At a glance Cisco public

Cisco N9300 Series Smart Switches with Cisco Hypershield

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
- Future proof your data center with DPU-enabled switches that can provide additional features with a software upgrade

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 feature 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 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.

Cisco N9300 Series Smart Switches

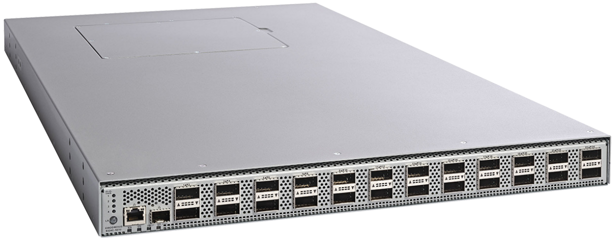

Figure 1. N9324C-SE1U (24x100GbE)

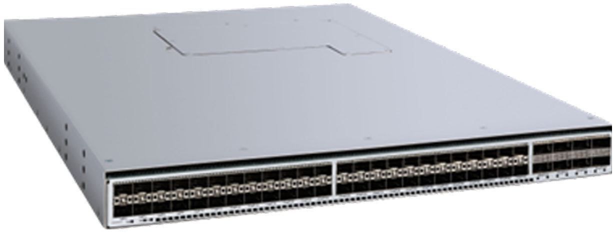

Figure 2. N9348Y2C6D-SE1U (48x25GbE, 2x100GbE, 6x400GbE)

* Layer-4 zone segmentation capabilities are with appropriate licensing and will be coming soon

What it does

AI-powered security in the data center fabric

Cisco Hypershield is designed to continuously and dynamically update policies as applications change, move, or expand. The Cisco N9300 Series Smart Switch utilizes programmable Data Processing Units (DPUs) to enforce Hypershield's policies directly within the switch, delivering high-performance, stateful segmentation on every port.

The Cisco N9324C Smart Switch offers 24x100G ports and is engineered to provide stateful Layer-3 and Layer-4 segmentation services, ideal for high bandwidth applications such as data center zones, interconnects, and cloud on-ramps.

The N9324C and N9348Y2C6D models, featuring a mix of 25G, 100G, and 400G ports, deliver Top-of-Rack (ToR) segmentation capabilities to address east-west segmentation use cases for workloads. These switches can be deployed as leaf switches or border gateways, with segmentation enforcement on every port.

Simplified management

The Cisco N9300 Series Smart Switches will integrate seamlessly into existing network operations using Cisco's NX-OS APIs and will be supported by Cisco Nexus® Dashboard 4.1, which can centrally monitor, manage, and configure network fabrics and devices. Security policies on the switch DPUs will be provisioned and managed by Hypershield's SaaS-based management tool, Cisco Security Cloud Control. This allows both operations teams to simultaneously manage the switch without conflict.

Cisco Security Cloud Control also ensures consistent security policies and orchestration across the enterprise. The unified system allows policies to be managed across a library of enforcement points within the Cisco® Hybrid Mesh Firewall solution. This includes agents in public-cloud workloads, on-premises Layer-4 segmentation Cisco N9300 Series Smart 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

The Cisco N9300 Series Smart Switches empower customers to optimize their network architecture and enhance security by integrating network and security services directly where they are most needed. Key features include:

- **Integrated security:** provides security natively within the data center fabric, ensuring robust protection without the need for additional hardware
- **Autonomous segmentation:** utilizes Cisco Hypershield to drive autonomous segmentation policies, enhancing security, and operational efficiency
- **Continuous security updates:** maintains an up-to-date security posture with seamless updates, minimizing disruption risks
- **High-performance segmentation:** delivers high-performance network segmentation, simplifying routing and reducing operational costs
- **Consistent policy enforcement:** extends consistent policy enforcement across multiple domains, ensuring uniform security standards

These switches are designed to streamline security management with a single, centrally orchestrated security policy, reduce the number of data center tools and dashboards, and provide high performance with reduced latency and a lower carbon footprint.

Learn more

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