ivanti Neurons

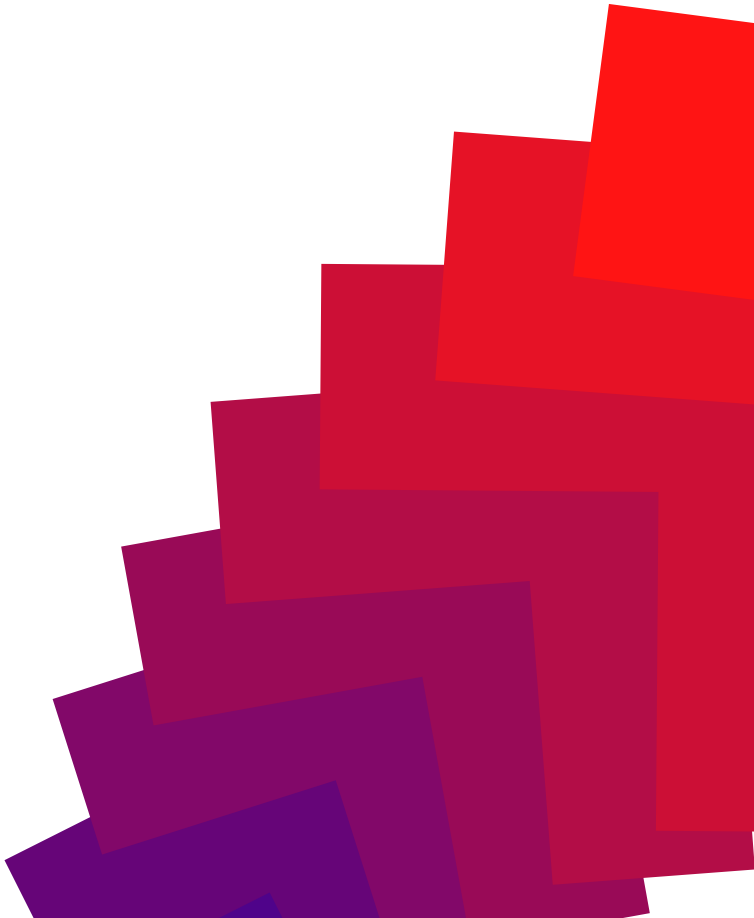
WHITEPAPER

Ivanti Neurons for Mobile Device Management (MDM) Cloud Security

Technical Security Controls applied to Ivanti Neurons for MDM

Background

The Ivanti Neurons for MDM (formerly MobileIron Cloud) service is Ivanti's cloud-based solution for provisioning and managing users bring-your-own-device (BYOD) and corporate-owned personally enabled (COPE) mobile devices. Ivanti Neurons for MDM enables IT administrators to deploy and enforce corporate security policy, deploy and manage enterprise apps, and establish usage policies for apps and content. The Ivanti Neurons for MDM service implements numerous technical security controls designed to help secure and isolate enterprise data at rest and data in motion, and to ensure the user's personal data remains private. Ivanti Neurons for MDM is SOC 2 Type II compliant, to ensure the security, availability, confidentiality, and privacy of its systems. The security controls and compliance factors are described further within this document. In addition to our SOC 2 certification, Ivanti Neurons for MDM has been granted the Federal Risk and Authorization Management Program (FedRAMP) Authority to Operate (ATO) from the United States Postal Service (USPS). Ivanti Neurons for MDM's solution successfully completed rigorous testing conducted by an accredited and independent FedRAMP Third-Party Assessment Organization (3PAO), which complies with the security controls of a FedRAMP authorized moderate impact level system. In addition, Ivanti Neurons for MDM performs continuous monitoring as defined by FedRAMP, and is audited annually by the U.S. Government. The complete list of FedRAMP moderate impact level security baseline requirements are itemized within the following spreadsheet.



Physical Security

Ivanti maintains physical access restrictions into its corporate headquarters (located at: 10377 South Jordan Gateway Suite 110 South Jordan, Utah 84095) including its data centers. These restrictions are enforced in several ways, including photo identification, controlled proximity and restricted visitor access badges based on job function, security cameras, and building lobby receptionists.

At third-party data centers, access is restricted only to authorized Ivanti employees or contract personnel. Ivanti employees do not have access to the Infrastructure as a Service (IaaS) provider data centers like Amazon Web Services (AWS). The Ivanti Technical Operations team reviews access into the data centers on a quarterly basis.

Secure Multi-tenancy Architecture

The Ivanti Neurons for MDM service infrastructure implements a multi-tenancy architecture that enables multiple customers (or tenants) to share physical hardware systems based on geography; powerful logical separation and database segmentation isolate tenant data and keep it secure. A consistent built-in security layer governs all access to the tenant user data. All access, whether directly or through the API, funnels through this single security layer at the application server. Each customer has a unique tenant identifier that is coded into every data or metadata object that is irrevocably linked to their associated Ivanti Neurons for MDM tenant. Every user has a unique user identification (ID) that is associated to only one tenant. Application objects like a user's mobile device, app, content, etc., are uniquely associated with only their tenant. Ivanti Neurons for MDM stores these links automatically and restricts access to these data objects based on user identification. When a user requests any data objects, the system applies a tenant filter to ensure it returns only data corresponding to the user's tenant.

Lastly, there is no direct access to the database without going through the single security layer. Even if access were inadvertently granted to someone who was unauthorized, they would still need to break through additional security safeguards, specifically the cryptography systems used for customer content and certain data types at rest within the Ivanti Neurons for MDM service.

Data at Rest Security

The Ivanti Neurons for MDM service employs today's strongest cryptography to encrypt specific data types at rest on disk and within the database. At the user level, passwords are salted with a one-way hash function using SHA-256-bits. The service uses the Advanced Encryption Standard (AES) algorithm to generate a tenant-specific symmetric key with a key size of 256-bits using Galois/Counter Mode (GCM) cryptographic block cipher. The symmetric key that is used to encrypt this data at rest is also encrypted using another unique master key, called a Key Encryption Key (KEK), also using AES 256-bit encryption. The KEK is securely stored within the database file system of the specific tenant in Ivanti Neurons for MDM.

All data in transit to and from the Ivanti Neurons for MDM service is secured using Transport Layer Security (TLS) versions 1.2 cipher suites. TLS v1.2 is the default setting.

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 maintains a layered defense-in-depth security strategy. At the Internet Protocol (IP) network level, externally-facing network firewalls are in place at the corporate perimeter boundary and network segments within the corporate network, including the data centers that host the Ivanti Neurons for MDM production systems. By default, all data center firewalls are configured to block all network traffic sourced from a less secure network. Corporate perimeter firewalls block all traffic from the public Internet and extranets. The only security exceptions created are for specific business-critical communications required to ensure the maximum availability and uptime of the Ivanti Neurons for MDM service without compromising security, confidentiality or privacy.

Secure Software Development Life Cycle

Ivanti employs a secure Software Development Life Cycle (SDLC) process for the product requirements, design, implementation, testing verification, and maintenance of system software and firmware. The SDLC process includes, but is not limited to, the following details. This process takes into consideration various factors, most notably the customer, functional and architectural requirements, although the security of the product is a high priority and baseline prior to moving to development and implementation work.

Also, the following processes are performed to ensure product security:

- Hardening procedures applied to UNIX and Linux-based servers (disabling execution of code)
- Deploying and updating antivirus software on all Technical Operations personnel laptops
- Using encrypted hard drive storage for code repositories
- Network monitoring and control tools are used to protect against unauthorized access

A threat-modeling exercise is performed in which potential vulnerabilities and attack vectors are identified based on the application of the product

To aid in product development and implementation, the execution of static analysis tools and manual code reviews of software components are performed. If third-party or open source software libraries are integrated into the product, application of software updates and security patches are managed.

Feature and functional testing, application security testing, and hardening are executed using sophisticated third-party penetration testing tools to detect cross-site scripting (XSS); cross-site request forgery (CSRF); SQL, operating system (OS) or LDAP injections; insecure direct object references; directory traversal; security misconfigurations; sensitive data exposure; broken authentication and session management; unvalidated redirects and forwards, and other security vulnerabilities.

If a high-priority customer found defect is reported after the product has been released, it is remediated or resolved using the ___. Any third-party or open-source libraries used are updated or patched if a security vulnerability is discovered internally or reported by a customer or partner. Any security vulnerabilities found in a released product are remedied in accordance with Ivanti's Vulnerability Management Policy.

In addition, more extensive security penetration testing is performed annually by contracting reputable third-party vendors. Security issues found during this testing process are remediated, resolved, and then validated.

Ivanti enforces Virtual Private Network (VPN) and Secure Shell (SSH) connections to the corporate site, and secures communication systems for transmission of private and confidential data in motion. All web connections are secured over HTTPS using Transport Layer Security (TLS) 1.2 cipher suite. Backup data is encrypted and stored at an offsite location where access is restricted to authorized Technical Operations personnel only.

24X7 Network Operations Center (NOC) and Security Operations Center (SOC)

Ivanti leverages an ISO27001-certified 24×7×365 network operations team, focused on Level 1 and Level 2 response with Level 3 and 4 staff on-call[1]. Ivanti monitors the NOC responses regularly for quality and adherence to SLA. Executive staff reviews NOC SLA reports to ensure optimal operations. The SOC actively monitors security incidents using a Security Incident and Event Management (SIEM) tool.

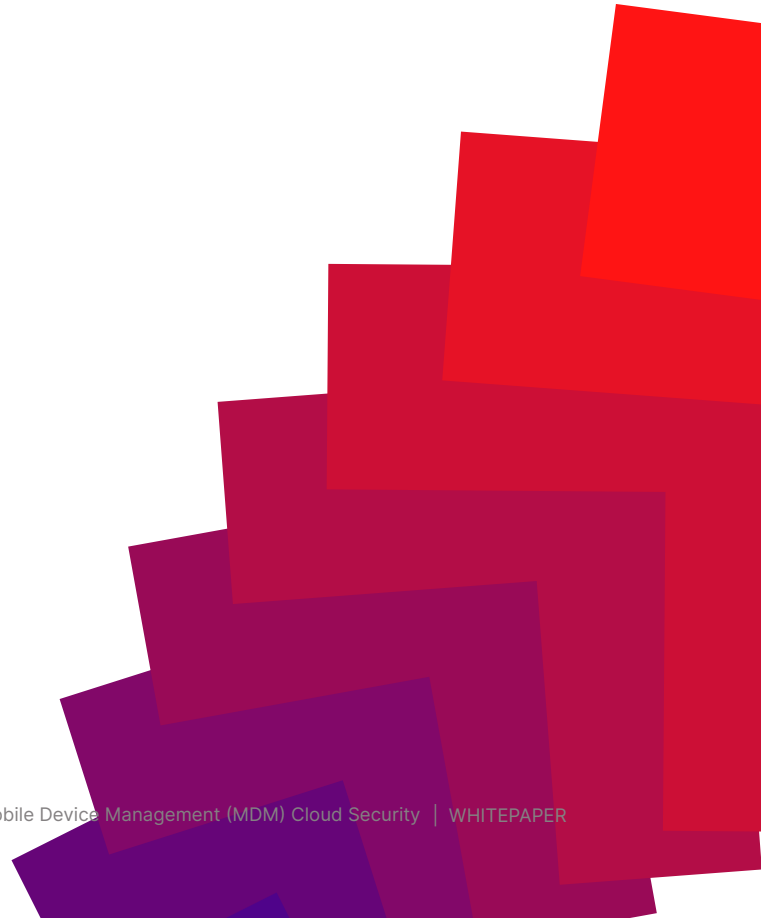
Third-Party Infrastructure as a Service Security

All of the Ivanti Neurons for MDM tenant clusters globally are hosted by Amazon Web Services (AWS). Physical access to the Ivanti Neurons for MDM production system requires biometric hand scan authentication to access the lobby entrance that is manned by security personnel and cameras throughout the entire facility on a 24-hour 7 day a week basis. Hand scan authentication is again required to gain access to the securely locked cage that protects the Ivanti Neurons for MDM hardware production systems. Additional security controls include a layered defense-in-depth network security that employs a firewall at the perimeter boundary and secure remote access communications to the servers.

AWS implements robust security practices by placing firewalls at their network gateway. AWS also employs a stringent physical access policy into its data centers and colocation sites. It is compliant with industry and government requirements for security, privacy, and confidentiality of data. Some of their IT Security standards they adhere to are SOC 1, SOC 2, SOC 3, FISMA, PCI DSS Level 1, and FIPS 140-2 compliance. Additional references can be found at the following link.

AWS Security

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



About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. Level 1 & Level 2: Incident response for known errors & responses with information gathering and troubleshooting and Level 3 & 4 support advanced troubleshooting, configuration and patch creation.