ivanti Neurons

WHITEPAPER

Ivanti Neurons for Mobile Device Management (MDM) Cloud Security

Technische Sicherheitskontrollen durch Ivanti Neurons for MDM

Hintergrund

Ivanti Neurons for MDM (ehemals Mobile Iron Cloud) ist eine cloudbasierte Lösung von Ivanti für die Bereitstellung und Verwaltung von BYOD (Bring-your-own-device)- und COPE (Corporate Owned, Personally Enabled)-Mobilgeräten. Mit Ivanti Neurons for MDM können IT-Administratoren die Sicherheitsrichtlinien des Unternehmens einrichten und durchsetzen, Unternehmensanwendungen bereitstellen und verwalten sowie Nutzungsrichtlinien für Anwendungen und Inhalte festlegen. Ivanti Neurons for MDM implementiert zahlreiche technische Sicherheitskontrollen, die dazu beitragen, Unternehmensdaten im Ruhezustand und in Bewegung zu sichern und zu isolieren sowie die Privatsphäre der Benutzerdaten zu wahren. Ivanti Neurons for MDM ist SOC 2 Typ II-konform, um die Sicherheit, Verfügbarkeit, Vertraulichkeit und den Datenschutz seiner Systeme zu gewährleisten.

Die Sicherheitskontrollen und Konformitätsfaktoren werden in diesem Dokument näher beschrieben. Zusätzlich zu unserer SOC 2-Zertifizierung hat Ivanti Neurons for MDM vom United States Postal Service (USPS) das Federal Risk and Authorization Management Program (FedRAMP) Authority to Operate (ATO) erhalten.

Ivanti Neurons for MDM hat die strengen Tests einer akkreditierten und unabhängigen FedRAMP Drittanbieter-Bewertungsorganisation (3PAO) erfolgreich durchlaufen und erfüllt damit die mit den Sicherheitskontrollen eines von FedRAMP autorisierten Systems, mit der Stufe „Moderate Impact“ (mäßige Auswirkungen).

Ferner bietet Ivanti Neurons for MDM eine kontinuierliche Überwachung, wie von FedRAMP definiert, und wird jährlich von der US-Regierung geprüft. Die vollständige Liste der FedRAMP-Sicherheitsanforderungen der Stufe „Moderate Impact“ (mittlere Auswirkungen) ist in der folgenden Tabelle aufgelistet.

Physische Sicherheit

Ivanti unterhält physische Zugangsbeschränkungen zu seiner Unternehmenszentrale (Anschrift: 10377 South Jordan Gateway, Suite 110, South Jordan, Utah 84095, USA) einschließlich seiner Rechenzentren. Diese Beschränkungen werden auf verschiedene Weise durchgesetzt, beispielsweise mittels Prüfung von Lichtbildausweisen, Ausweisen für einen kontrollierten Zugang je nach Funktion im Unternehmen und für einen eingeschränkten Zugang von Besuchern, durch Sicherheitskameras und Empfangspersonal im Eingangsbereich des Gebäudes.

Der Zugang zu den Rechenzentren von Drittanbietern ist nur autorisierten Ivanti-Mitarbeitenden oder Vertragspersonal erlaubt. Die Mitarbeitenden von Ivanti haben keinen Zugang zu den Infrastruktur-as-a-Service (IaaS)-Anbieter-Rechenzentren wie Amazon Web Services (AWS). Das Ivanti Technical Operations Team überprüft quartalsweise den Zugang zu den Rechenzentren.

Sichere Multi-Tenancy-Architektur

Die Serviceinfrastruktur von Ivanti Neurons for MDM implementiert eine Multi-Tenancy-Architektur, die es ermöglicht, dass mehrere Kunden (oder Tenants) die physischen Hardwaresysteme gleichzeitg nutzen können. Die leistungsstarke logische Trennung und Datenbanksegmentierung isolieren die Tentant-Daten und sorgen für deren Sicherheit. Eine konsistente, eingebaute Sicherheitsstufe regelt den gesamten Zugriff auf die Benutzerdaten. Jeder Zugriff, ob direkt oder über die API, durchläuft diese besondere Sicherheitsstufe auf dem Anwendungsserver.

Jeder Kunde hat eine eindeutige Tenant-Erkennung, die in jedem Daten- oder Metadatenobjekt kodiert ist, das unwiderruflich mit seinem Ivanti Neurons for MDM-Tenant verknüpft ist. Jeder User hat eine eindeutige Benutzeridentifikation (ID), die nur mit einem Tenant verbunden ist. Anwendungsobjekte, wie z. B. das mobile Gerät eines Users, die App, der Inhalt usw., sind eindeutig nur mit dem jeweiligen Tenant verbunden. Ivanti Neurons for MDM speichert diese Verknüpfungen automatisch und schränkt den Zugriff auf diese Datenobjekte basierend auf der Benutzeridentifikation. Wenn ein User Datenobjekte anfordert, wendet das System einen Tenant-Filter an, um sicherzustellen, dass es nur Daten, die dem Tenant des Users entsprechen, liefert.

Und schließlich gibt es keinen direkten Zugang zur Datenbank ohne den Umweg über die einzige Sicherheitsstufe. Selbst wenn jemandem versehentlich Zugang gewährt würde, müsste dieser dennoch zusätzliche Sicherheitsvorkehrungen durchbrechen, insbesondere die Kryptographie-Systeme, die für Kundeninhalte und bestimmte Datentypen im Ruhezustand innerhalb von Ivanti Neurons for MDM genutzt werden.

Sicherheit von Daten im Ruhezustand

Ivanti Neurons for MDM verwendet die derzeit stärkste Kryptographie zur Verschlüsselung bestimmter Datentypen im Ruhezustand auf der Festplatte und in der Datenbank. Auf der Benutzerebene werden die Passwörter mittels einer Einweg-Hashfunktion mit SHA-256-Bits generiert. Der Service verwendet den Advanced Encryption Standard (AES)-Algorithmus zur Erzeugung eines Tenant-spezifischen symmetrischen Schlüssels mit einer Schlüsselgröße von 256 Bits unter Verwendung des Galois/Counter Mode (GCM) kryptographischen Blockchiffre. Der symmetrische Schlüssel, der zur Verschlüsselung der Daten im Ruhezustand verwendet wird, wird ebenfalls mit einem anderen eindeutigen Hauptschlüssel, dem sogenannten Key Encryption Key (KEK), verschlüsselt, der ebenfalls eine AES-256-Bit-Verschlüsselung verwendet. Der KEK wird sicher im Datenbank-Dateisystem des jeweiligen Tenants in Ivanti Neurons for MDM gespeichert.

Alle Daten, die zu und von Ivanti Neurons for MDM übertragen werden, sind mit Transport Layer Security (TLS) Version 1.2 Cipher-Suites gesichert. TLS v1.2 ist die Standardeinstellung.

Application	Algorithm Protocol Compliance
Encryption of specific data types at rest	AES 256-bit GCM mode
Secure communications transmission (HTTPS)	TLS version 1.2 cipher suite
Password hashing	SHA-256 (8,000 rounds and 8 character salts)
Random Number Generation	SecureRandom
X.509 Public Key Infrastructure and Certificate Revocation List	RFC 5280

Ivanti verfolgt eine mehrstufige Defense-in-Depth-Sicherheitsstrategie. Auf der Netzwerkebene des Internetprotokolls (IP) befinden sich nach außen gerichtete Netzwerk-Firewalls an der Perimetergrenze des Unternehmens und in den Netzwerksegmenten innerhalb des Unternehmensnetzwerks, einschließlich der Rechenzentren die die Produktionssysteme von Ivanti Neurons for MDM hosten. Standardmäßig sind alle Firewalls der Rechenzentren so konfiguriert, dass sie den gesamten Netzwerkverkehr blockieren, der aus einem weniger sicheren Netzwerk stammt. Die Firewalls an der Perimetergrenze des Unternehmens blockieren den gesamten Datenverkehr aus dem öffentlichen Internet und den Extranets. Die einzigen Sicherheitsausnahmen gelten für bestimmte geschäftskritische Mitteilungen, die erforderlich sind, um die maximale Verfügbarkeit und Betriebszeit von Ivanti Neurons for MDM zu gewährleisten, ohne die Sicherheit, Vertraulichkeit oder den Datenschutz zu beeinträchtigen.

Sicherer Software-Entwicklungs-Lebenszyklus

Ivanti wendet einen sicheren Software-Entwicklungs-Lebenszyklus (SDLC) für die Produktanforderungen, Design, Implementierung, Test, Verifizierung und Wartung von Systemsoftware und Firmware an.

Der SDLC-Prozess beinhaltet, ist aber nicht beschränkt auf folgende Details. Bei diesem Prozess werden folgende Faktoren berücksichtigt, vor allem die Kunden-, Funktions- und architektonische Anforderungen, wobei die Sicherheit des Produkts eine hohe Priorität hat und die Grundlage für die Entwicklung und Implementierung ist.

Außerdem werden die folgenden Prozesse durchgeführt, um die Produktsicherheit zu gewährleisten:

- Härteverfahren für UNIX- und Linux-basierte Server (Deaktivierung der Ausführung von Code)
- Einsatz und Aktualisierung von Antivirensoftware auf allen Laptops der Mitarbeitenden im technischen Betrieb
- Verwendung verschlüsselter Festplattenspeicher für Code-Repositories
- Einsatz von Tools zur Netzwerküberwachung und -kontrolle, um den Schutz vor unbefugtem Zugriff zu gewährleisten

Es wird eine Übung zur Modellierung von Bedrohungen durchgeführt, bei der potenzielle Schwachstellen und Angriffsvektoren auf der Grundlage der Anwendung des Produkts identifiziert werden. Zur Unterstützung bei der Produktentwicklung und -implementierung, wird die Ausführung statischer Analysetools und manueller Code-Reviews von Software-Komponenten durchgeführt.

Wenn Softwarebibliotheken von Drittanbietern oder Open-Source-Software integriert werden, werden die Software-Updates und Sicherheits-Patches verwaltet.

Feature- und Funktionstests, Anwendungssicherheitstests und Härtetests werden mit hochentwickelten Penetrationstests von Drittanbietern durchgeführt. So können Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL-, Betriebssystem- oder LDAP-Injektionen, unsichere direkte Objektverweise, Directory Traversal; Sicherheitsfehlkonfigurationen, die Offenlegung sensibler Daten, fehlerhafte Authentifizierung und Sitzungsmanagement, nicht validierte Um- und Weiterleitungen und andere Sicherheitsschwachstellen erkannt werden.

Alle verwendeten Bibliotheken von Drittanbietern oder Open Source Bibliotheken werden aktualisiert oder gepatcht, wenn eine Sicherheitsschwachstelle intern entdeckt oder von einem Kunden oder Partner gemeldet wird. Alle Sicherheitsschwachstellen, die in einem freigegebenen Produkt gefunden werden, werden in Übereinstimmung mit der Ivanti-Richtlinie zum Schwachstellenmanagement behoben.

Ferner werden jährlich umfangreichere Penetrationstests durch die Beauftragung seriöser Drittanbieter durchgeführt. Sicherheitsprobleme werden behoben, gelöst und anschließend dann validiert.

Ivanti sorgt für Virtual Private Network (VPN)- und Secure Shell (SSH)-Verbindungen zum Unternehmensstandort und sichert die Kommunikationssysteme für die Übertragung privater und vertraulicher Daten in Bewegung. Alle Web-Verbindungen werden über HTTPS mit Transport Layer Security (TLS) 1.2 Cipher-Suites gesichert. Sicherungsdaten werden verschlüsselt und an einem ausgelagerten Ort gespeichert, auf den nur autorisiertes Personal aus dem technischen Betrieb Zugriff hat.

24/7-Network Operations Center (NOC) und -Security Operations Center (SOC)

Ivanti verfügt über ein ISO27001-zertifiziertes Netzwerkbetriebsteam, das rund um die Uhr im Einsatz ist und das sich auf die Reaktionsfähigkeit von Level 1 und Level 2 konzentriert sowie Mitarbeitende der Level 3 und 4 auf Abruf bereithält1. Ivanti überwacht die NOC-Reaktionen regelmäßig auf Qualität und die Einhaltung der SLA. Die leitenden Mitarbeitenden überprüfen die SLA-Berichte des NOC, um einen optimalen Betrieb zu gewährleisten. Das SOC überwacht aktiv Sicherheitsvorfälle mithilfe eines SIEM-Tools (Security Incident and Event Management)

Sicherheit von Infrastructure-as-a-Service-Drittanbietern

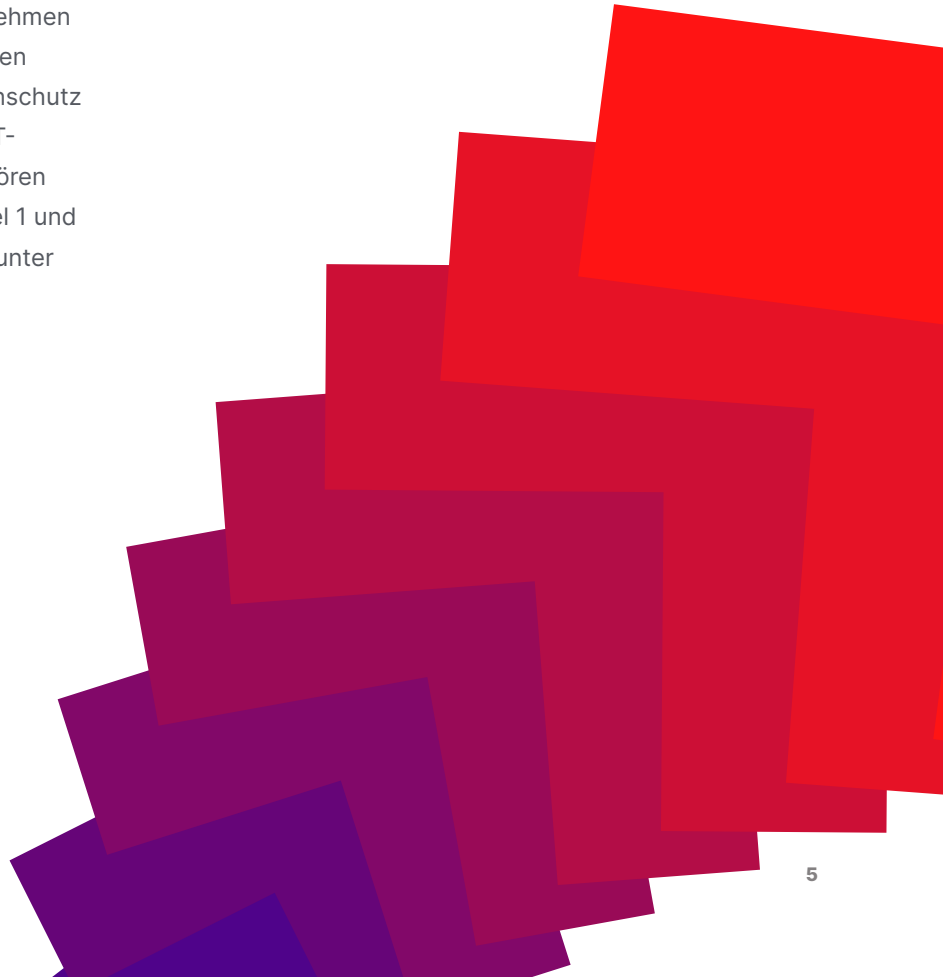
Alle Ivanti Neurons for MDM Tenant-Cluster werden weltweit von Amazon Web Services gehostet (AWS). Der physische Zugriff auf das Ivanti Neurons for MDM-Produktionssystem erfordert eine biometrische Handscan-Authentifizierung für den Zugang zur Eingangshalle, die rund um die Uhr von Sicherheitspersonal und Kameras in der gesamten Anlage überwacht wird. Auch hier ist die Handscan-Authentifizierung erforderlich, um Zugang zu dem sicher verschlossenen Käfig zu erhalten, der die Ivanti Neurons for MDM-Hardware-Produktionssysteme schützt.

Zu den zusätzlichen Sicherheitskontrollen gehören eine mehrstufige Defense-in-Depth-Netzwerksicherheit, die eine Firewall an der Perimetergrenze und eine sichere Fernzugriffskommunikation zu den Servern umfassen.

AWS setzt robuste Sicherheitspraktiken ein, indem es Firewalls an seinem Netzwerk-Gateway installiert. AWS wendet außerdem eine strenge Richtlinie für den physischen Zugang zu seinen Rechenzentren und Colocation-Standorten an. Das Unternehmen erfüllt die branchenüblichen und gesetzlichen Anforderungen an die Sicherheit, den Datenschutz und die Vertraulichkeit von Daten. Zu den IT-Sicherheitsstandards, die AWS einhält, gehören SOC 1, SOC 2, SOC 3, FISMA, PCI DSS Level 1 und FIPS 140-2. Weitere Referenzen finden Sie unter dem folgenden Link.

AWS Security

http://aws.amazon.com/security/



Über Ivanti

Ivanti macht den Everywhere Workplace möglich. Im Everywhere Workplace nutzen Mitarbeitende eine Vielzahl von Geräten, um auf IT-Netzwerke, Anwendungen und Daten zuzugreifen und von überall aus produktiv zu arbeiten.
Die Ivanti-Automatisierungsplattform verbindet die branchenführenden Lösungen des Unternehmens für Unified Endpoint Management, Zero Trust Security und Enterprise Service Management und bietet Unternehmen eine einheitliche Plattform für die Selbstheilung und den Schutz von Geräten sowie die Selbstbedienung seitens der User. Mehr als 40.000 Kunden, darunter 96 der Fortune-100-Unternehmen, haben sich für Ivanti entschieden, um ihre IT-Assets von der Cloud bis zum Edge zu erkennen, zu verwalten, zu sichern und zu warten sowie ihren Mitarbeitenden eine exzellente Benutzererfahrung zu bieten, egal wo und wie sie arbeiten.
Weitere Informationen finden Sie unter https://www.ivanti.com/de/ und folgen Sie @GoIvanti

Urheberrecht © 2023, Ivanti. Alle Rechte vorbehalten. IVI-2739 12/23 JC/FG

ivanti

For more information, or to contact Ivanti, please visit ivanti.com/lp/contact-us

1. Level 1 & Level 2: Incident Response für bekannte Fehler und Antworten mittels Erhebung von Informationen und Fehlerbehebung und um Level 3- & 4 Support erweiterte Fehlerbehebung, Konfiguration sowie Patch-Erstellung.