Cisco N9300 Series Smart Switches with Cisco Hypershield

Security infused into the data center fabric for unprecedented protection

Benefits

- Streamlines security management with a single, centrally orchestrated security policy
- Reduces the number of data-center tools and dashboards, leading to more efficient operations
- Provides high performance, a lower carbon footprint, and reduced latency
- Decreases costs by integrating connectivity and security into a single, cohesive solution
- Ensures comprehensive security services on every fabric port
- Enhances the efficiency of NetSecOps by simplifying management and automating policies
- Prevents advanced threats with an innovative, AI-native approach to segmentation
- Supports your data center to be future-ready with DPU-enabled switches through security software upgrades

Figure 1. Cisco N9300 Series Smart Switch (N9324C-SE1U)

Secure the AI-scale data center

AI has revolutionized modern data centers, but managing these complex infrastructures is challenging. Securing environments with both owned and unowned resources is difficult due to the complexity of security policy creation and enforcement, impacting digital resilience and troubleshooting. Upgrading infrastructure alone isn't sufficient; enhanced security and network services must be integrated natively within the data-center fabric.

A new approach is essential. Cisco is introducing a new family of data center switches that features programmable Data Processing Units (DPUs)—the Cisco N9300 Series Smart switch. These switches embed stateful services directly into the data-center fabric at scale, offering enhanced simplicity, greater service throughput, and improved cost efficiency.

The new Cisco N9300 Series Smart switch makes the data-center infrastructure future ready with an extensible platform for hardware-accelerated services. It initially supports Layer-4 zone-based segmentation powered by Cisco Hypershield and managed by Cisco Security Cloud Control. Future software upgrades will enable additional services such as large-scale NAT, IPsec encryption, IDS/IPS, event-based telemetry, and DDoS protection.

With the integration of Cisco Hypershield, we enable a first-of-its-kind data center security solution that combines an advanced AI-native, hardware-accelerated distributed security architecture with the data center fabric.

What it does

AI-powered security in the data-center fabric

Cisco Hypershield is set to manage security policies on the Cisco N9300 Series Smart switch, initially focusing on delivering high-performance, stateful segmentation on any network port.

At launch, the first Cisco N9300 Series Smart switch will offer 24x100G ports, enforcing security zones across fabrics and hybrid clouds with stateful Layer-3/Layer-4 segmentation. The second switch will provide 48x25G ports, introducing Top-of-Rack (ToR) segmentation capabilities to address Layer-4 east-west

Learn more

- Cisco N9300 Series Smart Switch web page
- Cisco N9300 Series Smart Switch Data Sheet
- Cisco Hypershield web page
- Cisco Hypershield Data Sheet
- Cisco Hybrid Mesh Firewall solution
- Cisco Security Cloud Control

segmentation use cases, which are closer to workloads. These switches can be deployed as leaf switches or as border gateways, with segmentation enforcement on every port. Cisco Hypershield will continuously and dynamically update policies as applications change, move, or expand.

Simplified management

Each Cisco N9300 Series Smart Switch integrates seamlessly into existing operations using the Cisco Nexus Dashboard and Cisco NX-OS open APIs to manage network policies. Hypershield's SaaS-based management tool, Cisco Security Cloud Control, will provision and manage the security policies running on the DPUs.

Additionally, Cisco Security Cloud Control ensures consistent security policies and orchestration across the enterprise. The unified system allows policies to be managed across a library of enforcement points within Cisco Hybrid Mesh Firewall solution. This includes agents in public cloud workloads, on-premises Layer- 4 segmentation Hypershield services switches, and traditional next-generation firewalls that provide deeper security functions such as IDS/IPS and URL filtering for more intensive security inspection. With the Cisco® Hybrid Mesh Firewall solution, the security team can place the appropriate level of controls across the enterprise fabric under a single management system.

A first-of-its-kind data center security solution

These switches enable customers to enhance their network architecture and security posture by placing network and security services closer to where they are needed. The Cisco N9300 Series Smart Switch:

- Provides security as part of the data center network
- Enables autonomous segmentation policies driven by Cisco Hypershield
- Keeps the security posture up to date without the risk of disruption
- Achieves optimal routing with integrated security
- Easily extends consistent policy enforcement across multiple domains

C45-4916751-00 02/25