DIE AUSWAHL DES BESTEN CYBER SECURITY MANAGEMENTS

Inhaltsverzeichnis

Cyber Security Management im Jahr 2021

Die Verwaltung aller Bereiche von Netzwerksicherheitslösungen in Ihrer Umgebung kann eine komplexe Aufgabe sein. Neben der Durchsetzung von Verteidigungsstrategien, die Zugriff, Identität, Compliance und Bedrohungsprävention umfassen, muss sie alle geschäftlichen Anforderungen berücksichtigen, schnelle Änderungen in der Netzwerkinfrastruktur zulassen, neue Technologien und Trends nahtlos adaptieren können und eine agile Bereitstellung von Anwendungen und Diensten ermöglichen.

Dieses Whitepaper nennt die wichtigsten Prinzipien für die postmoderne Cyber Security Management Plattform, die erforderlich ist, um sicherzustellen, dass Unternehmen das Beste aus den Kontrollmechanismen für die Cybersicherheit herausholen, in die sie investieren. Es liefert außerdem wichtige Bewertungskriterien für die Auswahl der besten Lösung und verweist auf die neueste Cyber Security Management Plattform von Check Point.

Der Bedarf an einem neuen Cyber Security Management

Das Konzept des Sicherheitsperimeters ändert sich ständig. Die digitale Transformation, getrieben durch die Anforderungen des Marktes, ist heute die erwartete Wachstumsstrategie fast jeden Unternehmens. Ganz zu schweigen davon, dass die Zahl der mobilen Mitarbeiter und Unternehmen zunimmt, was diese Sorge nur noch verstärkt. Das bedeutet, dass sich die Infrastruktur, die wir sichern müssen, nicht mehr in unseren physischen Räumlichkeiten befindet und nicht mehr an unsere physischen Netzwerke angeschlossen ist. Anwendungen und On-Demand-Dienste werden automatisch mit einem Mausklick bereitgestellt. Cloud-, Mobil- und IoT-Geräte verändern die IT-Landschaft rasant, bieten enorme Chancen, aber auch neue Risiken, die es zu bewältigen gilt.

Auch wenn sich die Landschaft verändert hat und es zunehmend mehr sicherheitsrelevante Sicherheitspunkte in verschiedenen Formfaktoren gibt, bleibt die Herausforderung dieselbe: Wie lässt sich diese wachsende Cybersicherheitsinfrastruktur sicher verwalten.

Um diese Herausforderungen zu meistern, muss das Cyber Security Management auf 4 Säulen aufbauen:

- **Automatisiert** in CI/CD-Pipelines zur Reduzierung von Konfigurationsfehlern, Beschleunigung von Bereitstellungen und Ermöglichung der Orchestrierung von Betriebsprozessen
- **Konsolidiert,** um die Wirksamkeit zu erhöhen, Opex- und Capex-Kosten zu reduzieren und eine klare Vision zu schaffen, die mit der Verwaltung von Richtlinien und Veranstaltungen unter einem Dach einhergeht, die eng miteinander verbunden sind
- **Dynamisch** und agil, um mit der nächsten großen Veränderung in der Cybersicherheit Schritt zu halten
- **Effizient,** damit das Cyber Security Management das Tempo der Veränderungen nicht verlangsamt

Diese vier Säulen bilden das Fundament der R81 Cyber Security Management Plattform von Check Point, der branchenweit fortschrittlichsten Software zur Bedrohungsprävention und zum Sicherheitsmanagement. Sie verwaltet die Sicherheit Ihres gesamten Unternehmens, der On-Premises-Netzwerke, der Cloud-Netzwerke und -Workloads, der Remote-Benutzer und deren Zugang zu Cloud-Anwendungen sowie des Internets und des IoT. Dieses Dokument konzentriert sich auf die Aspekte der Netzwerksicherheitsrichtlinien und des Bedrohungsmanagements der R81 Sicherheitsmanagement-Plattform von Check Point.

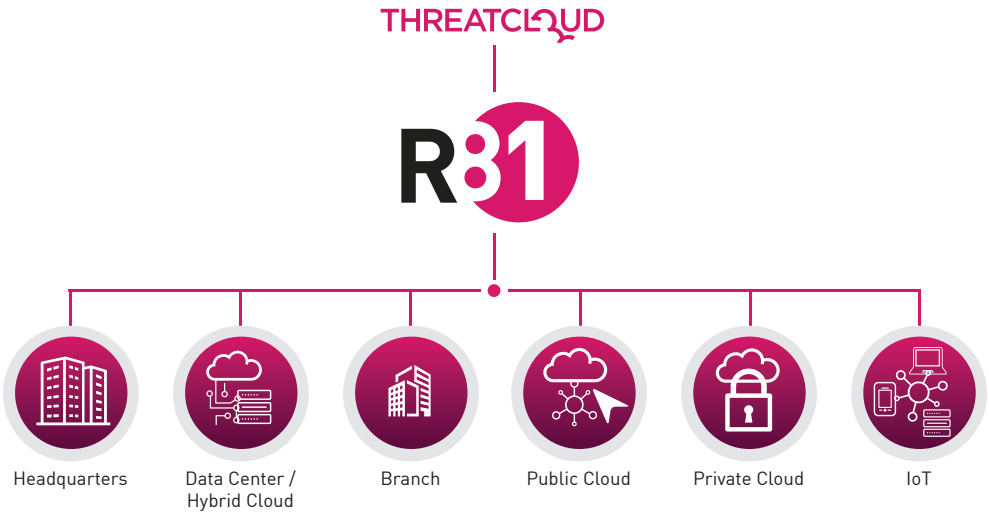


Abbildung 1: Bereitstellung von R81

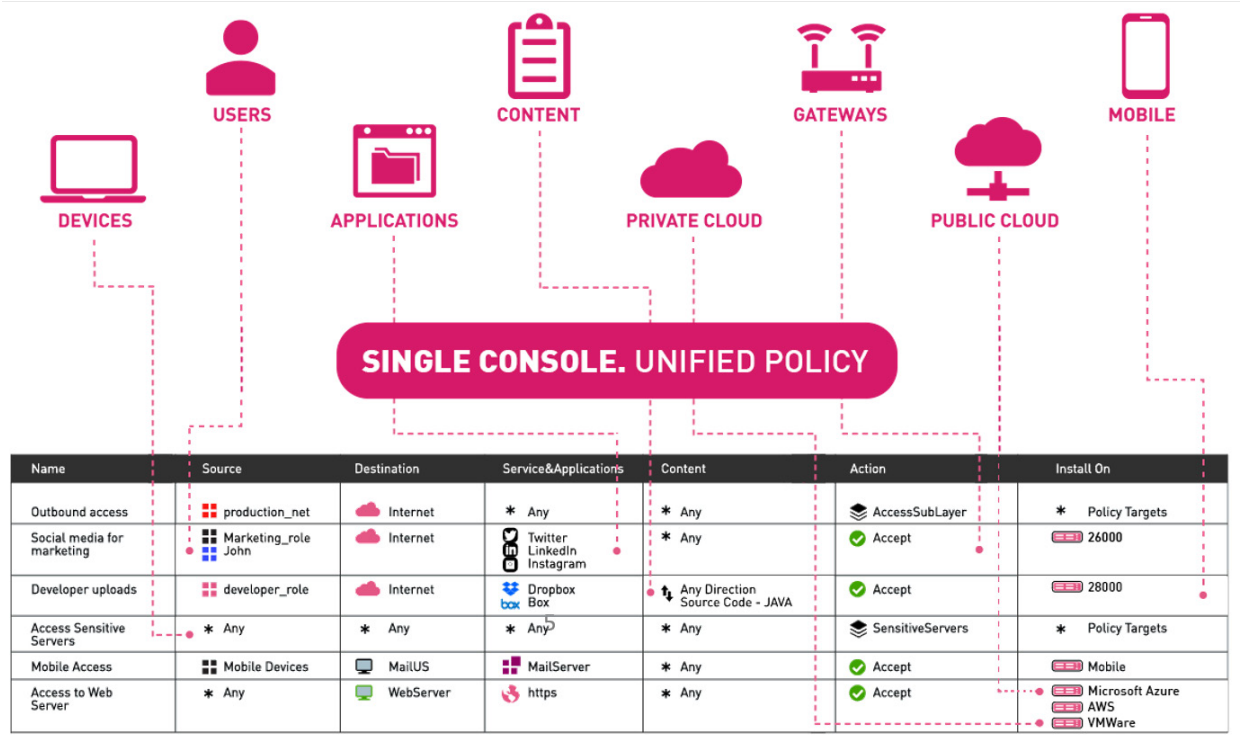
Einführung in eine neue Welt voller neuer Möglichkeiten

R81 vereinfacht diese Komplexität mit intuitiven Richtliniensteuerungen und ermöglicht eine zentrale und skalierbare Sicherheit mit Einblick in die Sicherheitslage des Unternehmens. Außerdem werden Sicherheitsadministratoren mit Werkzeugen ausgestattet, um Risiken und Bedrohungen zu minimieren und dennoch einen sicheren Zugriff auf Unternehmensressourcen zu ermöglichen.

HIGHLIGHTS

R81 bietet:

- Eine Konsole zur Verwaltung aller Netzwerksicherheitsaspekte, vom Zugriff bis hin zu Bedrohungsabwehrrichtlinien.
- Ein Höchstmaß an Sicherheit mit autonomer Bedrohungsprävention: R81 ist das erste KI-gesteuerte Sicherheitsrichtliniensystem, welches Schutz vor Zero-Day-Angriffen bietet.
- Schnelle Reaktion auf sich ändernde Sicherheitsanforderungen mit schnellster Richtlinieninstallation – Reduzierung der Installationszeit für Richtlinien um bis zu 90 % auf nur 10 Sekunden.
- Optimale Sicherheit für verschlüsselten Netzwerkverkehr (SSL): R81 verwendet die neuesten Standards für sichere Konnektivität (TLS 1.3 und HTTP/2). Eine dedizierte Richtlinienschicht ermöglicht es dem Administrator, die Entscheidung zur Überprüfung oder Umgehung des Netzwerkverkehrs einfach zu steuern.
- Richtlinienverwaltung der nächsten Generation, einschließlich intuitiver Richtliniensegmentierungsfunktionen (Inline Shared Policy), für eine bessere Verwaltung.
- Delegation und Zusammenarbeit ermöglichen es mehreren Administratoren, gleichzeitig und konfliktfrei an der gleichen Regelbasis zu arbeiten.
- Zero-Touch-Bereitstellung ermöglicht großen Unternehmen die effiziente Bereitstellung von Sicherheit.



R81 bietet einen vereinfachten Ansatz für die Verwaltung aller Netzwerksicherheitsaspekte einer bestimmten Organisation, unabhängig davon, wo die Durchsetzungspunkte eingesetzt werden. Dabei kann es sich um physische Geräte handeln, die die WAN-Randbereiche und internen Netzwerkgrenzen schützen, oder um virtuelle Anwendungen, die private, öffentliche und hybride Cloud-Umgebungen sowohl in Nord-Süd- als auch in Ost-West-Richtung schützen, sowie um Cloud FWaaS, um entfernte oder mobile Mitarbeiter und Büros sicher mit dem modernen Unternehmensnetzwerk zu verbinden.

Administratoren können Netzwerksegmentierung und Zugriffskontrolle, URL-Filterung, Anwendungskontrolle, Identity Awareness und Data Loss Prevention (Überprüfung des ein- und ausgehenden Datenverkehrs) innerhalb einer einzigen Regel und einer minimalen Anzahl von Konfigurationsmenüs für alle Durchsetzungspunkte konfigurieren. Zusammen mit der Verwendung von dynamisch definierten Objekten in der gesamten Sicherheitsrichtlinie (sowohl für Zugriffs-, HTTPS- als auch NAT-Richtlinien) ist dieser imperative Ansatz eine Reaktion auf die sich ständig verändernde Bedrohungslandschaft und die damit verbundenen Herausforderungen für das Unternehmen und verbessert Ihre allgemeine Sicherheitslage.

CHECK POINT
INFINITY

Wie Einsatz und Skalierbarkeit mit R81 funktionieren

Die Cyber Security Management Plattform R81 kann über virtuelle Anwendungen, speziell entwickelte Smart-1-Anwendungen oder als Cloud-Service über die Smart-1-Cloud-Plattform bereitgestellt werden, die über das Infinity Portal von Check Point verfügbar ist.

Hardware

Die R81 Management Suite kann auf dedizierten Smart-1 405 | 410 | 625 | 6000-L | 6000-XL Geräte eingesetzt werden, die für Leistung und Skalierbarkeit optimiert sind und deren Hardware und Betriebssystem von Grund auf gestärkt sind.

Virtuelle Geräte

Die R81 Management Suite kann als virtuelles Gerät auf VMware ESXi™, KVM und Microsoft Hyper-V® oder in öffentlichen Cloud-Umgebungen, einschließlich Google Cloud Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure® und Azure GovCloud, bereitgestellt werden.

Sicherheitsmanagement aus der Cloud

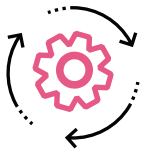
Angepasst an die individuellen Bedürfnisse jedes Unternehmens, egal ob sich der Administrator im Büro oder an einem anderen Ort befindet. Smart-1-Cloud führt volle Funktionsparität mit R81 ein und bietet eine dynamische Managementschnittstelle, die sich je nach Bedarf erweitert und keinerlei Wartung erfordert.

Verwalten von Plattform-Updates

Nach der Bereitstellung und Konfiguration von R81 werden alle weiteren Wartungsaspekte im Zusammenhang mit der Bereitstellung neuer Pakete und Sicherheitsgateway-Aktualisierungen von dem zentralen Bereitstellungstool übernommen. Das R81 Central Deployment Tool ermöglicht die Durchführung von Upgrades zwischen Hauptversionen (sowie alle Arten von Hotfixes) nativ über die SmartConsole. Administratoren können diese Erweiterung nutzen, um den betrieblichen Aufwand für das Upgrade ihrer VSX-Gateways, Cluster-Gateways oder einzelner Standorte zu reduzieren. Ob große oder Hotfix-Installation, beim Upgrade von Clustern wird es auf dem Standby-Cluster-Mitglied installiert, dieses Mitglied neu gestartet und ohne Paketverlust oder Beeinträchtigung des Datenverkehrs auf das nunmehrige Standby-Mitglied verschoben.

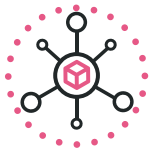
Die vier Säulen:
Bausteine der R81 Cyber Security Plattform

Auf die Frage, was ihrer Meinung nach der beste Ansatz für die Verbesserung der Sicherheit in ihren Organisationen wäre, gaben 69 % an, die Konsolidierung auf weniger Sicherheitsanbieter zu bevorzugen.



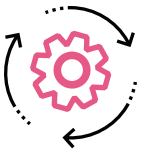
Automatisierte Sicherheit

Konsolidierte Sicherheit



Dynamisch

Effizienter Betrieb



Automatisierte Sicherheit

Die Effektivität des Cyber Security Managements wird an der Fähigkeit gemessen, routinemäßige Sicherheitsaufgaben zu automatisieren. Die Automatisierung der Sicherheit schafft agile Sicherheit, die Administratoren bei ihrer täglichen Arbeit unterstützt. Es kann die Arbeitsbelastung des Cybersicherheitsteams reduzieren und es ihnen ermöglichen, sich auf strategischere Aufgaben zu konzentrieren.

Die Automatisierung erfolgt durch die Verwendung von APIs, Skripten oder Playbooks auf der Grundlage von Best Practices und wird zur programmatischen Wiederholung einer Vielzahl von Sicherheitsvorgängen verwendet. Dies beginnt häufig mit allgemeinen Aufgaben zur Änderung von Richtlinien wie dem Erstellen von Objekten und Richtlinienregeln oder Sicherheitsprofilen. Mit den richtigen Sicherheitstools und dem Cyber Security Management lassen sich komplette Sicherheitsarchitekturen in Cloud-Umgebungen auf Knopfdruck implementieren.

Ein häufiger Anwendungsfall für die Automatisierung ist die Erstellung von Self-Service-Portalen für Cybersicherheitsoperationen. Durch die Verwendung verfügbarer APIs können Webportale erstellt werden, die es nicht geschultem Personal wie Helpdesk- und Systemadministratoren ermöglichen, der Richtlinie spezifische Regeln hinzuzufügen. Dies trägt zur Verbesserung der Produktivität bei, indem schnellere Arbeitsabläufe geschaffen werden, die den Zeitaufwand für die Verwaltung von Sicherheitsvorgängen verringern.

Ein weiterer Anwendungsfall ist die starke Integration mit Automatisierungs-Tools wie Ansible oder Terraform, um mehrere Admin-Funktionen in einem oder mehreren Vorgängen auszuführen (R81 ermöglicht das Hinzufügen oder Löschen von bis zu 27 Objekttypen innerhalb eines einzigen API-Aufrufs) oder einem bestimmten Playbook zu folgen, um eine neue Richtlinie zu erstellen, einschließlich Netzwerkobjekten, Diensten und Zugriffsrichtlinienschichten wie Application Control und URL-Filterung, und diese auf ausgewählten Sicherheits-Gateways zu installieren.

Infrastructure as Code (IaC)

Infrastructure as Code (IaC) ist der Prozess zur Verwaltung und Bereitstellung von Computer-Rechenzentren über maschinenlesbare Definitionsdateien anstelle von physischer Hardware-Konfiguration oder interaktiven Konfigurations-Tools. Private und öffentliche Cloud-Infrastrukturen werden durch einen solchen Prozess mit Hilfe von Skripten oder deklarativen Definitionen im Code verwaltet, anstelle von manuellen Prozessen. IaC ist daher ein wesentlicher Bestandteil für die Public Cloud, mit dem komplexe Rechenzentren durch die richtige Modellierung des Geschäftsprozesses aufgebaut werden können.

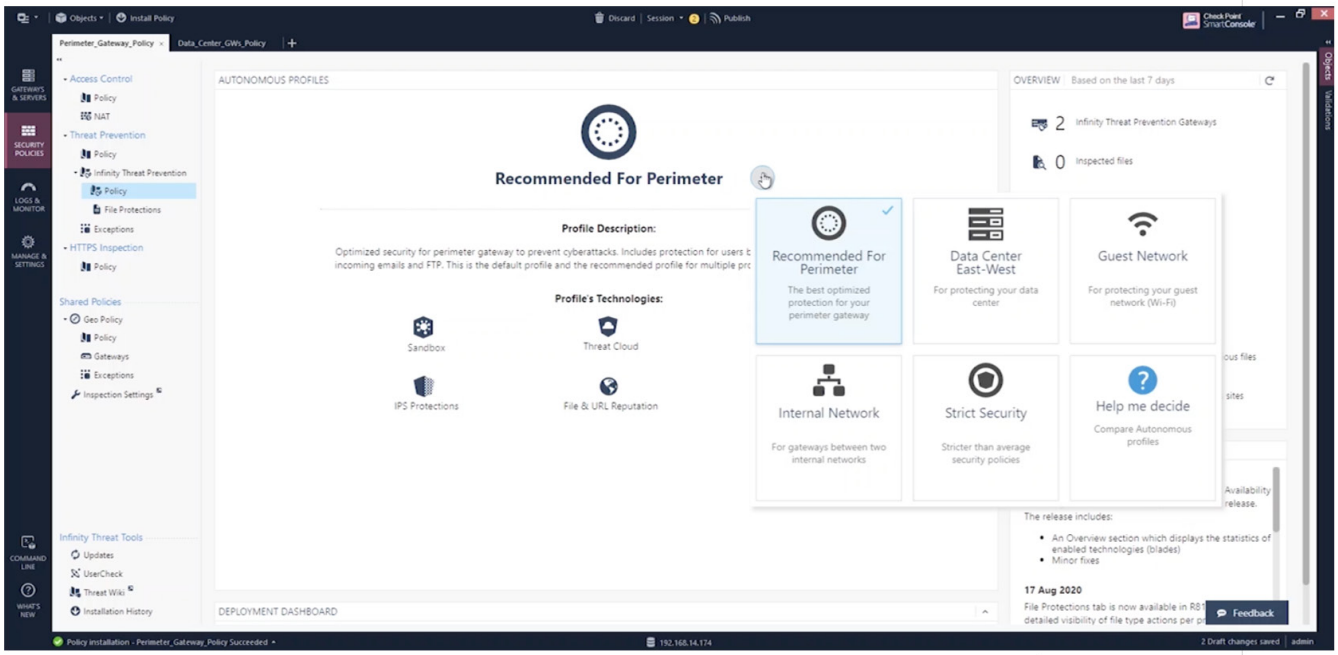
Das Sicherheitspersonal bewältigt täglich eine Flut von Warnmeldungen und verlässt sich möglicherweise auf manuelle und inkonsistente Prozesse, die mit den sich weiterentwickelnden Technologien, die von Kriminellen eingesetzt werden, einfach nicht mithalten können. Security Orchestration, Automation and Response (SOAR) verbindet Mitarbeiter des Security Operations Center (SOC) mit Check Point-Produkten, um jeden Schritt bei der Erkennung und Reaktion zu rationalisieren und manuelle Prozesse durch automatisierte Workflows zu ersetzen, die eine optimierte Triage, Untersuchung und Eindämmung gewährleisten.

Autonome Bedrohungsprävention

Da die Sicherheitsrichtlinien immer umfangreicher und ausgeklügelter werden, wird die Konfiguration der am besten geeigneten Sicherheitsmaßnahmen immer komplexer. Administratoren müssen zusätzliche Zeit investieren, um herauszufinden, was die beste Sicherheitskonfiguration ist. Was wäre, wenn es anstelle von viel manueller Arbeit einen schnelleren, automatisierten Weg gäbe, Sicherheitsprofile zu definieren? R81 stellt das branchenweit erste autonome System zur Bedrohungsprävention vor, das von Check Point Research entwickelt wurde: Infinity Threat Prevention.

- KI-gesteuerte Sicherheitsrichtlinien zum Schutz vor Zero-Day-Angriffen
- Implementierung von Best Practices mit einem einzigen Klick
- Security Gateways werden sofort konfiguriert
- Richtlinien werden kontinuierlich und automatisch aktualisiert

Infinity Threat Prevention reduziert den Verwaltungsaufwand erheblich und stärkt die Sicherheitslage des Unternehmens durch Bereitstellung von fünf sofort einsatzbereiten Richtlinienprofilen, die speziell auf verschiedene Segmente im Unternehmensnetzwerk zugeschnitten sind. In jedem Profil sind unterschiedliche Präventionstechnologien und Schutzmaßnahmen aktiviert, unterschiedliche Protokolle gescannt, die alle die Best Practices repräsentieren, die von Check Point als die relevantesten für das geschützte Segment ermittelt wurden.



Für Sicherheitsadministratoren bedeutet das:

- Keine routinemäßige Wartung erforderlich
- Konfigurationen mit einem Klick einstellen und vergessen
- Sicherheit stets auf dem neuesten Stand mit den neuesten Zero-Day-Schutzmaßnahmen und Best Practices

Wenn eine bestimmte Organisation ein Sicherheits-Gateway zum Schutz des Perimeters und ein anderes Gateway zum Schutz der Cloud-Rechenzentren hat, wird das Profil „Recommended for Perimeter“ (Empfohlen für Perimeter) für die Perimeter-Gateways und das Profil „Data Center East-West“ (Rechenzentrum Ost-West) für das as zweite ausgewählt. Nach der Installation der Richtlinie werden die Gateways sofort gemäß den Best Practices von Check Point konfiguriert und setzen automatisch neue Funktionen, erweiterte Schutzmaßnahmen und andere Best Practices durch.

Der Administrator kann die geschützten Netzwerke entsprechend der eigenen Richtlinie anpassen und das Profil schrittweise in seiner IT-Umgebung einsetzen, während alle anderen Netzwerke im Modus „Detect only“ (nur erkennen) sind, und erst später auf „All“ (Alle) ändern, um gemäß dem Profil geschützt zu werden.

Konsolidierte Sicherheit

Nur eine konsolidierte Sicherheitsarchitektur kann der Raffinesse und dem Umfang der heutigen Cyberangriffe entgegenwirken, indem sie alle Sicherheitsdurchsetzungspunkte sowohl aus der Managementperspektive als auch aus der Perspektive der geteilten Informationen zusammenführt. Die Kommunikation von Erkenntnissen über verdächtige Aktivitäten zwischen den verschiedenen Durchsetzungspunkten (ob vor Ort, in der Cloud, mobil oder am Endpunkt) ist unabdingbar, um die Bedrohungslandschaft eines Unternehmens zu verstehen und das damit verbundene Risiko zu managen.

Das R81 Cyber Security Management befindet sich im Kern der konsolidierten Sicherheitsarchitektur von Check Point und ermöglicht es dem Sicherheitsadministrator, in jedem Segment des Unternehmens das gleiche Sicherheitsniveau zu gewährleisten. Es bietet eine einheitliche Sicht auf die Konfiguration von Sicherheitsrichtlinien und die Sichtbarkeit von Bedrohungen über Netzwerke, Endpunkte, mobile Geräte, IoT-Geräte und Clouds (öffentlich, privat und hybrid) hinweg und setzt die entsprechenden Zugriffs- und/oder Bedrohungsschutzrichtlinien an den relevanten Durchsetzungspunkten ein.

Das Prinzip der Konsolidierung wird auch dadurch erreicht, dass alle Durchsetzungspunkte bei Bedarf dieselben Informationsströme nutzen. Der ThreatCloud Intelligence Data Lake wird dynamisch aktualisiert, wobei die Feeds aus einem Netzwerk von globalen Bedrohungssensoren, Angriffsinformationen von Gateways weltweit und Malware-Feeds aus den Forschungslaboren von Check Point verwendet werden. Basierend auf den daraus resultierenden Sicherheitsinformationen werden aktualisierte Schutzmaßnahmen und Signaturen erstellt und an alle Durchsetzungspunkte übermittelt.

Benutzerdefinierte Intelligenz-Feeds

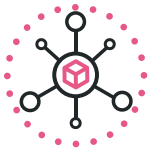
Mit R81 kann der Administrator benutzerdefinierte Intelligence Feeds überwachen oder Indicators of Compromise (IoCs) mit minimalem Overhead direkt über die SmartConsole verwalten. Administratoren können benutzerdefinierte Feeds entsprechend den Anforderungen des Unternehmens hinzufügen, löschen und ändern, indem sie ein spezielles Menü zur Verwaltung und zum Abrufen von Feeds von einem Server eines Drittanbieters direkt zum Security Gateway bereitstellen, die später von den Anti-Virus- und Anti-Bot-Technologien durchgesetzt werden.

Konsolidierte Überwachung des Datenverkehrs und verbesserte Indizierungsfähigkeiten

Das Menü für Protokolle und Überwachung bietet eine umfangreiche und anpassbare interaktive Ansicht aller Netzwerk- und Sicherheitsaktivitäten, die auf physischen/internen Gateways, Cloud-basierten Gateways, End-/Mobilgeräten und IoT aufgezeichnet wurden. Administratoren können den Bereich der Rohprotokollansicht verwenden oder eine der vordefinierten Ansichten im Ansichten-Untermenü wählen. Jede Ansicht ist ein interaktives Dashboard, das aus mehreren anwählbaren Widgets besteht, die anpassbare Bereiche bilden und dem Administrator einen Überblick über das Netzwerk und die Ereignisse basierend auf verschiedenen Themen bieten, z. B. Remote-Benutzer, MITRE Att&ck (mit einer grafischen Darstellung einer aktualisierten MITRE-Heatmap, um die wichtigsten Techniken zu lokalisieren und zu den relevantesten aufzuschlüsseln) oder Bedrohungsprävention.

R81 führt eine verbesserte Admin-Erfahrung bei der Suche nach Schlüsselwörtern ein, da die Indizierungs-Engine **Solr 7.7** die Leistung der Indizierungs- und Berichtsmechanismen deutlich verbessert. Dadurch können Sicherheitsadministratoren mit einer vordefinierten, intuitiven und einfachen Abfragesyntax reibungslose und schnelle Protokollabfragen, Berichte und Ansichten für die gesamte Umgebung erstellen.

Solr ist besonders zuverlässig, skalierbar und fehlertolerant und bietet verteilte Indizierung, Replikation und lastverteilte Abfragen, automatisiertes Failover und Recovery, zentralisierte Konfiguration und mehr. Solr ist die Basis für die Such- und Navigationsfunktionen einer Vielzahl der weltweit größten Internetseiten.



Dynamisch

Im Gegensatz zu traditionellen Netzwerken, die statisch sind und sich kaum verändern, ist das moderne Netzwerk virtualisiert, dynamisch und grenzenlos. In einem modernen Netzwerk können neue Anwendungen überall bereitgestellt werden. Virtuelle Instanzen können jederzeit aktiviert, repliziert, ersetzt oder zwischen Rechenzentren und Clouds migriert werden. Das heißt, dass alles dynamisch wird und sich Attribute wie IP-Adressen im Handumdrehen ändern können. Dies erfordert einen dynamischen Weg zur Steuerung, Sicherung und Überwachung solcher Umgebungen.

R81 ermöglicht dynamische Sicherheit über dynamische Objekte (Dynamic Objects), indem es die automatische Bereitstellung von Sicherheits-Gateways auf jedem Hypervisor und jeder Cloud ermöglicht. Außerdem werden bei Änderungen in der Cloud-Umgebung die Durchsetzungspunkte in der Umgebung automatisch aktualisiert, um einen Schutz in Echtzeit zu gewährleisten.

Dynamische Objekte

Über vertrauenswürdige APIs verbindet sich die R81 CloudGuard Controller-Komponente mit dem Software-Defined-Data-Center (SDDC) und bindet die virtuelle Cloud-Umgebung ein. Alle Assets, einschließlich Sicherheitsgruppen und Tags, werden auf den Management-Server importiert und können als Teil des Konfigurationsprozesses der Zugriffsrichtlinien verwendet werden.

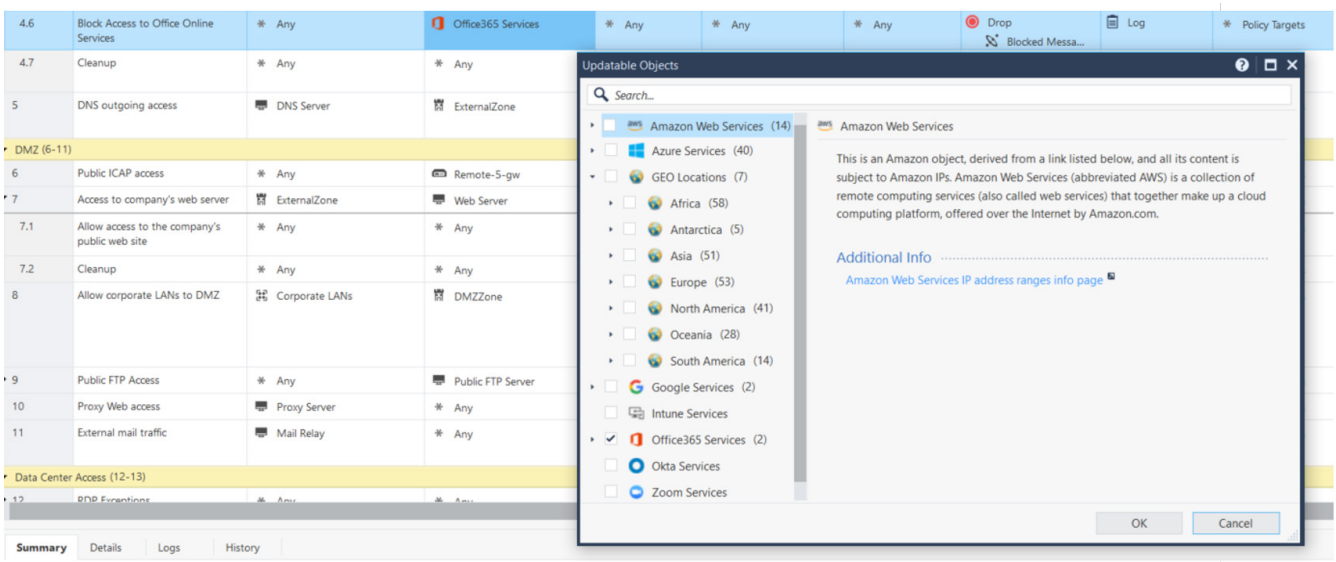
Die Steuerungsinfrastruktur wird auch verwendet, um die IoT-Discovery-Engine aller wichtigen Hersteller für die automatische Gerätezuordnung und -klassifizierung zu integrieren und letztendlich granulare IoT-Richtlinien zu generieren, die im gesamten Netzwerk angewendet werden können (z. B. kann ein Drucker eines bestimmten Herstellers nur über ein autorisiertes Protokoll mit dem ePrint-Dienst kommunizieren).

Identitäts-Tags

Eine Erweiterung des Identitäts- und Zugriffsbereichs, mit der Sie externe Identifikatoren (z. B. Cisco® Security Group Tags oder andere von einer beliebigen Identitätsquelle bereitgestellte Gruppen) in den Abgleich der Zugriffsrollen einbeziehen können. Diese externen Identifikatoren funktionieren wie ein Tag, der einem bestimmten Benutzer, einer Maschine oder einer Gruppe zugewiesen werden kann.

Aktualisierbare Objekte

R81 verlässt sich auf den Cloud-Service von Check Point, um IPs für Länder und gängige SaaS-Dienste wie Microsoft Office 365 automatisch zu aktualisieren. Das Gateway ruft regelmäßig Informationen ab, so dass bei der Verwendung in einem Prozess zur Durchsetzung von Richtlinien die genauesten Daten verwendet werden. Wenn eine Verbindung mit einem aktualisierbaren Objekt übereinstimmt, setzt das Gateway den Namen und das Merkmal dieses Objekts in spezielle Felder des Protokolls. Wenn Sie auf ein Protokoll doppelklicken, können Sie diese sehen.



Der andere Mechanismus für aktualisierbare Objekte ist die UI-Auflösung von Check Point für IPs nach Ländern. Diese basiert auf einer kontinuierlich aktualisierten Datei. Die Auflösung erfolgt bei der Abfrage des Log-Servers und liefert Informationen für jede IP, auch wenn sie nicht mit den geografischen Schutz- bzw. aktualisierbaren Objekten übereinstimmt.

HTTPS-Prüfung

Ab R80.40 ist eine HTTPS-Inspektionsrichtlinie als Schicht verfügbar, die entweder wiederverwendet werden kann oder für ein bestimmtes Richtlinienpaket einzigartig ist. Außerdem werden aktualisierbare Objekte unterstützt, so dass Administratoren ihre Regeln für angeheftete Zertifikatsanwendungen mithilfe von verwalteten aktualisierbaren Objekten konsolidieren können. Check Point hat eine Liste von HTTPS-Diensten zusammengestellt, von denen bekannt ist, dass sie in Szenarien verwendet werden, in denen die HTTPS-Inspektion nicht in der Lage ist, das Vertrauen zwischen dem Client und dem Security Gateway herzustellen und daher den Datenverkehr nicht untersuchen kann. Diese HTTPS-Dienste sind Teil des aktualisierbaren Objekts „HTTPS services - bypass“ (HTTPS-Dienste – Bypass).

In den letzten Versionen wurden viele Verbesserungen vorgenommen, darunter die Unterstützung von TLS 1.3 und die sichere Handhabung von SNI (Server Name Indication) (patentierte Technologie). Wenn wir uns die Zertifikatsdetails genauer ansehen, sind möglicherweise mehrere DNS-Namen aufgeführt, da sie alle dasselbe Zertifikat verwenden. Daher ist die Verwendung des im Zertifikat aufgeführten allgemeinen Namens (Common Name, CN) kein zuverlässiger Anhaltspunkt, wenn das Feld für den alternativen Namen (Subject Alternative Name, SAN) verwendet wird, um mehrere verschiedene Standorte abzudecken. Die Verwendung von SNI, anstatt sich auf den CN des Zertifikats zu verlassen, liefert spezifischere und genauere Informationen über die angeforderte Webseite.

Wir verlassen uns derzeit auf die nicht verschlüsselte SNI-Erweiterung für den Abgleich der Regelbasis, die mit dem Serverzertifikat verifiziert wird.

NAT-Richtlinie

R81 führt eine neue dynamische NAT-Regelbasis ein, die Zugriffsrollen unterstützt, die verschiedene Netzwerke, Benutzer oder Maschinen durch Angabe einer Gruppe oder eines Identitäts-Tags, eines aktualisierbaren Objekts, von Domain-Objekten und Sicherheitszonen repräsentieren, um erweiterte NAT-Richtlinien mit mehr Flexibilität und weniger Komplexität zu erstellen. Beispielsweise kann ein aktualisierbares Objekt „Office365 Services" (Office365-Dienste) verwendet werden, um eine statische No-NAT-Regel zu generieren, bei der der gesamte interne Datenverkehr oder der von der HR-Zugangsrolle generierte Datenverkehr für Office365 bestimmt ist, nicht mit NAT versehen wird.

Der andere Mechanismus für aktualisierbare Objekte ist die UI-Auflösung von Check Point für IPs nach Ländern. Diese basiert auf einer kontinuierlich aktualisierten Datei. Die Auflösung erfolgt bei der Abfrage des Log-Servers und liefert Informationen für jede IP, auch wenn sie nicht mit den geografischen Schutz- bzw. aktualisierbaren Objekten übereinstimmt.

Generisches Rechenzentrum

Die Funktion „Updatable Objects" (Aktualisierbare Objekte) wurde in R80.20 eingeführt und hat aufgrund ihres Beitrags zur Betriebseffizienz (null Wartung) sehr schnell an Popularität gewonnen. Aktualisierbare Objekte stellen beliebte Services und öffentliche Cloud-Plattformen dar, aber das ist vielleicht nicht genug.

Wenn der Administrator benutzerdefinierte externe IP-Feeds konsumieren möchte, seine eigenen Feeds erstellt oder die Zugriffsverwaltung an seine Kollegen delegieren muss, ist das generische Rechenzentrum die richtige Antwort. Diese Funktion wurde in R81 eingeführt und nutzt die dynamische Datencenter-Infrastruktur (wenn Daten an der Quelle geändert werden, wird das Sicherheits-Gateway nahezu in Echtzeit mit den Änderungen aktualisiert).

Anwendungsfall: Die DevOps-Teams erstellen und löschen massenhaft Maschinen, was einen hohen Aufwand für das Sicherheitsteam und die Ticket-Bürokratie zur Folge hat. Jetzt können Sicherheitsadministratoren ein Objekt definieren, das den JSON-Feed repräsentiert, der alle IPs enthält, die Zugriff benötigen. Dieses Objekt muss nur einmal in der Richtlinie installiert werden und alle nachfolgenden Änderungen werden dann automatisch durchgeführt. Dies führt zu null Tickets und macht den Sicherheitsadministrator vom Geschäftsverhinderer zum Befähiger und was noch wichtiger ist: Es macht die DevOps-Teams glücklich.

Rechenzentrum-Abfrageobjekte

Mit Rechenzentrums-Abfrageobjekten können Administratoren jetzt ein Abfrageobjekt basierend auf ausgewählten Attributen über mehrere Rechenzentren hinweg erstellen (Namen, Typen, IP-Adresse oder Tags). Dies vereinfacht und erleichtert die Verwaltung der Richtlinien-Regelbasis, da mehrere Objekte von verschiedenen Cloud-Plattformen in einem einzigen Rechenzentrums-Abfrageobjekt dargestellt werden können. Außerdem können Administratoren die Richtlinie erstellen, noch bevor sie ein Rechenzentrum in der SmartConsole konfigurieren. Dies erleichtert die Verteilung der Zuständigkeiten zwischen Sicherheitsadministratoren und anderen Teams, die möglicherweise Rechenzentren in der SmartConsole erstellen müssen.

Das neue Abfrageobjekt wird auf die gleiche Weise wie die Rechenzentrums-Objekte verwendet. Wie bei Rechenzentrums-Objekten zieht der CloudGuard Controller beim Hinzufügen der Rechenzentrums-Abfrage zur Regelbasis die Assets aus allen Rechenzentren im Abfrageobjekt und aktualisiert das Sicherheits-Gateway entsprechend.

Beispiel 1:
Rechenzentrums-Abfrageobjekt

Gilt für alle aktuellen und zukünftigen Rechenzentren.

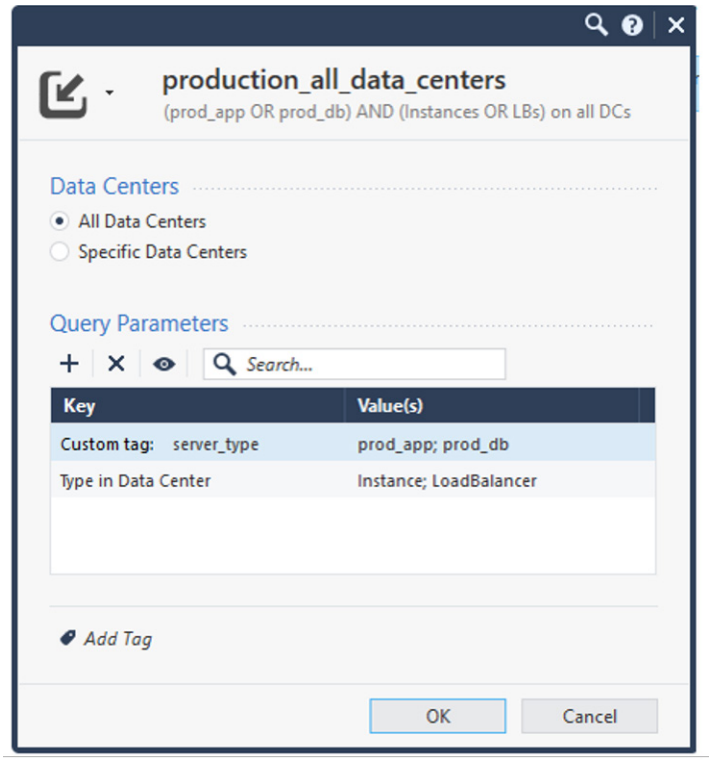
Dies ist die Abfragelogik:

- Alle Assets vom Typ Instanzen ODER Load Balancer
- **UND**
  - Getaggt mit

  "server_type=prod_app"

  OR

  "server_type=prod_db"



Beispiel 2: Regelbasis

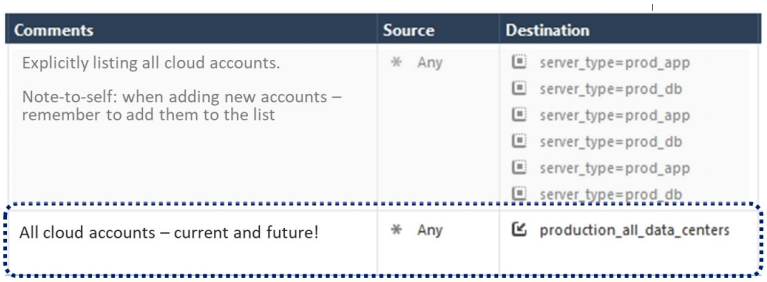
Bei früheren Versionen müssen Sie mehrere Tag-Objekte für mehrere Konten verwenden.

- Die Regeln müssen für jedes hinzugefügte Rechenzentrum aktualisiert werden.
- Regeln können nicht nur die Logik für Instanzen oder Load Balancer haben.

R81 verwendet Rechenzentrum-Abfrageobjekte:

- Die Regel muss nicht aktualisiert werden, wenn neue Rechenzentren hinzugefügt werden.
- Die Regel kann komplexe ODER- und UND-Verknüpfungen enthalten, um die Richtlinie zu verbessern.

R80.X



R81

Effizienter Betrieb

Cyber Security Management Plattformen müssen mit wachsenden Netzwerken, einer steigenden Anzahl von Geräten, disruptiven Technologien und der Komplexität des IT-Betriebs umgehen. Dies erfordert ein intelligentes und effizientes Cyber Security Management, das den Aufwand für das Cyber Security Management reduziert und gleichzeitig die betriebliche Effizienz erhöht.

Richtlinienschichten

Effizienz kann auf viele Arten erreicht werden. Ein Beispiel ist die Segmentierung der Richtlinie in überschaubare Abschnitte. Jeder Abschnitt oder jede Teilrichtlinie kann auf ein anderes Netzwerk oder eine Geschäftsfunktion ausgerichtet werden. Diese Teilrichtlinien können unabhängig voneinander bereitgestellt und von verschiedenen Administrationsteams verwaltet werden, ohne Zugriff auf die gesamte Richtlinie zu gewähren. Dies ermöglicht die Erstellung hochgradig gesicherter Richtlinien und erlaubt gleichzeitig die Verteilung der Arbeitslast zwischen den Teams.

Gleichzeitige Administrator-Sitzungen

Ein weiteres Beispiel für betriebliche Effizienz ist das Erstellen sicherer Workflows, die es mehreren Administratoren ermöglichen, gleichzeitig an derselben Richtlinie zu arbeiten, ohne dass es zu Konflikten kommt. Dies reduziert den Zeitaufwand für die Durchführung von Sicherheitsaufgaben, da sie gleichzeitig durchgeführt werden können ohne das Risiko, die Änderungen der anderen zu überschreiben und ohne Kollisionen.

Mit R81 können mehrere Administratoren an der SmartConsole in der gleichen Domäne, mit den gleichen Richtlinien und sogar an der gleichen Regel und zur gleichen Zeit arbeiten. Um Konfigurationskonflikte zu vermeiden, wird die gesamte Arbeit in Sitzungen durchgeführt. Administratoren können sogar mehrere Sitzungen gleichzeitig geöffnet haben. Dies ist sehr hilfreich, wenn Sie an einem großen Projekt arbeiten und eine dringende Richtlinienänderung vornehmen müssen.

Jede Sitzung ist privat und getrennt von anderen Sitzungen. Änderungen können von anderen Administratoren nicht gesehen werden, bis die Änderungen veröffentlicht werden. Um die Sitzungen privat zu halten, werden Objekte gesperrt, wenn sie von einem Administrator geändert werden. Andere Administratoren sehen nur, dass das Objekt gesperrt ist; sie können es aber nicht ändern. Wenn ein Objekt gesperrt ist, wird der Name des Administrators, der an diesem Objekt arbeitet, angezeigt. Dies hilft den Administratoren, die Arbeit an gemeinsamen Ressourcen zu koordinieren.

Wenn alle Änderungen abgeschlossen sind, gibt der Administrator die Sitzung frei. Erst dann werden die Änderungen öffentlich und für alle anderen Administratoren sichtbar. Nur öffentliche Daten können auf Gateways installiert werden. Alle Änderungen werden sofort in der Datenbank des Management-Servers gespeichert. Bei einer versehentlichen Unterbrechung der Verbindung geht keine Arbeit verloren. Administratoren können Änderungen während einer Sitzung verwerfen, und sie können nach Belieben eine neue Sitzung öffnen.

Änderungsbericht (Sitzungen und Revisionen)

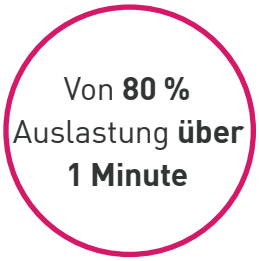
In R81 können wir einen Änderungsbericht generieren, der brauchbare Audit-Daten aller Änderungen zwischen zwei verschiedenen Sitzungen oder aus einer anderen Revision (markiert durch den Vorgang „Publish“ (Veröffentlichen), der eine neue Revision erzeugt) auflistet. Auf diese Weise können wir Vergleiche anstellen, um herauszufinden, welche Änderungen an den Schichten der Zugriffskontrolle oder der Bedrohungsprävention vorgenommen wurden, bevor der letzte Veröffentlichungsvorgang stattgefunden hat. Dies ist äußerst nützlich, wenn beispielsweise jemand eine Änderung vorgenommen hat, die den Ausfall eines bestimmten Dienstes verursacht hat, und der Administrator den Zeitpunkt der Änderung identifizieren muss.

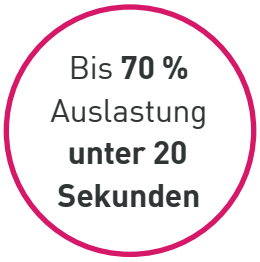
Mehrfach installierte Richtlinien-Sitzungen

Ab R81 können ein oder mehrere Administratoren verschiedene Aufgaben zur Richtlinieninstallation auf mehreren Gateways gleichzeitig ausführen. Bei früheren Versionen können Sie dieselbe Aufgabe zur Richtlinieninstallation nur auf mehreren Gateways gleichzeitig ausführen. Es können maximal 5 Aufgaben zur Richtlinieninstallation (von verschiedenen Richtlinien) gleichzeitig ausgeführt werden. Wenn mehr als 5 Anfragen zur Richtlinieninstallation gesendet werden, wird jede Anfrage, die über die ersten 5 hinausgeht, in eine Warteschlange gestellt. Die aktuell laufenden und die in der Warteschlange befindlichen Aufgaben werden praktischerweise im Fenster „Recent Tasks“ (Neueste Aufgaben) auf demselben Bildschirm angezeigt.

Beschleunigte Installation von Richtlinien

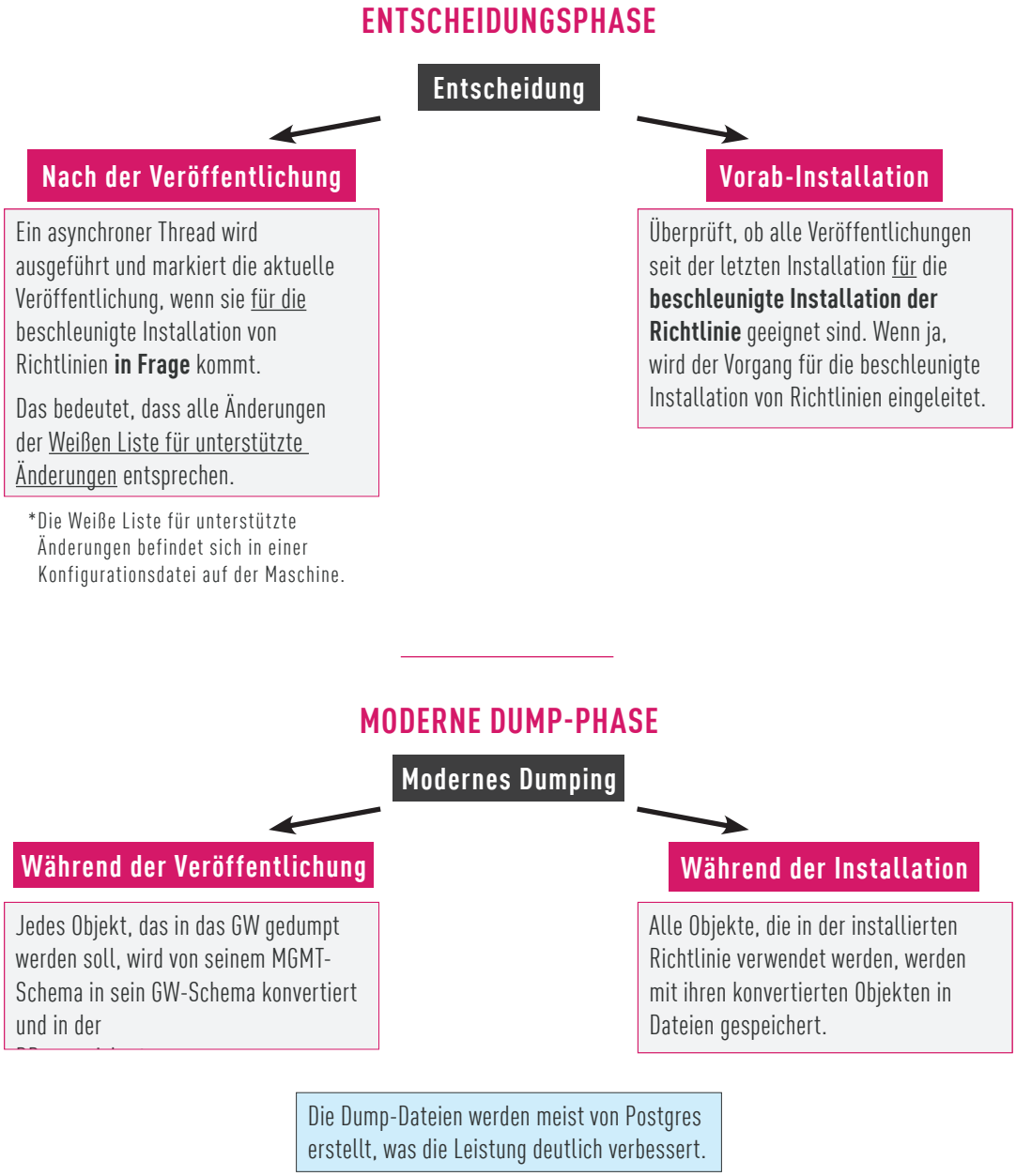
Mit R81 wird die Funktion „Accelerated Install Policy“ (Beschleunigte Installation von Richtlinien) eingeführt. Aufgrund mehrerer Infrastrukturänderungen auf der Seite des Sicherheits-Gateways hat sich die Rechenleistung auf der Verwaltungsseite, die für die Verarbeitung der Sicherheitsrichtlinieninformationen erforderlich ist, drastisch verringert.





Die Richtlinieninstallation wird abhängig von den Änderungen beschleunigt, die seit der letzten Installation an der Zugriffskontrollrichtlinie vorgenommen wurden. Sie wird nur dann beschleunigt, wenn alle seit der letzten Installation vorgenommenen Änderungen alle gängigen Objekte und Objekttypen umfassen (z. B. alle Aktionen, die sich auf geordnete Ebenen und deren Standardspalten, Hosts und Netzwerkobjekte, dynamische und Domänenobjekte, Zugriffsrollen, Rechenzentrumsobjekte, Netzwerkdienst und viele mehr beziehen). In allen anderen Fällen wird die Richtlinieninstallation nicht beschleunigt.

Der Beschleunigungsprozess gliedert sich in zwei Hauptteile, die Entscheidungsphase und den Richtlinien-Dump.



Lizenzen – Automatisches Aktivieren von Lizenzen und Verträgen für alle Produkte von Check Point

Lizenzen und Verträge für Check Point Produkte werden in den meisten gängigen Szenarien automatisch aktiviert und berechtigt, dazu muss der Security Management Server oder das Security Gateway mit dem Check Point User Center verbunden sein. Sollte dennoch Bedarf an einer manuellen Bedienung von Lizenzen bestehen, kann ein Administrator ab R81 Lizenzen direkt in der SmartConsole-Anwendung anzeigen, hinzufügen und löschen.

Zusammenfassung

Sicherheitsmanagement ist der Schlüssel zur Maximierung der Sicherheitseffektivität bei gleichzeitiger Steigerung der betrieblichen Effizienz. Letztendlich ist Ihre Sicherheit nur so stark wie Ihre Fähigkeit, sie zu verwalten.

In diesem Whitepaper haben wir eine Auswahl der wichtigsten Unterscheidungsmerkmale des Sicherheitsmanagements von Check Point beschrieben, um einerseits unsere Fähigkeiten hervorzuheben, andererseits aber auch die vielfältigen Anforderungen zu beleuchten, die für ein echtes Sicherheitsmanagement der Enterprise-Klasse erforderlich sind. Das Cyber Security Management muss auf 4 Säulen aufbauen: Automatisierte Sicherheit, konsolidierte Sicherheit, dynamischer und effizienter Betrieb.

Die Realität zeigt, dass es sehr schwierig ist, Managementlösungen nach der Implementierung zu ersetzen. Daher müssen Sicherheitsexperten bei der Bewertung ihrer Managementanforderungen und der Fähigkeiten ihrer potenziellen Anbieter gründlich und methodisch vorgehen.

Bei Check Point war das Management schon immer eine Kernkompetenz, und wir entwickeln unsere Fähigkeiten ständig weiter, um den Anforderungen unserer Kunden und des Marktes gerecht zu werden.

Weitere Informationen zum Sicherheitsmanagement
von Check Point finden Sie auf der Website
https://www.checkpoint.com/products/unified-cyber-security-platform

Headquarter (weltweit)
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: +972 3-753-4555 | Fax: 972-3-624-1100 | E-Mail: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com