzwerkressource zuzugreifen, überprüft WatchGuard seine Anmeldeinformationen anhand des Anwenderverzeichnisses und gewährt den Zugriff basierend auf den ihm zugewiesenen Berechtigungen.

Integration von Gruppenrichtlinien WatchGuard Lösungen lassen sich in Gruppenrichtliniensysteme, wie z. B. Active Directory Group Policy, integrieren, um granulare Zugangskontrollrichtlinien auf der Grundlage von Anwendergruppen anzuwenden. Diese Richtlinien definieren Zugriffsberechtigungen für bestimmte Netzwerkressourcen, Anwendungen und Dienste, um sicherzustellen, dass Anwender nur auf die Ressourcen zugreifen können, die sie zur Erfüllung ihrer Aufgaben benötigen.

Zentrale Konfiguration und Verwaltung: Die Integration von WatchGuard Lösungen in Anwenderverwaltungs- und Gruppenrichtliniensystemen bietet mehrere Vorteile:

- Die automatisierte Erstellung und Pflege von Anwenderkonten reduziert den Verwaltungsaufwand und sorgt für Konsistenz der Anwenderidentitäten.
- Die Integration von Gruppenrichtlinien ermöglicht eine granulare Kontrolle über den Anwenderzugriff auf Netzwerkressourcen, Anwendungen und Dienste.
- Die Anwenderauthentifizierung und -autorisierung auf der Grundlage vertrauenswürdiger Anwenderverzeichnisse und Gruppenrichtlinien stärkt die Netzwerksicherheit.
- Die optimierte Anwenderverwaltung und Zugangskontrolle vereinfacht die Einhaltung von Datenschutzbestimmungen und Sicherheitsstandards.
- Durch die Durchsetzung von Zugriffsbeschränkungen auf der Grundlage von Anwendergruppen und -richtlinien können Sie das Risiko eines unbefugten Zugriffs auf sensible Daten und Systeme minimieren.

03 Fazit

Herkömmliche NAC fungiert als Torwächter für Ihre digitale Sicherheit, indem sie jede Identität rigoros bestätigt, bevor sie den Zugang gewährt – eine entscheidende Rolle, die mit einem Schloss an der Haustür vergleichbar ist. So wie ein Schloss allein jedoch kein sicheres Zuhause gewährleistet, erreicht der Netzwerkzugang seine maximale Effektivität, wenn er in eine umfassende Sicherheitslösung integriert wird. Hier zeichnet sich die NAE- und Unified Security Platform-Architektur von WatchGuard aus, die ein ganzheitliches Sicherheitsökosystem bietet, das Endpoint-Schutz, Multifaktor-Authentifizierung, Intrusion Detection und mehr umfasst.

Es mag zwar verlockend sein, Lösungen von verschiedenen Anbietern zusammenzustellen, aber dieser Ansatz kann umständlich und verwirrend sein und Schwachstellen hinterlassen. „Es ist wichtig, NAE als Teil einer gesamten Sicherheitsstrategie zu betrachten. Anstatt sich mit einem einzigen Schloss zufrieden zu geben, sollten Sie sich für WatchGuard entscheiden, um die einheitliche, vereinfachte Leistung der intelligentesten Art, Ihr Netzwerk zu sichern, zu genießen – eine wichtige Entscheidung, um in der sich ständig weiterentwickelnden Bedrohungslandschaft von heute wirklich beruhigt zu sein.

WEITERE INFORMATIONEN

Warum Sie WatchGuard Network Security kaufen sollten

Netzwerkzugangserzwingung und -kontrolle

Warum Sie WatchGuard Secure Wi-Fi kaufen sollten

Warum Sie Identity Security kaufen solten

Einfacheres Sicherheitsmanagement

Warum sie WatchGuard Endpoint Security kaufen sollten

Warum Sie WatchGuard kaufen sollten

WatchGuard Network Security und sicheres WLAN
Übernehmen Sie die Kontrolle über Ihren Netzwerkzugang

Gewähren Sie Zugang auf der Grundlage von Vertrauen, nicht nur von Identität, und optimieren Sie Ihre Sicherheitsabläufe mit automatisierter Durchsetzung, um wertvolle IT-Ressourcen zurückzugewinnen.

Auf unserer Website finden Sie weitere Informationen:

www.watchguard.com/wgrd-solutions/security-trends/zero-trust

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cyber-Sicherheit. Unser Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, mit der ihre Unternehmen an Größe und Geschwindigkeit gewinnen und gleichzeitig die betriebliche Effizienz verbessern können. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, welche die fünf wichtigen Elemente einer Sicherheitsplattform umfassen – umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, betriebliche Ausrichtung und Automatisierung – und sorgen somit für den Schutz von mehr als 250.000 Kunden. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.de.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 **INTERNATIONALER VERTRIEB:** +1 206 613 0895 **WEB** www.watchguard.com/de