Ivanti supports NIST SP 800-171

Enabling secure mobility is one of the fundamental ways governments agencies, federal system integrators and other organizations that work with controlled unclassified information (CUI) can deliver the benefits of modern work to employees and constituents. However, before enterprises can embrace the efficiencies of modern endpoints, apps and cloud services, they must ensure that comprehensive security does not become an afterthought. Because of this, several U.S. federal guidelines exist to ensure consistency across organizations that do business with the U.S. federal government.

One of these, NIST SP 800-171 (Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations), provides mandatory guidelines and oversight for initiatives that utilize CUI across non-federal systems and organizations. Security controls defined in NIST SP 800-171 extend beyond traditional unified endpoint management (UEM) capabilities to include the ability to report, mitigate and remediate all discovered vulnerabilities across the mobile workforce and app infrastructure.

Ivanti's comprehensive security platform enables federal agencies to meet many of the compliance controls for mobile endpoints that outlined in NIST SP 800-171.

NIST SP 800-171 control families supported by Ivanti

There are 110 controls grouped into 14 control families in the NIST SP 800-171 special publication. Ivanti provides endpoint security for the control families highlighted below.

- **Access Control**
- **Identification & Authentication**
- Personnel Security
- **Audit & Accountability**
- Maintenance
- **Risk Assessment**
- Awareness & Training
- Incident Response
- Physical & Environmental Protection
- **Configuration Management**
- **Media Protection**
- Security Assessment
- **System & Information Integrity**
- **System & Communications Protection**

Additional security standards and compliance certifications that Ivanti holds, but not limited to, are:

- FedRAMP Authority to Operate
- FIPS 140-2 Affirmation
- NIAP Common Criteria Certification
- SOC 2 Type II
- Data Privacy Framework

How Ivanti supports NIST SP 800-171

See what's on the network

Ivanti's controls ensure that only authorized, compliant endpoints can access resources and CUI on federal government networks. Our trusted workspace enables admins to define and enforce granular compliance policies, manage and distribute only apps that have been fully vetted and approved, and enable access control and multifactor authentication (MFA). Ivanti also detects and remediates known and zero-day threats on mobile devices, even without internet connectivity, to reduce data loss without disrupting user productivity.

Know who is on the network

Ivanti extends the same level of security provided by personal identity verification (PIV) cards to mobile devices to authenticate users for federal networks and applications. We have an embedded inline gateway that manages, encrypts and secures traffic between mobile devices and back-end government systems. Ivanti also provides secure, conditional access control for cloud services such as Microsoft Office 365, G Suite, Box, Dropbox, etc.

Our mobile threat defense automatically deploys to all devices, putting 100% user adoption and immediate compliance within reach. Admins can continuously analyze the integrity of managed devices to ensure vulnerabilities at the device, network and app level. If a threat is detected, the solution can mitigate it locally on the mobile device.

Understand what is happening on the network

Ivanti Secure UEM solutions, encrypt all data at rest and in transit on mobile devices, and leverages FIPS 140-2 validated crypto libraries. Users can securely leverage email (S/MIME) and Ivanti's productivity suites like Docs@Work and Web@Work. Admins can remotely configure, deploy and update compliance policies, as well as manage the lifecycle and security of mobile applications with no user intervention. Ivanti's integrated mobile threat defense and continuous diagnostics and mitigation (CDM) capabilities also work with Samsung Knox and the latest Android Enterprise administrative policy and privacy controls.

Ivanti provides per-app virtual private network (VPN) session security to connect each managed application to the federal government's network, along with various configurations and support for traditional VPNs and the trusted internet connections (TIC). This ensures all federal data is continuously encrypted and protected against attacks and mitigates zero-day attacks. One-touch enrollment and our ability to support enterprise-class PIV-D-derived credentials for single sign-on (SSO) and MFA provides the best possible user experience while maintaining a strong cybersecurity posture. Enforced analytics and adaptive risk-based policies account for the type of endpoint, app, network, user, location and more.

Ivanti's unique UEM platform automatically deploys mobile threat defense on organization and employee-owned mobile devices. Our integrated pane of glass with a Splunk forwarder built into our administrative console provides real-time analytics and intelligence that detects threats and attacks on mobile endpoints. Admins quickly gain visibility into devices, operating systems, network and mobile applications' risk and vulnerability scores. Machine learning (ML) algorithms and behavior-based methodologies detect mobile threats, and actionable intelligence provided by the app's analytics engine quickly mitigates and remediates mobile threats. Admins can limit exposure to possible exploitations by remediating attacks before they infiltrate the device. Our automated, tiered compliance actions provide alerts about risky behaviors, proactively shut down attacks on the device, isolate compromised devices from the network and remove malicious apps and their content.

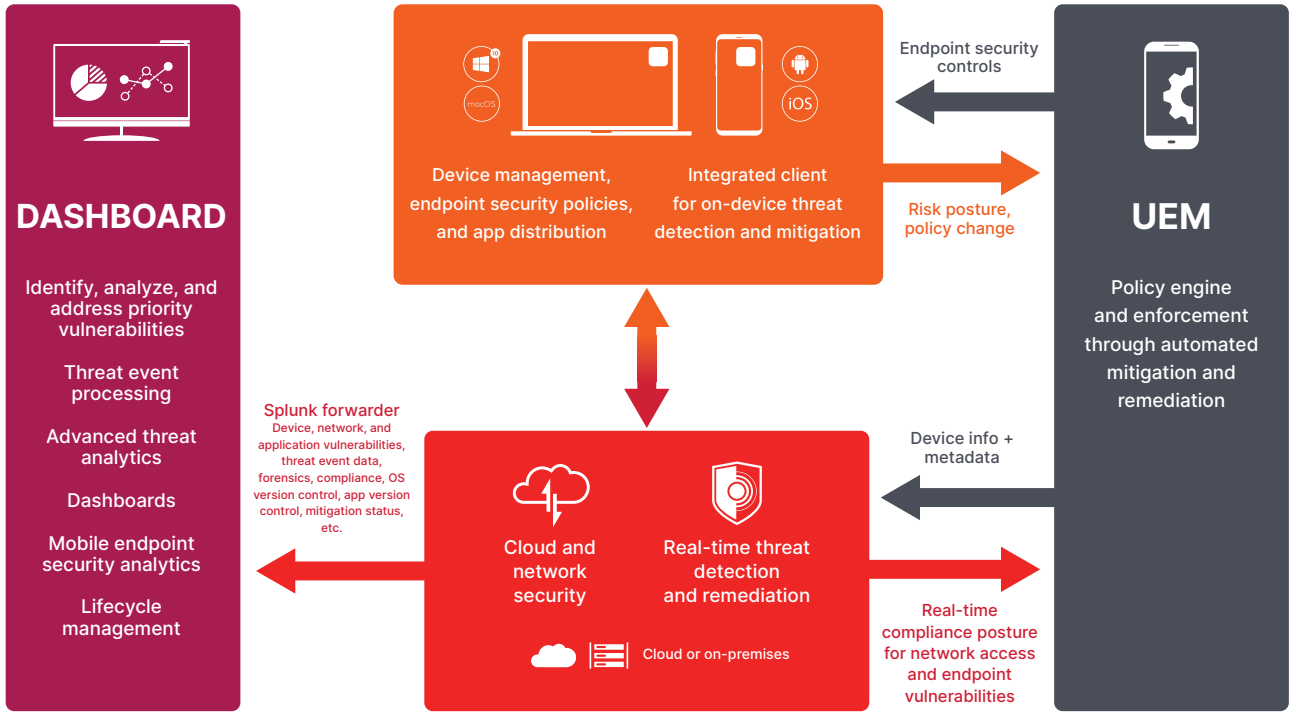
Protect data across multiple endpoints

Ivanti provides continuous visibility into what is happening on endpoints and mobile apps that connect to federal and corporate networks or cloud services. Administrators can configure and apply consistent data security policies and enforce tiered remediation and mitigation actions across all endpoints. This ensures secure access to enterprise email, calendars and contacts while preserving the native user experience.

If bring your own device (BYOD) initiatives are in place, Ivanti maintains user privacy while enforcing federal compliance policies and control over federal resources and data. Encryption protects sensitive federal data at rest on endpoints and in motion across any network or cloud service. Secure, instant access to enterprise resources and unauthorized file sharing prevention also safeguard against data loss.

Ivanti protects CUI by continuously identifying mobile cybersecurity risks. Admins can prioritize these risks based on potential impacts and mitigate them immediately on the device. The solution can then disable access to email, VPN and Wi-Fi, or even remove data at rest from the device while preventing access to corporate and federal network and cloud services. In addition, admins can implement a graduated set of local compliance actions over a period of time to increase user compliance while keeping productivity constant.

Ivanti Reference Architecture



Dashboards and reporting

Ivanti's intuitive dashboards and custom reports provide deep visibility into device compliance, user access control, app security and privacy risks. In addition, web APIs, Splunk forwarders and a reporting database export data into a centralized security information and event management (SIEM) system. App security and privacy risk summary reports provide insight into app risk scoring, app behaviors and context so admins can take necessary actions.

About Ivanti

Ivanti is an enterprise software company that provides a comprehensive IT and security cloud-based platform. Ivanti provides software solutions that scale with our customers' needs to help enable IT and Security to improve operational efficiency while reducing costs and proactively reducing security risk. The Ivanti Neurons platform is cloud-native and is designed as a foundation of unified and reusable services and tools for consistent visibility, scalability and secure solution delivery. Over 34,000 customers, including 85 of the Fortune 100, have chosen Ivanti to meet challenges head-on with its end-to-end solutions. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and we are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com and follow @GoIvanti.

ivanti

For more information about our solutions for the U.S. federal government, or to contact Ivanti, please visit: ivanti.com/industries/federal-government