Cisco N9300 Series Smart Switches with Cisco Hypershield



© 2026 Cisco and/or its affiliates. All rights reserved.

Secure data center networks for the agentic era AI and agentic workloads from modern applications are reshaping the data center, generating machine-scale east/west traffic, connecting hyper-distributed workload types, and evolving faster than traditional security architectures can keep pace.

Cisco N9300 Series Smart Switches change the equation, fusing proven Cisco Nexus® networking with programmable data processing units (DPUs) to enforce security inline, right where the workloads live. Cisco Hypershield™ centralizes security policy and distributes enforcement across every point in the fabric, so your security posture scales as fast as your environment does.

The result: a data center built to secure the AI agentic era, without the complexity, latency, or cost of traditional architectures.

© 2026 Cisco and/or its affiliates. All rights reserved.

Fuse security with networking

Table 1. Fuse security with networking

Contain Threats Closer	Scale Without Chokepoints	Simplify operations
Enforce stateful segmentation directly in the fabric.	Distribute security services across switches instead of relying only on centralized appliances.	Combine networking, security enforcement, and telemetry in a compact platform.

Better together

Cisco Hypershield defines the policy. Cisco 9300 Series Smart Switches enforce it.

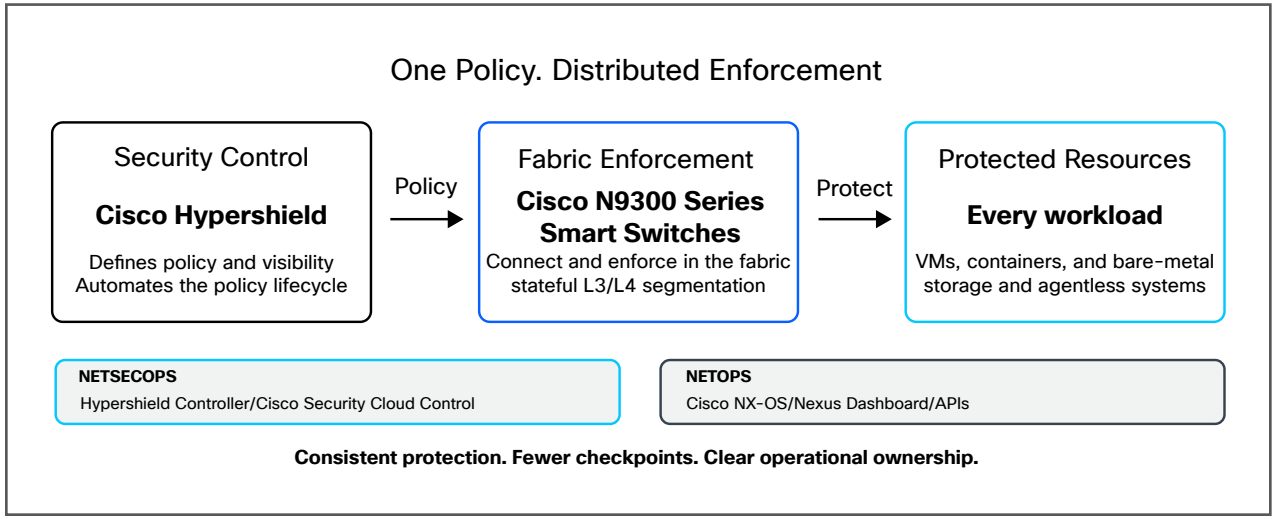


Figure 1. Consistent protection across every workload

Table 2. One policy, distributed enforcement, clear operational ownership.

Consistent policy across Cisco N9300 Series Smart Switches and workload agents **Enforcement closer to applications and data** **Less traffic hairpinning through centralized inspection points**	Shared network and security context for faster troubleshooting Independent NetOps and NetSecOps control with coordinated outcomes

Architectures that create value

Customer need	How N9300 Smart Switches and Hypershield deliver
Top-of-rack segmentation	Turn the access layer into a distributed enforcement point for connected workloads
Zone-based segmentation	Apply high-scale, stateful policy between application, tenant, and security zones
Data-center interconnect and cloud edge	Combine routing, segmentation, and security services in a compact platform
Mixed and agentless workloads	Extend protection to workloads where installing host agents is impractical

Select the enforcement model



Figure 2. N9348Y2C6D-SE1U | 48-port top-of-rack



Figure 3. N9324C-SE1U | 24-port services

© 2026 Cisco and/or its affiliates. All rights reserved.

Table 3. Cisco N9300 Smart Switches

Model	Connectivity	Services capacity	Designed for
N9348Y2C6D-SE1U	48 x 25G, 2 x 100G, 6 x 400G	800G DPU services throughput	Top-of-rack and east/west workload segmentation
N9324C-SE1U	24 x 100G	800G DPU services throughput	Top-of-rack, zone segmentation, cloud edge, and data-center interconnect

Both models combine a Cisco® Silicon One® E100 networking ASIC with programmable AMD DPUs.

Table 4. Clear operational ownership

Team	Management tools	Primary responsibility
NetOps	Cisco NX-OS, Nexus Dashboard, and NX-API	Fabric connectivity, routing, switch lifecycle, network policy, and telemetry
NetSecOps	Hypershield on-premises controller or Cisco Security Cloud Control	Security policy, stateful segmentation, compliance, and security telemetry

Purpose-built controls for each team, with shared context for coordinated operations and faster troubleshooting.

“With the Cisco N9300 Series Smart Switches, we brought together high-performance networking, stateful segmentation and policy enforcement into a single platform. That let us modernize our infrastructure and strengthen security without adding complexity or compromising performance.”

Kevin Ludwig,
AVP of Information Technology, XiFin, Inc.

© 2026 Cisco and/or its affiliates. All rights reserved.

For more information

- Cisco N9300 Series Smart Switches
- Cisco N9300 Series Smart Switch Data Sheet
- Cisco Hypershield
- Cisco Hypershield Data Sheet
- Cisco Hybrid Mesh Firewall solution
- Cisco Security Cloud Control
- Cisco Nexus One Solution Overview
- Cisco Live Protect

Deployment Flexibility

On-premises and air-gapped: Use the Cisc Hypershield on-premises controller for local security management.

Connected: Integrate with Cisco Security Cloud Control for cloud-based management and broader visibility.

Table 5. Build security

Build security into your next data center refresh Start with the network. Add distributed enforcement where it is needed. Scale protection as the data center grows.	SMART SWITCH + HYPERSHIELD

Learn more

- Cisco N9300 Series Smart Switches
- Cisco N9300 Series Smart Switches Data Sheet
- Cisco Hypershield
- Cisco N9300 Series Smart Switches FAQ

Capabilities, licensing, scale, and availability depend on the applicable software release and subscription. Confirm current requirements with Cisco documentation or your Cisco representative.

© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C45-4916751-04 08/26