WatchGuard Cloud: Das Konzept

Einführung

Der Einsatz Cloud-basierter Dienste nimmt in allen Segmenten der IT-Branche weiterhin zu, einschließlich kleiner und mittlerer Unternehmen, dezentral aufgestellter Unternehmen und Managed Security Service Providers (MSSPs). Organisationen verlagern ihre Workload in die Cloud, um von Vorteilen wie folgenden zu profitieren: niedrigere Gesamtbetriebskosten, bessere Skalierbarkeit, mehr Sicherheit und höhere Zuverlässigkeit. Jede Organisation hat berechtigte Bedenken, wenn es um die Cloud oder die Implementierung einer eigenen Serverplattform geht. Jeder Administrator, der eine Cloud in Betracht zieht, hat grundlegende Befürchtungen hinsichtlich Datensicherheit, Datenschutz und Datensouveränität.

WatchGuard Cloud ist die neueste as-a-service-Lösung von WatchGuard. Sie hostet die Anwendung AuthPoint für Multifaktor-Authentifizierung und WatchGuard Cloud Visibility für zentralisierte Protokollierung und Berichterstellung der WatchGuard Firebox-Appliances und wird letztlich alle Cloud-basierten Dienste von WatchGuard hosten (einschließlich Threat Detection and Response, DNSWatch und DNSWatchGo). Das gesamte Endpoint-Portfolio ist in eine native Cloud-Plattform integriert, von Panda Adaptive Defense 360 und Endpoint Protection bis hin zu Panda Patch Management und System Management. Wir haben WatchGuard Cloud so entwickelt, dass Sie von allen Vorteilen der Cloud profitieren. Gleichzeitig wird auf Bedenken im Zusammenhang mit dem Speichern von Daten auf einem fremden Computer eingegangen. Durch das Hosten dieser Anwendungen in der Cloud kann WatchGuard die Leistung, Skalierbarkeit und Sicherheit zugrunde liegender Cloud-Dienste nutzen und bietet den Total Security Suite-Kunden den einfachsten Weg eines umfassenden Schutzes.

Well-Architected Framework

WatchGuard Cloud wurde auf Basis der Richtlinien des Amazon Web Services (AWS) Well-Architected Framework entwickelt. Das Well-Architected Framework identifiziert 5 Hauptsäulen für eine robuste Cloud-Bereitstellung: Operational Excellence, Sicherheit, Zuverlässigkeit, Leistung/Effizienz und Kostenoptimierung. In dieser technischen Kurzbeschreibung zeigen wir anhand dieses Framework, wie WatchGuard Cloud die Vorteile der Cloud nutzt, und widerlegen gleichzeitig die gängigsten Einwände. Es ist aufgrund der Natur der Daten, die in WatchGuard Cloud gespeichert werden, besonders wichtig, unseren Ansatz im Hinblick auf Sicherheit und Zuverlässigkeit zu verstehen.

WatchGuard Cloud – Design und 5 Säulen

WatchGuard Cloud und die darin gehosteten Anwendungen nutzen eine Microservices-basierte Architektur mit 3 Schichten, die definiert, wie Daten über das System übergeben werden und verschiedene Funktionen miteinander interagieren. Microservices sind Softwarekomponenten, die eine streng

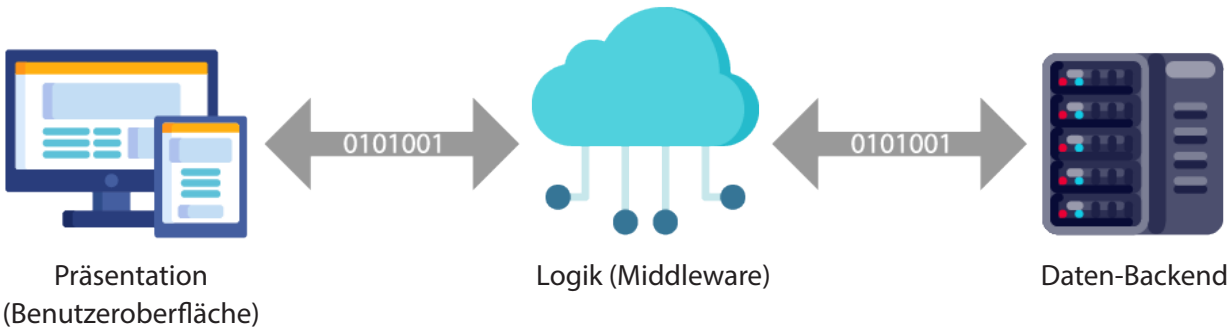

Abbildung 1: Architektur mit 3 Schichten

definierte Funktionalität haben und in unabhängigen Paketen (Containern) gebündelt sind. Jeder dieser Container kann zuverlässig und skalierbar bereitgestellt werden.

Wie im Diagramm gezeigt, ist die Benutzeroberfläche komplett vom Backend-Datenspeicher isoliert und muss über eine Middleware-Ebene zum Lesen oder Ändern von Daten im System kommunizieren.

Operative Spitzenleistung

WatchGuard stellt durch viele Verfahren sicher, dass die Cloud -Plattform in Einklang mit den WatchGuard-Standards sowie den Erwartungen unserer Kunden und Partner arbeitet. WatchGuard nutzt DevOps-Methoden sowie CI/CD-Mechanismen, um sicherzustellen, dass Bug Fixes regelmäßig durchgeführt und neue Funktionen nahtlos bereitgestellt werden. Bereitstellungen werden vor der Produktionsfreigabe in mehreren Umgebungen platziert. Vor dem Abrufen von Updates in jede Phase sind Genehmigungen erforderlich. Computing- und Storage-Instanzen werden unter Verwendung von Infrastructure-as-Code erstellt, sodass wie für jede andere Softwarefunktion Tests und Versionskontrollen erfolgen können. Die Plattform nutzt Anwendungsprotokollierung, wodurch Technik- und Produktteams betriebliche Einblicke erhalten. Auf diese Weise können wichtige Leistungsindikatoren nachverfolgt werden, wie Systemverfügbarkeit für Container und Antwortzeit für Microservices. Auf diese Weise können wir sicherstellen, dass potenzielle Kundenprobleme schnell identifiziert und behoben werden.

Sicherheit

WatchGuard verfolgt das Principle of Least Privilege für die gesamte WatchGuard Cloud-Plattform: von der Steuerung der Dienste, die mit anderen kommunizieren dürfen, über die Informationen, die für einen bestimmten Account angefordert werden können, bis zu den Berechtigungen, die verschiedene Nutzer auf der Web-Benutzeroberfläche haben. Für Microservices werden sehr eingegrenzte Berechtigungen gewährt – unter Verwendung von Identity and Access Management(IAM)-Richtlinien, die den Zugriff auf Backend-Systeme und -Server verhindern (mit Ausnahme derer, für die sie explizit eine Berechtigung haben). Diese Berechtigungen werden vom DevOps-Team verwaltet und auditiert. So wird die unkontrollierte Zunahme von Richtlinien verhindert. WatchGuard Cloud-Entwicklern stehen folglich nur die Dienste bereit, die sie für die Implementierung von Funktionalität benötigen.

WatchGuard Cloud schützt alle Daten im System durch die Verschlüsselung aktiver und inaktiver Daten. Während der Aufnahme werden alle Daten mit TLS unter Verwendung privater Zertifikate verschlüsselt, um Hijacking oder Man-in-the-Middle-Angriffe zu vermeiden. Alle in WatchGuard Cloud gehosteten Client-Anwendungen nutzen AWS IoT, um sichere Kommunikationskanäle einzurichten. Diese werden verwendet, um Informationen zwischen Remote-Agents, wie AuthPoint-Gateways oder WatchGuard Fireboxes, und der Cloud zu übertragen. Von Nutzern erstellte Tunnel sind nicht erforderlich. In der Cloud sind die Daten entweder logisch oder kryptographisch getrennt – abhängig von der geplanten Verwendung der Daten und den Leistungsanforderungen. Daten, die schnell für mehrere Accounts abgerufen oder aggregiert werden müssen, werden in verschiedenen Berichterstellungsdatenbanken gespeichert. Diese sind über einen WatchGuard-Schlüssel verschlüsselt. Daten, die länger gespeichert werden sollen, werden mit einem Schlüssel verschlüsselt, der spezifisch für den Account des Mandanten (Kunde oder Partner) ist. Alle Datenabrufanforderungen umfassen ein Token, das Informationen zum Account und zur Rolle des Nutzers enthält. Dieses Token wird durch die Middleware und den Datenspeicher validiert, um sicherzustellen, dass der Benutzer die korrekten Berechtigungen zum Abrufen oder Ändern der Daten hat.

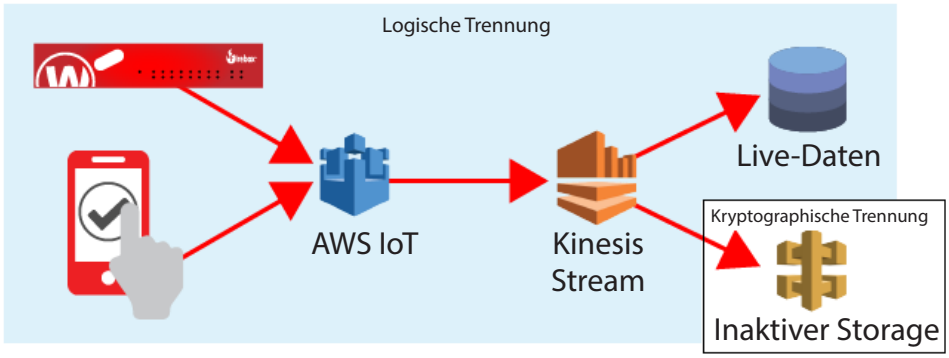

Abbildung 2: Sichere Kommunikation

WatchGuard hat kaum Einblicke in die Nutzerkomponente der Plattform und kann nur Informationen anzeigen, die mit dem Betrieb der Plattform und der zugrunde liegenden Anwendungen zusammenhängen. WatchGuard kann keine partner- oder kundenspezifischen Anwendungsinformationen aus der Plattform anzeigen, ohne dass der Nutzer dem WatchGuard-Support oder Technikern explizit Zugriff gewährt. Die Aufbewahrung von Anwendungsdaten im System hängt von der Abonnementstufe des Kunden ab und kann zwischen Anwendungen oder sogar Geräten variieren. Während der Produktaktivierung der ersten Cloud-Lizenz des Kunden werden dem Nutzer verschiedene geographisch verteilte Rechenzentren präsentiert, in denen ihre anwendungsspezifischen Daten gespeichert werden. Die unterstützten Rechenzentren sind Vereinigte Staaten (USA) für Nord-, Mittel- und Südamerika, Deutschland (DEU) für Europa, den Nahen Osten und Afrika sowie Japan (JPN) für Asien. Sobald eine Region ausgewählt wurde, können keine Änderungen mehr vorgenommen werden; Kunden, die Daten in mehreren Regionen speichern möchten, sollten individuelle Accounts erstellen, die der gewünschten Region entsprechen, und Produkte im entsprechenden Account aktivieren. Metadaten für Accounts, Systemnutzer und Lizenzierungsinformationen werden auf WatchGuard-Servern in den Vereinigten Staaten gespeichert und über sichere, virtuelle private Netzwerke verschlüsselt und in die Cloud übertragen.

Zuverlässigkeit

WatchGuard nutzt viele Prozesse und Dienste, um sicherzustellen, dass WatchGuard Cloud bei Bedarf verfügbar ist. Wie oben erwähnt, verwendet WatchGuard Cloud eine Kombination aus Infrastructure-as-Code, Containerization, automatischer Skalierung und Anwendungslastausgleich, um Ausfallzeiten auf ein Minimum zu reduzieren, selbst während Systemupdates. Die zugrunde liegenden Server werden mit automatischen Skripts instanziiert, um sicherzustellen, dass Bereitstellungen konsistent, wiederholbar und quellgesteuert sind. Jeder Server hostet einen oder mehrere Container, die eine Untergruppe verknüpfter Funktionalität in der Plattform unterstützen. Wenn durch steigende Nachfrage die Serverressourcen strapaziert werden, gehen zusätzliche Server online. Die überschüssige Last wird vom Load

Balancer auf den neuen Server verlagert. Derselbe Mechanismus kann umgekehrt genutzt werden, um Systemupdates durchzuführen oder fehlerhafte Hosts zu isolieren; Server mit neuem Code werden bereitgestellt. Der Load Balancer verlagert Last von den alten Servern und überträgt Verbindungen zu den aktualisierten Containern. Da jeder Server einen begrenzten Funktionalitätssatz hostet, kann die Plattform den problematischen Server bei Erkennung eines Fehlers, der sich auf Dienste auswirkt, isolieren. Das restliche System arbeitet normal weiter.
WatchGuard Cloud nutzt Computing- und Storage-Ressourcen in Kombination mit Multi-Region-Verfügbarkeit in mehreren Availability Zones (AZs) in jeder Region. Dies stellt sicher, dass die Plattform vor einem unwahrscheinlichen Ausfall in großem Umfang geschützt ist, der sich auf das gesamte Rechenzentrum auswirkt. Es werden regelmäßig Snapshots erstellt. Daten können aus dem inaktiven Storage neu geladen werden, um sicherzustellen, dass Datasets vollständig und konsistent bleiben.

Leistung/Effizienz

WatchGuard Cloud sorgt für Leistung/Effizienz, da wir die richtigen Tools für die Plattform sowie den Kunden verwenden. Die Bereitstellung von Umgebungen für mehrere Regionen und die Auswahl der nächstgelegenen Region durch Kunden stellt sicher, dass die Latenz minimal ist. Der Grund hierfür: Die Computing- und Storage-Ressourcen befinden sich in der Nähe des Nutzers. Durch das Vorhandensein mehrerer Regionen kann WatchGuard ferner Systemupgrades außerhalb der Stoßzeiten für jede Region planen, sodass die Auswirkungen auf die Nutzer minimal sind.
Ein großer Vorteil des Wechsels zur öffentlichen Cloud ist der große Katalog an verwalteten Diensten. WatchGuard Cloud nutzt AWS IoT für die Kommunikation zwischen der Plattform und Remote-Elementen, wie Fireboxes oder AuthPoint-Agents. Dieser Dienst bedeutet, dass WatchGuard keine Techniker für die Entwicklung und Wartung eines sicheren Routing- und Geräteverwaltungsmechanismus benötigt. IoT ermöglicht es uns ferner, schnell neue Typen von Remote-Geräten in WatchGuard Cloud zu integrieren, da alle Geräte dieselbe Sprache sprechen und dieselben Schnittstellen verwenden. Nachdem das Remote-Gerät mit der Cloud verbunden ist und Daten sendet, nutzen wir AWS Kinesis Streams für die Übertragung der Daten in die Berichterstellungsengine und Storage Buckets. Kineses erspart uns die aufwändige Wartung von Servern, die Daten an ihre Ziele weiterleiten. Unsere Entwickler können sich zudem auf die Bereitstellung der Funktionen fokussieren, die unsere Kunden wünschen.

Kostenoptimierung

Wie zuvor erwähnt, nutzt die WatchGuard Cloud-Plattform automatische Skalierung auf allen Servern. Dadurch kann der Plattform bei Bedarf sehr schnell Kapazität hinzugefügt werden. Ferner hat das System die Möglichkeit, die Menge an Computing-Leistung wieder zu reduzieren, die außerhalb der Stoßzeiten konsumiert wird. Die Plattform nutzt auch reservierte Instanzen, wenn die Nachfrage über einen längeren Zeitraum voraussichtlich konstant ist. Dies resultiert in Kosteneinsparungen zur Erfüllung von Baseline-Computing-Anforderungen. WatchGuard hat Cloud-Dienste gewählt, die mehrere Probleme auf einheitliche Art und Weise lösen, wie IoT für sichere Kommunikation und Konfiguration von Agents und Appliances rund um die Uhr. Zusammengefasst: WatchGuard bietet Anwendungsdienste in WatchGuard Cloud zu Kosten, die für kleine und mittelständische Unternehmen sowie dezentral aufgestellte Unternehmen tragbar sind.

Zusammenfassung

WatchGuard Cloud wurde enwickelt und implementiert, um den Wechsel unserer Kunden und Partner in die Cloud zu vereinfachen und einen zuverlässigen, sicheren und nützlichen Dienst bereitzustellen, der Administrationsprobleme minimiert. Durch die Verwendung von Anwendungen, die in WatchGuard Cloud gehostet sind, profitieren unsere Kunden von den Vorteilen von Security-as-a-Service, wie niedrigeren Gesamtbetriebskosten, besseren Einblicken in Netzwerk- und Sicherheitsereignisse und nahtlose und skalierbare Bereitstellung.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 Kunden zu schützen. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für kleine und mittlere sowie dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz 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 www.watchguard.de