ivanti neurons

DATASHEET

Protecting Data While Empowering Enterprises to Act Against Cyberattacks

Ivanti Neurons for RBVM & ASOC Security

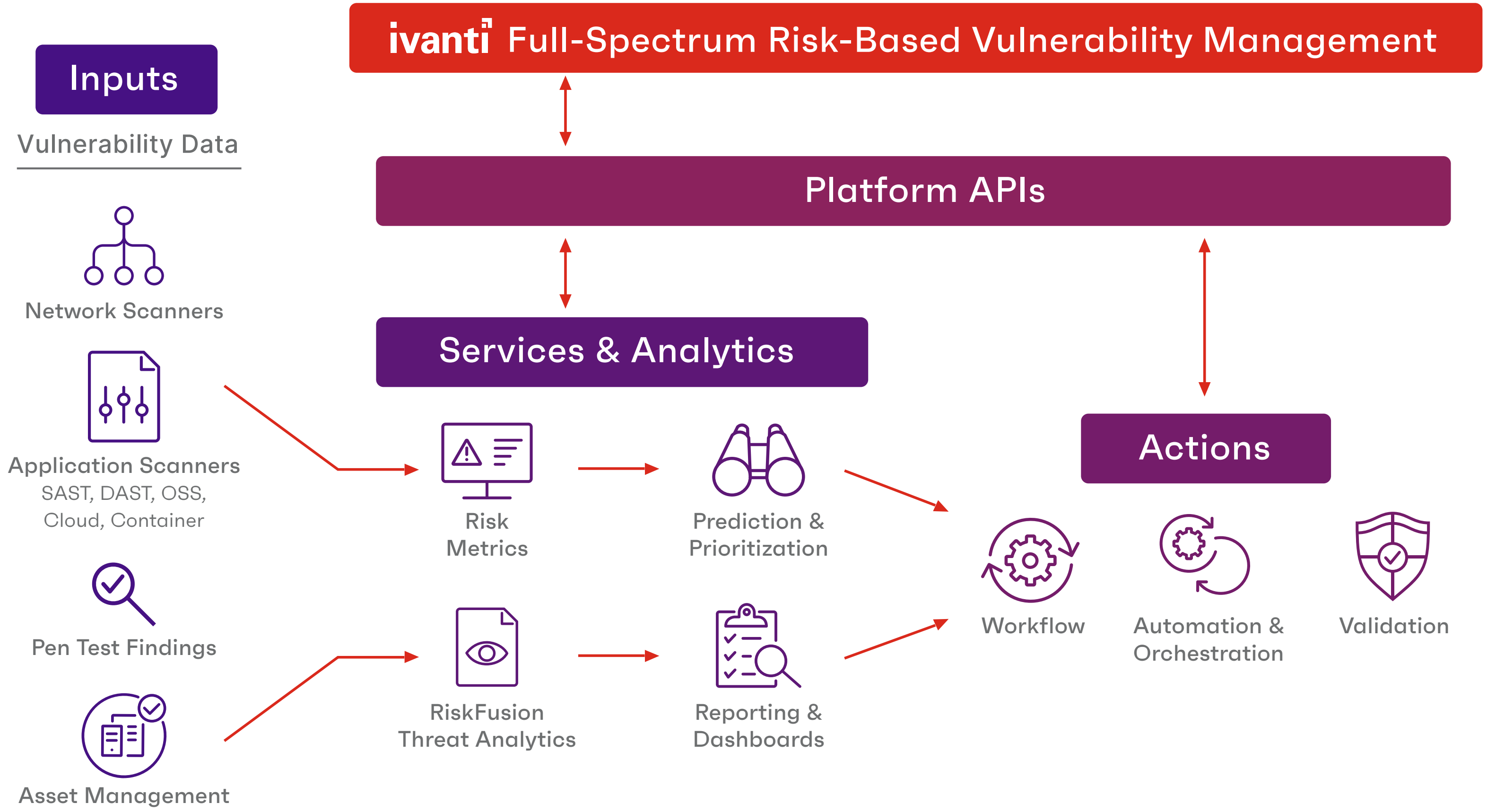
Securing your data while protecting your enterprise

At Ivanti we are focused on providing the very best vulnerability management and prioritization to measure and control cybersecurity risk. We do this in such a way that your network, application and cloud-based data is all protected using industry best practices to ensure it is only accessed by authorized personnel.

Overview

Ivanti Neurons for Risk-Based Vulnerability Management (RBVM) and Ivanti Neurons for App Security Orchestration & Correlation (ASOC) transform cyberrisk management into a more proactive, collaborative and real-time discipline. These products embody the expertise and deep knowledge Ivanti has gained from defending critical networks against the world's most dangerous cyberadversaries.

Ivanti Neurons for RBVM & ASOC are software as a service (SaaS) offerings and, as such, Ivanti is committed to protecting the data our customers access, store and process. Ivanti maintains appropriate administrative, technical and physical procedures to safeguard the Ivanti Neurons for RBVM & ASOC platform, infrastructure and associated customer data.



Cloud infrastructure and compliance

To deliver its proactive cyberrisk management software, Ivanti has partnered with Amazon Web Services (AWS). Ivanti Neurons for RBVM & ASOC are hosted in the AWS GovCloud (US) in the U.S., which is an isolated AWS Region designed to fulfill the most stringent regulatory and compliance requirements of U.S. government agencies and security-conscious U.S.-based clients.

Ivanti Neurons for RBVM & ASOC are also offered in EU (Frankfurt) and Asia-Pacific (Mumbai) to meet geo-specific data restriction standards.

The AWS GovCloud (US) is compliant with the U.S. International Traffic in Arms Regulations (ITAR) and the Federal Risk and Authorization Management Program (FedRAMP). Furthermore, AWS GovCloud (US) has received an Agency Authorization to Operate (ATO) from the U.S. Department of Health and Human Services (HHS), utilizing a FedRAMP accredited Third-Party Assessment Organization (3PAO) for several AWS services.

The AWS GovCloud (US) Region provides the same fault-tolerant design as other regions, with two availability zones. In addition, the AWS GovCloud (US) Region is a mandatory AWS Virtual Private Cloud (VPC) service by default to create an isolated portion of the AWS Cloud and launch Amazon EC2 instances that have private (RFC 1918) addresses.

The AWS cloud infrastructure has been designed and managed in alignment with regulations, standards and best practices including:

- PCI DSS Level 1
- ISO 27001
- FedRAMP
- DIACAP and FISMA
- ITAR
- FIPS 140-2
- CSA
- MPAA
- HIPAA
- SOC 1 / SSAE 16 / ISAE 3402 (formerly SAS70)
- SOC 2
- SOC 3

Further, AWS GovCloud (US) has been granted a Joint Authorization Board Provisional Authority to Operate (JAS P-ATO) and multiple Agency Authorization (A-ATO) for high impact level, allowing us to secure highly sensitive data and content for U.S. DoD and U.S. Intelligence customers. AWS is NIST compliant and is hardened in line with NIST standards.

More information about AWS GovCloud (US) is available on the AWS website. Additionally, upon request, Ivanti can make AWS GovCloud (US) compliance reports and certifications (e.g., SOC 1, SOC 2, FedRAMP) available to customers and/or prospects.

Finally, Ivanti internal business operations are SOC 2 compliant and adhere to the NIST SP 800-53 as a primary security risk management program, but also reference ISO 27001 and CCM. Ongoing annual SOC 2 Type 2 audits are conducted by an independent CPA firm. Internal and external vulnerability scanning plus penetration testing of our systems are performed regularly. Penetration testing of our cloud service are conducted by in-house assessment teams and we undergo annual penetration testing by third-party security firms.

Authentication and authorization

Ivanti Neurons for RBVM & ASOC support security assertion markup language (SAML) authentication configuration. This process can be configured with third-party systems, including Active Directory Federated Services (ADFS). The Ivanti Neurons for RBVM & ASOC platform acts as the service provider with the third-party system serving as the identity provider for authentication.

Users can authenticate to Ivanti Neurons for RBVM & ASOC using the platform's user interface or via API. When using Ivanti Neurons for RBVM & ASOC credentials for authentication instead of SAML, the platform provides configurations for password history, password length and security questions.

The platform always enforces two-factor authentication via email for all users. Each user can convert and configure a time-based multi-factor authentication device/application for their two-factor authentication. Additionally, the platform meets NIST standards and uses TLS 1.2 with secure ciphers for authentication communication, regardless of SAML or local authentication.

Predefined user roles (manager, group manager, user and technician) are leveraged in conjunction with group access for granular functionality control and access to data based on the users' assigned groups. Users are assigned to groups and group data can only be viewed by users assigned to those groups. This functionality allows for complete data segregation and access control to all platform data.

Further data segregation can be achieved by multi-client functionality (separate Ivanti Neurons for RBVM & ASOC accounts) when required by a customer that has multiple entities to manage and allows grouping data within any individual entity. This feature provides data access and segregation at the entity management level as well as across the enterprise.

Cloud infrastructure and security

Ivanti Neurons for RBVM & ASOC reside behind network-based security solutions. In addition, AWS GovCloud (US) has effective controls in place to protect against physical penetration by malicious or unauthorized people.

As defined in our SOC 2 policy, infrastructure access is limited to the Ivanti SRE Team and access control is enforced with two-factor authentication. Data is encrypted at rest (using AES-256 encryption algorithm) and in transit (using SHA-256 bit key). All Ivanti personnel access to aid in troubleshooting and/or platform uptime maintenance is audited as per the SOC 2 policies.

Application security

Ivanti utilizes some of the most advanced technology for internet security available today. When you access the application using an Ivanti-supported browser, Transport Layer Security (TLS v1.2) technology protects your information using both server authentication and classic encryption, ensuring that your data is safe, secure and available only to registered users in your organization. In addition, as per the SOC 2 policy, regular human penetration testing is performed.

Access controls

Ivanti ensures authentication and authorization controls are appropriately robust for the risk to the data, application and platform. Ivanti Neurons for RBVM & ASOC are accessible only over encrypted SSL / TLS channels. The use of two-factor authentication is required to log in to the platform.

Ivanti Neurons for RBVM & ASOC use a role-based access control (RBAC) policy with a set of predefined roles. This ensures each user is assigned to the minimum required privileges. In addition, users can be assigned to specific groups in conjunction with the role to restrict the access to assets (hosts, applications, cloud, container).

Password policies

Ivanti Neurons for RBVM & ASOC enforce a strong password policy for all active user accounts. The policy includes, but is not limited to:

- Users are provided a one-time password during account creation. Subsequently, users must pick new passwords before they can log in to the platform.
- Passwords must contain at least eight characters, including an uppercase letter, a number and a special character.
- Passwords can be configured to expire after one week to a maximum of 16 weeks.
- Passwords are encrypted using a one-way hash.
- Users will be locked out after a set number of unsuccessful authentication attempts and an IP address will be blocked after a defined number of unsuccessful attempts within a defined time range.
- Users are not allowed to use previously used passwords when changing or resetting their password. The number of previously used passwords that the platform remembers is configurable.

Continuous application scanning and monitoring

Ivanti continuously gathers and analyzes information regarding new and existing threats and vulnerabilities, actual attacks on the infrastructure, and the effectiveness of the existing security controls. Monitoring controls include related policy and procedure, virus and malicious code, intrusion detection, as well as event and state monitoring. Related logging processes provide an effective control to highlight and investigate security events.

Ivanti performs regular network scans, application scans and manual vulnerability assessments. Application scans are performed every quarter to identify OWASP Top 10 and CWE Top 25 Most Dangerous Software Errors. Network scans are also performed on a quarterly basis. Security events are logged (log files), monitored (appropriate individuals) and addressed (timely action documented and performed). Network components, workstations, applications and any monitoring tools are enabled to monitor user activity.

Organizational responsibilities for responding to events are defined. Configuration checking tools are utilized (or other logs are utilized), which record critical system configuration changes. Ivanti monitors access rights to ensure access adheres to the least privilege principle commensurate with the user's job responsibilities, logs all access and security events, and uses software that enables rapid analysis of user activities. The log permission restricts alteration by administrators. The retention schedules for various logs are defined and enforced.

When it comes to vulnerability management, Ivanti follows a well-defined process to remediate findings based on risk ratings. Ivanti performs platform updates on a regular basis so that any security patches can be applied in a timely fashion. In the case of critical vulnerabilities as determined by our Risk Management Team, Ivanti applies patches as quickly as possible and could incur unscheduled downtime in such cases.

To assure application stability and availability, the Ivanti SRE Team is notified in case of excessive network bandwidth utilization, low performance thresholds, a server crash, an application crash and other such scenarios to ensure a timely response. Ivanti also utilizes load balancing techniques for optimized resource utilization, maximized throughput, reduced latency and fault-tolerant configurations.

Data security

Data segregation

Ivanti protects your organization's data from all other customer organizations by using a unique organization identifier, which is associated with each user's session. Once you log in to your organization, your subsequent requests are associated with your organization using this identifier. Stored data is encrypted.

Data encryption

Customer data within Ivanti Neurons for RBVM & ASOC is encrypted at all times, both in transit and at rest. Data at rest is secured through database encryption and file system encryption using the AES 256 algorithm. Data in transit encryption is managed through TLS v1.2. All data files (e.g., uploaded scanner reports) are stored on an encrypted drive with restricted access. The key management for aforementioned encryption solutions is handled by AWS GovCloud (US).

IP address whitelisting

Ivanti Neurons for RBVM & ASOC provide each client the ability to configure a whitelist for IP addresses that can log in to the platform. If the user is attempting a login from another IP address via UI/API they will be presented with an error. Within the Ivanti Neurons for RBVM & ASOC infrastructure, communication is restricted via firewall access control lists (ACL), using whitelisting of applications and machines.

Data backup

Ivanti performs incremental data backups at five-minute intervals, retaining the data for the last 72 hours. Customer data is stored within the customer's region and does not leave that boundary (e.g., on AWS GovCloud (US) in the U.S.). Backup data is encrypted by default. A full data backup is performed daily and retained for three days.

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 neurons

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