Partner VT (October 2026) v2

Notice: The content listed below are just a few highlights from the latest Partner VT. For more detailed updates, refer to the related links below or contact your Cisco Channel team.

Cisco **Partner Virtual Team:** For internal and partners to receive updates and roadmaps from the BUs on the solutions and technologies being developed.

Secure Firewall & Secure Access: (Day 1)

Secure Firewall (models):

- **240P:** Desktop, 4x PoE, 3.2 Gbps (1024B) for NGFW traffic profiles (10.1)
- **CSF6120 & CSF6130:** ASA s/w for AI Data Centers, SP's, 300+ Gbps /RU (9.24)
- **CSF6160 & CSF6170:** 635 Gbps for NGFW, advanced FPGA chip, NVMe slots (10.0 & 9.24)
- **FTDvU:** Available for Private Cloud (KVM ESXi) (10.0) - unlimited extends to AWS (10.1)

Secure Firewall (features):

- **Hybrid Private Access** Deployments can now support IPv6 Traffic Flows (10.1)
- **Auto Tunnel Setup -** Automatic config push to Firewall and Secure Access (10.1)
- **Multicast Across SVTI Site-to-Site Tunnels** - FTD/ASA multicast routing to Static VTI (10.1)
- **CSDAC Air-Gap Support:** for OT, FED, installed on FMC - vCenter, Cyber Vision etc. (10.1)
- **EVE: SSH & STUN:** fingerprints from SSH key exchanges & STUN binding requests (10.1)
  - **Port-agnostic detection:** Identify SSH/STUN sessions no matter which port used (10.1)
  - **Process-level attribution:** Tie sessions back processes, expose malware in tunnels (10.1)
  - **Malware-initiated connection detection**: Detect trojan launch SSH/STUN sessions (10.1)
- **Encrypted DNS Inspect:** DNS over HTTPS (DoH) HTTP/1.1, 2, 3 - decrypt & inspect (10.1)
- **SnortML:** URL queries, URL-encoded POST data, multipart/form-data POST data. (10.1)
  - **SnortML default** in Security over Connectivity IPS policy (10.1)

Live Protect:

- **Vulnerability shielding:** Identify affected assets, Deploy Shield, Monitor, Patch (GA)
- **Available on select Cisco platforms** – N9000, CW9800, 8000 Router etc. (today – future)

Post-Quantum Cryptography (PQC):

- Quantum-safe communications across core Cisco portfolio (June 2027)

Secure Access:

- **Access Policy:** Extending Enterprise policy capabilities (GA)
  - **Geolocation:** Construct source based geolocation policies for tighter access control (GA)
  - **Policy Edit Lock:** Prevent conflicting policy changes, time based edit with override (GA)
  - **Advanced Boolean:** Two and three way 'AND' capabilities for flexibility (GA)
- **Destination List Alerts:** Trigger maint. workflows for integrations (e.g. STIX/TAXII etc.) (GA)
- **Enhanced DGA Detection:** Improved for AI modeling for DGA, Predicative protection (GA)
- **Enterprise Data Loss Prevention (DLP):** Real-time DLP, SaaS API, Endpoint & Email DLP (GA)
- **Endpoint DLP:** Securing confidential data before it leaves the device (GA)
- **User Entity & Behavior Analysis:** Detect anomalies (e.g. Impossible Travel, File Spikes) (GA)
- **DSPM:** Discovery classification sensitive data - smart scanning (GA)
- **Secure Access with Enterprise Browser:** Device trust, Posture, DLP, Access Control (GA)
- **Agent Gateway:** LLM, API & MCP Gateways (BETA)
- **Public MCP Server:** OpenSource, 72+ tools (Destination lists, search for Domains etc.) (GA)
- **Cisco Secure Access Splunk Add-on:** Event Snapshots (GA)

Umbrella SIG & DNS:

- **End of Sale** (Jan 2027) – End of Support / Service (Jan 2029)

Hypershield / Vuln Mgmt.: (Day 2)

Hypershield:

- **Controller Architecture:** On-Premise Mgmt., Optional Global Mgmt. via SCC (GA)
- **Policy Definition and Validation:** Unordered Policy, Network Connection Map (GA)
- **Management:** RBAC with OIDC Auth, Centralized Management of Syslog (GA)
- **Data Plane:** Inter and Intra VRF and VLAN Segmentation etc. (GA)
- **Policy Studio:** Individual intents, translates & routes to products, enforce (CY27)

Vulnerability Mgmt.

- **Open Source:**
  - **Project CodeGuard:** Translators for the popular coding agents (Prevention)
  - **Antares:** Returns a ranked list of suspect files (Detection)
  - **Foundry Security Spec:** A blueprint, not a scanner you install (Governance)

Identity / Cloud Control / Secure Networking: (Day 3)

Identity Services Engine (ISE): (cs.co/ise-roadmap)

- **Cisco Cloud Control:** Free (Cisco) & Paid (*Entra ID*, *Okta* etc.) tiers for Identity (GA)
- **Java8 to Java21:** Improved garbage collection, improved throughput etc. (4.0)
- **Oracle to Postgres:** Data Connect tables should not change (4.0)

Access Manager: (cs.co/am-roadmap)

- **Network Access:** RADSec over TLS, Eduroam Phase 2, TEAP (CY27+)
- **User Identity:** IdP - Duo, Google, Okta, On prem AD, etc. (CY27+)
- **Endpoint Identity:** Endpoint Profiling – mDNS, HTTP probes etc. (CY27+)

Cisco Cloud Control:

- **Regional Residency:** Data & control planes localized AWS or regional clouds (CY27)

Secure Networking:

- **Attach:** LDoS (Cat Center), Un-attached devices, AVoIP (Control Hub) (GA)
- **Secure:** Segmentation / Identity, Live Protect, Fabris App in C3, PQC (SD-WAN) (GA)
- **Observe:** ThousandEyes, Cisco Data Fabric, Splunk - Secure Net Essentials (GA)

Random Related Links:

		Identity Training
PVT Presentations	Firewall Perf. Est v2	Security Essentials
PVT Q&A Team Room	Secure Firewall	Security Trials Console
Firewall Feature Matrix	ISE Release Notes	Fire Jumper Landing
Firewall Migration Tool	Quantum-Safe Computing	FireStarter

Available | Beta / Private Preview / Targeted availability | Estimate