Security Architecture Summit (May 2024) v1

Notice: The content listed below are just a few highlights from the latest Security Architecture Summit. For more detailed updates, refer to the Community link posted or contact your Cisco Channel team.

Cisco Partner

Cisco **Security Architecture Summit:** For internal and partners to receive updates and roadmaps from the BUs on the solutions and technologies being developed.

Network & SSE: (Day 1)

Security AI Strategy:

- **AI Assistant in Secure Access :** Simplify and speed up, reduce human error. (GA)
- **XDR AI Assistant:** Recommend action, Investigate IOC, Incident summary (Future)
- **AI Assistance:** Embedded Mode (XDR, CDO, Duo) & Unified Mode (Future)
- **Secure Access AI:** Threat Visibility, Leakage Prevention, Threat Prevention (GA)
- **Email Threat Defense AI:** Natural language understanding, 30+ Detectors (GA)

Secure Firewall:

- **1200 Series:** System-on-a-Chip, (2) Desktop and (3) Rackmount models (Dec 2024)
- **Individual Mode Clustering:** Clusters can use individual data interfaces (FTD v7.6)
- **Virtual Firewall on DPU:** NIC w/ Data Processing Unit in Server or Switch (Future)
- **QUIC (HTTP/3):** Decryption and Inspection (FTD v7.6)
- **SnortML:** Neural Exploit Engine uses ML to expand IPS capabilities (FTD v7.6)
- **Selective Traffic Decryption:** Goal: Classify 90% as benign, inspect 10% (Future)

Hypershield:

- **Hypershield**: Workload to Workload protection (on-prem & in cloud) (Aug 2024)

Secure Access:

- **VPN Mgmt. Tunnels**: Auth against directory services before login, etc. (July 2024)
- **Auto Upgrade Connector:** Lifecycle mgmt., less Admin overhead (July 2024)
- **Image Scanning (OCR):** Related to DLP, scan images in multi-languages (July 2024)
- **SSH Clientless:** Remote access for SSH (July 2024)
- **Unifying Posture:** Auth user and attributes about what connecting with (Oct 2024)
- **Optimized HTTP/3:** Allow ZTNA Clients to operate natively (e.g. QUIC) (Jan 2025)
- **Universal L7 Controls:** Fingerprint, Identify & write policy on traffic (July 2024)
- **Virtual Appliance:** Support for those moving into....(July 2024)
- **RBI for Private Apps:** Control user from directly accessing local App (Oct 2024)
- **Identity Intelligence:** Info about user (where user is, how connecting...) (Jan 2025)
- **Much, much more…**

Identity & Access: (Day 2)

Identity Intelligence:

- **Integrations:** Duo, XDR & Secure Access, ISE via pxGrid cloud (Future)
- **Risk/Threat Score(s):** In design & planning stage now (Future)

Identity Services Engine (ISE):

- **Integrations:** App Centric Infrastructure, Cat Center, SD-WAN Manager (July 2024)
- **General Availability:** Workload Context, Cloud FMC, Secondary SGTs (GA)
- **General Availability:** Policy Matrix UI Enhancements (v3.4 patch 2 - Oct 2024)
- **General Availability:** Meraki, SXP v5 (v3.4 patch 3 - Jan 2025)

Cyber Vision:

- **IoT:** Cyber Vision 5.0, new UI (June 2024)

Threat Detection & Response: (Day 3)

XDR:

- **Detection Analytics (Cisco):** Secure Access, Identity Intelligence (July 2024)
- **Detection Analytics (3rd Party):** MS Defender, Palo Alto NGFW / Cortex, etc. (July 2024)
- **Threat Hunting (Cisco):** Cisco Identity Intelligence (July 2024)
- **Threat Hunting (3rd Party):** Service Now (ITSM), ThreatQuotient (TIP) etc. (July 2024)
- **Automation & Response (3rd Party):** Jira, MS Teams, ZenDesk, ServiceNow, etc. (July 2024)
- **Asset Insights (3rd Party):** AWS, MS Azure, Google Cloud (GCP), Darktrace, etc. (July 2024)

Cloud Security: (Day 4)

Multicloud Defense:

- **CSP Integration:** CloudWAN Services insertion (AWS). Azure Marketplace (July 2204)
- **Portfolio Integration:** Static object sharing w/CDO, S2S VPN, OnPre to Cloud VPN (July 2024)
- **Product Enrichment:** Azure NAT GW Orchestration, GRE tunnel insp., etc. 2.0 (July 2024)

Cloud Application Security (Panoptica):

- **Integrations:** Multicloud Defense, Vulnerability Mgmt., Secure Endpoint (GA)
- **Graph query:** Security graph, vector database, turned on as MVP (preview)
- **API Security gateways:** AWS GW, AWS VPC Traffic Mirroring, ApigeeX, NGINX (GA)
- **Platform maturity:** Scaling Improvements, Platform operations (July 2024)
- **New Features:** Policy mgmt. framework across, CSPM, CWP, AIPSec (July 2024)
- **New Features (cont.):** CDR, DSPM and GenAI Assistance as scheduled (July 2024)
- **Network Security:** v1 is Multicloud Defense (July 2024)
- **Identity Permission Analysis:** A step towards CIEM (July 2024)
- **Policy Management** (July 2024)
- **Future features:**
  - GenAI Attack Engine
  - Supply Chain Policy enforcement
  - VM & Serverless Runtime Scanning
  - Deeper toolchain integration (Jira, GitHub)
  - End to end risk visibility (from code to prod)

Random Related Links:

- **Summit Presentations**
- **Summit Q&A Team Room**
- Fire Jumper Academy
- Beers with Talos
- ISE Demos
- ISE Webinars
- ISE Instant Demo
- ISE Resource Guide
- Oort Demo (Genie)
- Oort Podcast
- Multicloud Defense
- Splunk Acquisition

Available | Targeted availability | Estimate

WO-05242024