Security in the Cisco Intersight Platform

Delivering secure, software-as-a-service management

Secure management you can trust

When your IT infrastructure resides in an enterprise data center, at the network edge, and in remote and branch offices, the use of separate tools in each location poses management challenges. The Cisco Intersight® platform consolidates and automates management for your Cisco Unified Computing System™ (Cisco UCS®) servers, converged, and hyperconverged infrastructure. Whether you access Intersight software through a cloud-based software-as-a-service portal or through an appliance you host in your data center, we make it easy to securely deploy, operate, and manage your IT infrastructure.

A changing management landscape

Conventional IT infrastructure lifecycle-management tools use point products with multiple element managers. With Cisco UCS, we changed the game for both IT infrastructure and the way that systems are managed. Combining converged infrastructure and embedded model-based management, Cisco UCS simplifies and automates computing to make daily operations easier and more efficient. With Cisco Intersight Software-as-a-Service (SaaS) and the on-premises Cisco Intersight Virtual Management Appliance, we have taken the next step in extending our management umbrella to encompass Cisco UCS, converged, and hyperconverged infrastructure wherever it is located.

Introducing Cisco Intersight

Whether you use the cloud-based portal or a local appliance, Cisco Intersight combines the benefits of cloud-based management with security similar to that of on-premises systems. This management and automation platform is enhanced by analytics and machine-learning techniques to increase efficiency and continuously evolve, so you can simplify management of your IT infrastructure.

The software monitors the health and relationships of infrastructure components that use Cisco UCS and converged and hyperconverged infrastructure. Telemetry and configuration information is collected and stored in accordance with Cisco information security requirements. Your data is isolated and displayed to you through an intuitive user interface. Because the software scales easily and frequent updates are implemented without impact, this simplified and consistent infrastructure management approach removes the difficulties of supporting typical tools and appliances (Figure 1).

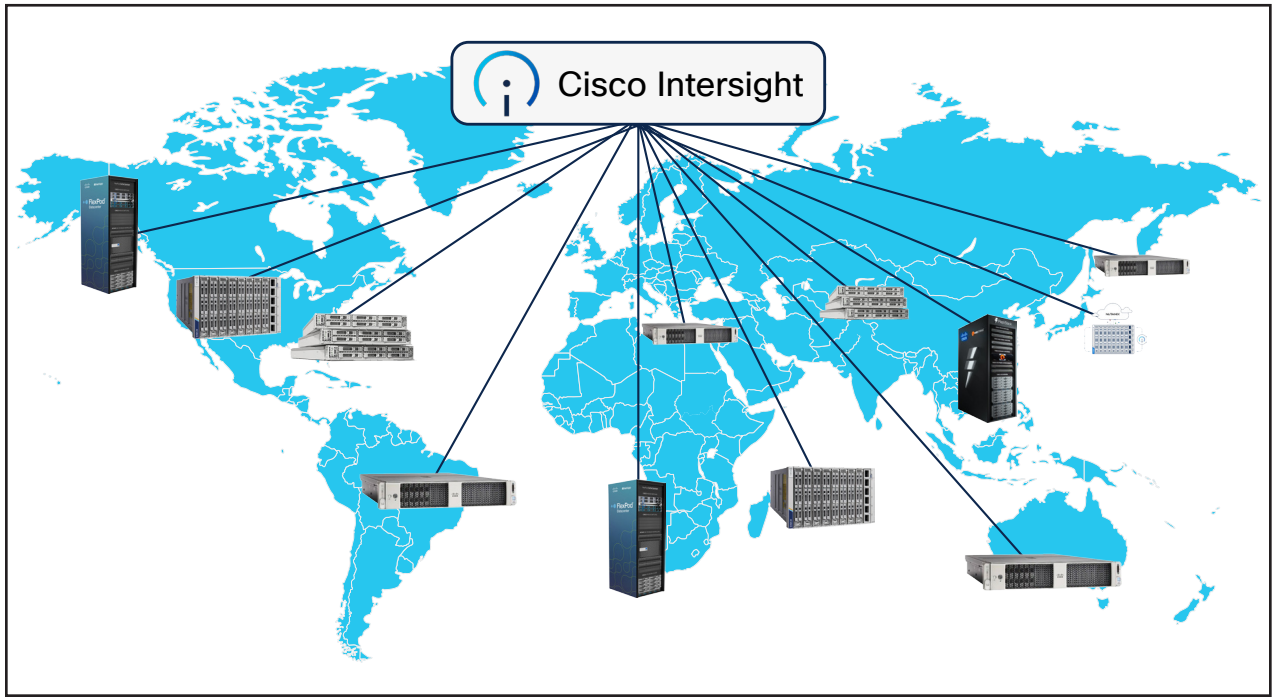

Figure 1. Cisco Intersight simplifies infrastructure lifecycle management regardless of where your IT resources are located.

Cisco Intersight platform

The Cisco Intersight Software-as-a-Service (SaaS) platform helps you translate your intent—what you want to accomplish—into infrastructure configuration, ongoing management, and proactive optimization. With this cloud-based, subscription-model solution, all you have to do is claim your servers, converged or hyperconverged infrastructure, and fabric interconnects in the user interface; license the service; place your resources in logical groupings (such as remote-or branch-office locations or virtualization clusters); and use role- and policy-based interfaces to configure and manage your resources wherever they are located.

Built-in security

The Cisco Intersight platform uses a layered security architecture that builds on industry-standard security technologies. It also encrypts data, complies with strict Cisco security and data handling standards, and separates management and IT production network traffic for additional isolation. As a result, you can have confidence that your cloud-based systems management platform offers the strong security you require.

The importance of security

Your organization must respond to a rapidly changing cybersecurity landscape in which attacks are continually becoming more sophisticated and frequent. When we started designing the Cisco Intersight platform, we knew that security would be of paramount importance. So we built a cloud-based SaaS management platform that offers the strong security you require. Recognizing that some organizations prefer to host a local management server, we also offer the Cisco Intersight Virtual Appliance, which provides the same services. Both of these offerings are SaaS and are kept up to date with our continuous integration process.

Security in the Cisco Intersight platform

The Intersight platform is developed, integrated, and tested using the Cisco Secure Development Lifecycle guidelines. This secure product development and deployment practice has several components ranging from inherent design and development practices, testing the implementation, and creating a set of recommendations for deploying with maximum security. Cisco development processes and the Intersight platform are ISO 27001 certified.

The result is built-in protection to provide device, system, infrastructure, and services security. Using a layered security architecture, Intersight builds on the same industry-standard security technologies that are used widely in Internet commerce. It also encrypts data, complies with strict Cisco security and data handling standards, and separates management and IT production network traffic for additional isolation.

Single sign-on

Single Sign-On (SSO) authentication enables you to use a single set of credentials to log in to multiple applications. With SSO, you can log in to Intersight with your corporate credentials instead of your Cisco ID. Intersight supports SSO through SAML 2.0, acts as a Service Provider (SP), and enables integration with identity providers (IdPs) for SSO authentication.

User authentication and role-based access control

Intersight accounts form the authentication domain for users. The accounts control all resource access, and authenticated users are restricted from seeing any data in accounts where they are not authorized. With the SaaS platform, Cisco login IDs can be used for authentication with the identity provider for

Cisco.com, which includes support for multifactor authentication. Both SaaS and on-premises Intersight implementations allow integration with external identity management systems to meet existing customer authentication requirements.

The Cisco Intersight framework uses granular access control with privileges managed per resource. Intersight software allows configuration of users and groups into several roles, and each user or group can be a member of multiple roles. Roles implemented include the following privileges:

- **Account administrator:** Full control and management capabilities for the Cisco Intersight account and devices under management.
- **Read-only:** Read-only visibility to resources under management.
- **Device technician:** Administrative device actions including device claim to a Cisco Intersight account.
- **Device administrator:** Administrative device actions including device delete from a Cisco Intersight account.
- **Server administrator:** Server lifecycle and policy-based management.
- **User access administrator:** User, group, and identity provider configuration.

In addition to the system-defined roles mentioned above, you can create user-defined roles. Please see the Intersight help pages for specifics on managing roles and resources.

Device connection

Cisco UCS, converged, and hyperconverged solutions are connected to the Intersight SaaS platform or on-premises virtual appliance through a device connector that is embedded in the management controller of each system (Figure 2). The device connector supports an encrypted connection for devices to send information to and receive control instructions from the Intersight platform.

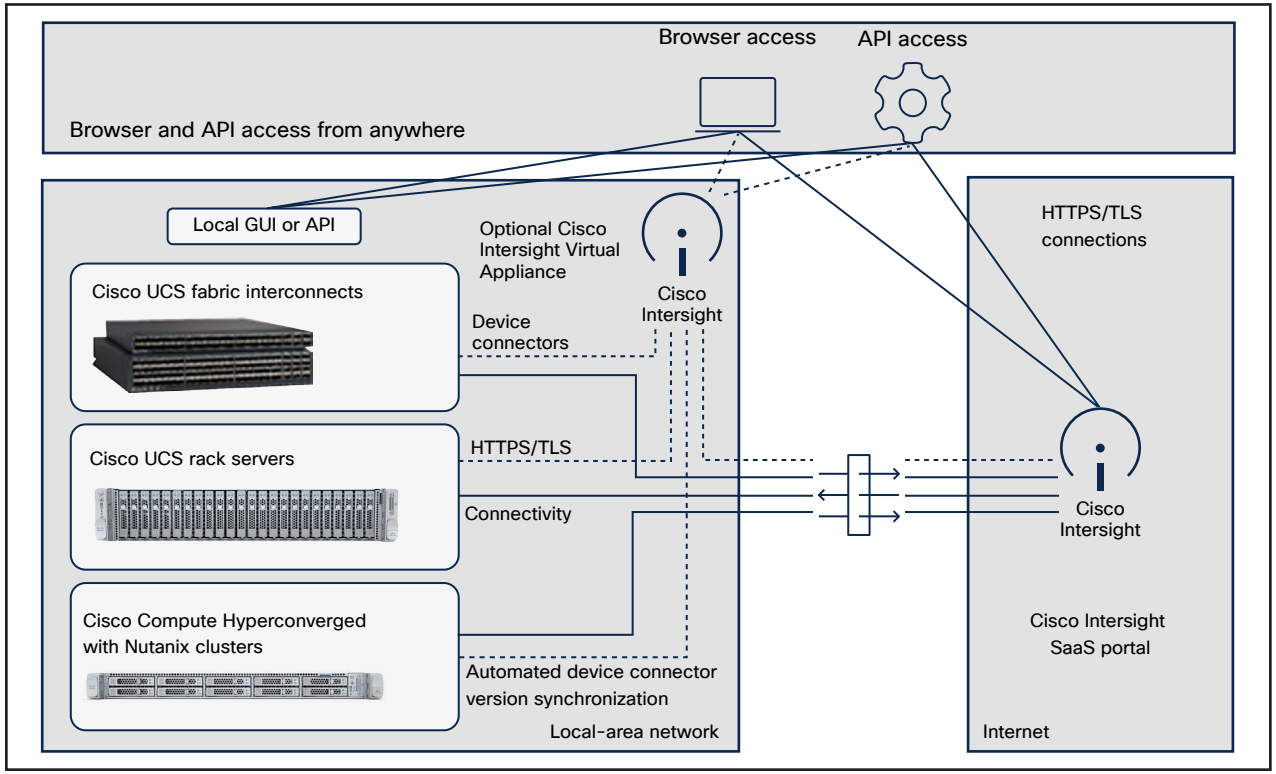

Figure 2. The Intersight platform separates user and device traffic and communicates using industry-standard HTTPS and TLS protocols.

Data encryption and connection security

All data exchanged between devices and the Intersight platform uses industry-standard encryption and security protocols. Connected devices use Transport Layer Security (TLS) with restricted ciphers and HTTPS on the standard HTTPS port 443. All data sent to Intersight is encrypted using the Advanced Encryption Standard (AES) with a 256-bit, randomly generated key that is distributed with a public-key mechanism. In addition, every device connection to the portal is authenticated with a cryptographic token so that only legitimate devices can be managed, thus closing a potential Trojan horse attack vector.

All connections are initiated from the device. Thus firewalls can block all incoming connection requests; only HTTPS port 443 needs to be enabled for outbound connections. As a result, firewalls do not need any other special configuration to enable Intersight connectivity. Devices can be configured to use HTTPS proxy servers to add an additional layer of security through indirection.

To help ensure connection security and prevent man-in-the-middle attacks, devices connecting directly to the Intersight platform use single-destination HTTPS URLs. The platform presents a certificate signed by a Certificate Authority (CA). If an unsigned certificate is presented, the devices will not connect to the portal. Intersight software and the device connector create a secure management framework that provides real-time information related to device security. This approach also allows connected devices and Intersight software to stay synchronized with the latest connection security updates.

Secure device claiming with two-factor authentication

To monitor and manage devices with the Intersight platform, they first must be claimed from an Intersight account. Devices can be claimed using a browser by going to the SaaS or virtual appliance portal and clicking on the **Claim Devices** tab. Device IDs and a claim code, both of which are unique to the device, are retrieved from the device. You can find the device ID and claim code through the device's local management interface. The claim code is refreshed every 10 minutes as an additional safeguard to ensure that the administrator claiming the device has physical access to it.

Two-factor authentication is used to verify the identity and authenticity of each device being claimed. This authentication mechanism adds another layer of security to the device-claiming process. It requires access to the device as well as device identification information that is validated against your Intersight account. In the event that an unauthorized user guesses or learns device information, the user cannot claim a device without access to the device's management interface.

The device-claiming process allows the user to set the device as read-only or allowing control from the Intersight platform. Devices configured as read-only cannot be modified by Intersight software regardless of user privileges within the Intersight account. Devices also can be unclaimed or removed from a Cisco Intersight account through the portal.

Compliance with industry security standards

The Intersight platform meets or exceeds Infosec's requirements applying to numerous industry standards. Details on current certifications, data privacy, and security within the Intersight platform are available at the Cisco Trust Portal (https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=intersight). There's also a guide on security hardening in the Intersight Platform at https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/compute-intersight-hardening-guide-wp.html.

Data collected and encryption at rest

The Intersight platform has complete visibility into and control over managed systems, the same as local API access. Data collected from device connectors on managed systems may include the following:

- **Inventory and configuration data** for fabric interconnects and all servers and nodes, including storage controllers, network adapters, I/O modules, and CPUs.
- **Server operational data** (such as faults) that can be used by the Intersight platform to provide automated recommendations.
- **Technical support files** that can be created when requested by the Cisco® Technical Assistance Center (Cisco TAC).

Note that device connectors do not collect sensitive data that may be stored in the connected systems, such as passwords.

If you use the Cisco Intersight Virtual Appliance, you have control over whether the above data is passed on to the cloud-based portal. If you opt out of additional data collection, the above information is kept locally. The Intersight help pages have more information on data collected by the on-premises Cisco Intersight Virtual Appliance.

For all data collected, the following additional security practices are implemented:

- **Customer data** is kept separate from other customer data through virtual data segregation. Data requests by Cisco Intersight services return data specific to the customer account only, and per-customer encryption keys are used for access.
- **Long-term persistent data** is encrypted at rest. Block storage or similar volume encryption is enabled for all data and tenant files.
- **Third-party access** to data is not permitted.

Compliance with Cisco security and data handling standards

Protecting infrastructure and data requires a close partnership between the Cisco IT and Information Security (InfoSec) organizations. Part of Cisco's Security and Trust Organization (STO), Infosec works with Cisco IT to help ensure that the products we build and the infrastructure we operate are secure. These groups work together to support business productivity while protecting our systems and data from internal and external threats. Instead of focusing on security hardware and software alone, we take a holistic, pervasive approach to security by:

- Developing, integrating, and testing Intersight using the Cisco Secure Development Lifecycle guidelines.
- Incorporating several product development and deployment components into our methodology, ranging from inherent design and development practices, to testing the implementation, and finally to creating a set of recommendations for deployments that maximize the security of the system.
- Fostering a security-conscious culture to reduce the attack surface and provide a robust security posture.
- Implementing security-focused policies and processes.
- Embedding security throughout our infrastructure.

In conjunction with our emphasis on people and processes, we enforce security-focused policies for:

- **Access management:** We enforce requirements for managing user and administrative access to information assets and information systems through proper controls for authentication, authorization, and auditing.

- **Auditing and risk assessment:** We enforce compliance with security and data integrity policies and investigate incidents and monitor user and system activity as appropriate.
- **Cloud security:** The service is cloud-based, and the services we use must adhere to our security requirements.
- **Cryptographic controls:** We use cryptographic controls to protect the confidentiality, integrity, and availability of information assets.
- **Data protection:** We specify requirements for classifying, labeling, and protecting data. These policies define the relative sensitivity of information and determine how this information is treated and disclosed to Cisco employees and other parties.
- **Information security:** We enforce policies specifying the confidentiality, integrity, and availability of information assets.
- **Network access:** We identify authorized users and devices that can access our networks.

Separation of the management network

The out-of-band control plane in the Intersight platform separates management data from IT production and application data. Management data, such as configuration and monitoring information and statistics, flows from devices to the Intersight portal. IT production and application data is sent directly to its destination on your production data network.

The use of an out-of-band architecture means that users are not affected if devices are unable to communicate with Intersight software due to Internet or other service disruptions. Users can still access local management and production networks, and all deployed policies and settings continue to be enforced. In addition, local user authentication is unaffected, and local configuration interfaces remain available.

Security advantages

The management approach of the Cisco Intersight platform offers many security advantages compared to typical monitoring and management tools:

- **Efficiency:** The Intersight platform offloads the responsibility of platform management, allowing IT staff to focus on other tasks and priorities.
- **Device connectivity:** Devices that are managed by Intersight automatically connect and report their configuration and operational status, including their active firmware and software versions.
- **Autonomy:** No human interaction is required on the device after the initial connection is made. There is no agent or other software to install or maintain.
- **Synchronization:** With self-updating device connectors, each device automatically synchronizes with the Intersight platform. Patches and security updates can be pushed to the device connector, as needed with no user action required.
- **Analysis:** Based on data that is automatically collected, Cisco Intersight provides recommendations for infrastructure updates that are needed to keep your hardware, firmware, and software compliant with Cisco's latest tested combinations.
- **Simplicity:** Cisco Intersight provides a single location for tracking and reporting endpoint security and compliance.

"We strive to be trustworthy, transparent, and accountable. That means leaving no stone unturned in our search for threats to our infrastructure or data."

Michele Guel, distinguished engineer and chief security architect, Cisco

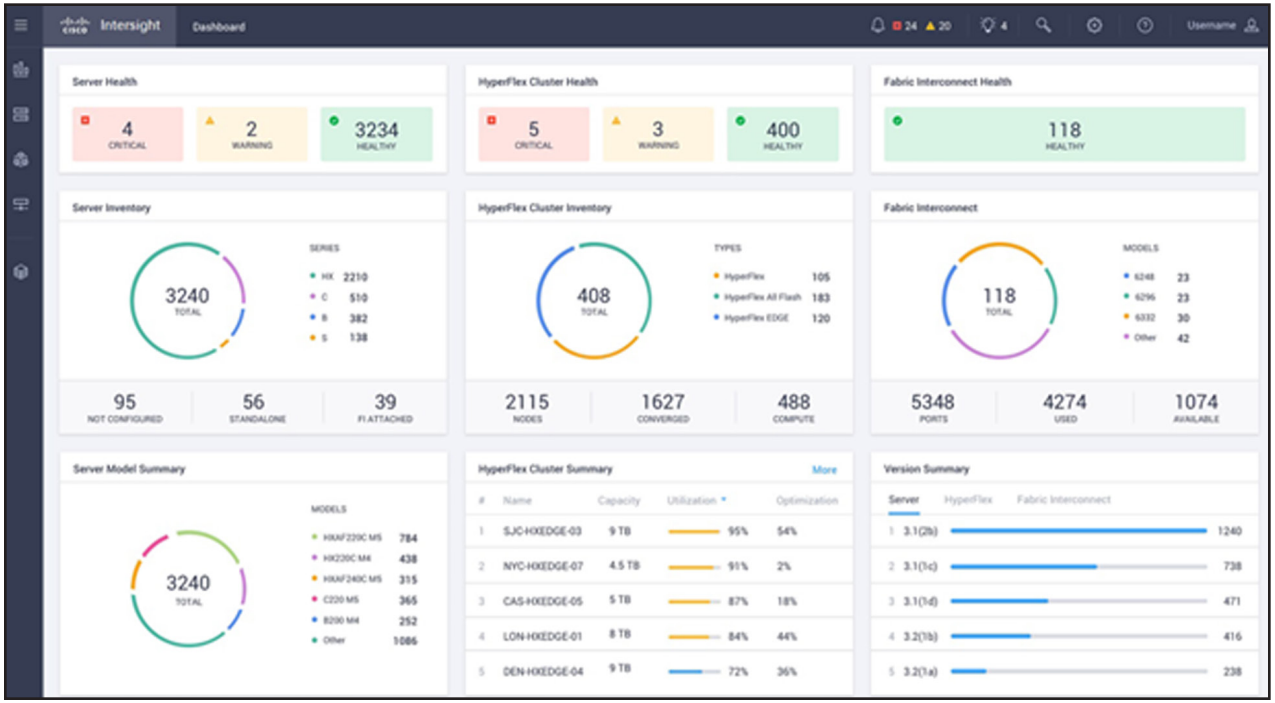

Figure 3. Cisco Intersight dashboard

Portal infrastructure

Intersight management is available through a cloud-based portal. Cisco personnel are available 24 hours a day, 7 days a week, for logistical security, operational, and change-management support. All services are replicated across multiple independent data centers so that user services fail over rapidly in the event of a data center failure.

Data center reliability and availability

- Rapid escalation procedures across multiple operations teams.
- Independent outage alert system.
- Replication of all data (including metrics and device configurations) across data centers.
- Real-time replication of data between data centers.
- Rapid failover of Intersight services in the event of a hardware failure or other data center outage.
- Preservation of end-user network functions, even if portal connectivity is interrupted, through an out-of-band architecture.
- Regular testing of failover procedures.

Secure, out-of-band architecture

- No disruption of your IT production or management network if the connection is interrupted.
- Storage of only management network data.
- Encryption of sensitive data when it is stored.
- Regular penetration testing of data centers.

Data center certification and compliance

- Contact the Cisco Intersight Security and Data Privacy team for specific questions about data center certifications and compliance reports.

For more information

To learn more about the Cisco Intersight platform, visit https://www.cisco.com/go/intersight.

To learn more about Cisco's approach to operational security, visit https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/cs-sec-03232016-operational-security.html.

To learn more about Cisco UCS, visit https://www.cisco.com/go/ucs.

To learn more about Cisco converged infrastructure, visit https://www.cisco.com/site/us/en/solutions/computing/converged-infrastructure/index.html.

To learn more about Cisco Compute Hyperconverged with Nutanix, visit www.cisco.com/go/hci.

Delivering security advantages

The SaaS management approach of the Cisco Intersight platform offers many security advantages compared to local and agent-based monitoring and management tools:

- **Efficiency:** The Cisco Intersight portal offloads the responsibility of platform management, allowing IT staff to focus on other tasks and priorities.
- **Device connectivity:** Devices that are managed by Cisco Intersight automatically connect and report their configuration and operational status, including their active firmware and software versions.
- **Autonomy:** User interaction is not required on the device after initial connection. There is no agent or other software to install or maintain.
- **Synchronization:** With self-updating device connectors, each device automatically synchronizes with Cisco Intersight. Patches and security updates can be pushed to the device connector as needed, with no user action required.
- **Analysis:** Based on data that is automatically collected, Cisco Intersight provides recommendations for infrastructure updates that are needed to keep your hardware, firmware, and software compliant with Cisco's latest tested combinations.
- **Simplicity:** Cisco Intersight provides a single location for tracking and reporting endpoint security and compliance.

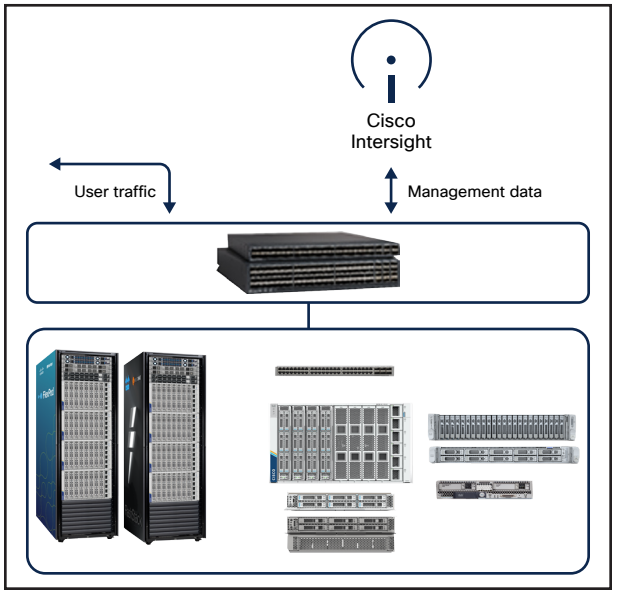

Figure 4. Traffic separation