

Security Information & Event Management (SIEM)

- Cisco Splunk
- ExaBeam
- Fortinet FortiSIEM

Endpoint Detection and Response (EDR) & Extended Detection and Response (XDR)

- Cisco XDR/NAC/ISE/SNS/SecureX
- Palo Alto Networks Cortex
- CrowdStrike Falcon XDR
- Forescout Asset Discovery, Device Posture Management and NAC

Network Traffic Analysis (NTA)

- SolarWinds NTA
- Darktrace AI/ML NTA
- NetScout Arbor Insight and Probes

Security Orchestration, Automation, and Response (SOAR)

- Palo Alto Networks Cortex
- Rapid7 InsightConnect
- Darktrace Antigena AI SOAR

Threat Intelligence & Threat Feed

- CrowdStrike Falcon Intelligence
- McAfee Advanced Threat Defense (ATD)
- Palo Alto Networks Unit 42 Threat Intelligence
- Darktrace AI/ML Threat Analysis Platform

Enterprise Anti-DDoS solution

- Radware DefensePro
- NetScout Arbor

Deception Technology

- Attivo ThreatDefend Deception Platform
- Guardicore Centra Deception
- Illusive Networks

Standalone security appliances (inc. virtual) – Firewall, IPS, NAC...

- Cisco
- Huawei
- Juniper
- Fortinet
- Palo Alto Networks

