At-a-Glance

Cisco Security Solutions for Service Providers earn the industry's first third-party validation for securing physical and hybrid network functions virtualization environments.

Demonstrated Value

- Security effectiveness
- Service chaining and stitching with third parties
- Dynamic security orchestration in SDN and NFV
- Security services in a virtualized multitenant environment
- Performance, scalability, and resiliency with few disruptions

"The EANTC team found Cisco's suite of capabilities more than capable of meeting the needs of today's progressive enterprises and service providers, whether in a virtualized environment or when a hardware-based solution is needed to deliver certain levels of performance and scale."
– Light Reading

Cisco Service Provider Security Solutions – EANTC Validation

New Opportunities, New Threats

Massive digital transformation is creating significant new opportunities for service providers. The number of Internet-connected devices will grow from 15 billion today to 500 billion by 2030. The rise of cloud computing is a game changer for service provider service delivery, resulting in greater efficiency, higher capacity, and reduced costs.

Regrettably, as modern networks evolve, the attack surface that service providers must protect is expanding. Financially motivated attackers recognize the opportunity and devise sophisticated methods to infiltrate networks and steal newly digitized assets.

$87K
Loss for every 1K data files breached[1]

$1.45M
Average lost business cost per attack[1]

60%
Of security breaches compromise data in hours[2]

[1] Verizon – 2015 Data Breach Investigations Report

[2] Ponemon Institute – 2015 Cost of Data Breach Study: Global Analysis

Security is foundational to seizing emerging business opportunities created by the digital economy. It is critical to protect your customers and your own organization from threats, and security can also be a huge business enabler. Security as a service to your customers will differentiate your business offerings and create new revenue streams. Imagine a comprehensive threat-centric security solution, delivered with network functions virtualization (NFV) technology to protect your business, customers, services, and infrastructure. With validated Cisco NFV security solutions, you can now quickly and confidently adopt these solutions and capitalize on digital growth opportunities.

Test Overview and Results

The comprehensive battery of tests performed by EANTC demonstrates that the Cisco evolved security architecture delivers industry-leading performance and security effectiveness for service providers.

Test 1: Security Effectiveness

EANTC demonstrated that service providers can keep their networks and their customers safe by blocking the most advanced threats before they can damage their business. EANTC deployed the Cisco Firepower NGIPS and the Radware distributed denial-of-service (DDoS) defense across the test network, including customer premises, the service provider network edge, the service provider data center, and the cloud. It validated a dramatic reduction in time to detection (TTD) of known threats from the current industry estimates of 100 to 200 days[3] to mere hours.

Test 2: Service Deployment Agility

This test showed that service providers can simplify new security service deployment to increase business agility. Two virtual security service chains were dynamically orchestrated. The first was used to measure time to verify and mitigate a business-crippling DDoS attack. The second showed how Cisco Firepower Threat Defense can stop attacks as they happen with the Cisco ASA firewall, NGIPS, and Cisco Advanced Malware Protection (AMP).

[3] Cisco Annual Security Report

Test 3: Simplified Orchestration, Lower Cost and Complexity

Test 3 validated that security can be dynamically orchestrated across both SDN and NFV in hours. The virtual Cisco ASA firewall and NGIPS were dynamically allocated by the Cisco Application Centric Infrastructure (ACI) Application Policy Infrastructure Controller (APIC). This integration with Cisco virtual security technologies enables rapid orchestration, so you can quickly spin up and down security virtual network functions (VNFs).

Test 4: Consistent Security for Multitenant NFV Environments

The fourth test focused on a key service provider business imperative: to isolate and protect each individual customer's workflow without disrupting other customers' service. The test showed that data center security services can be protected, scaled, and managed in an end-to-end multitenant NFV environment without impact to an individual customer's performance or service.

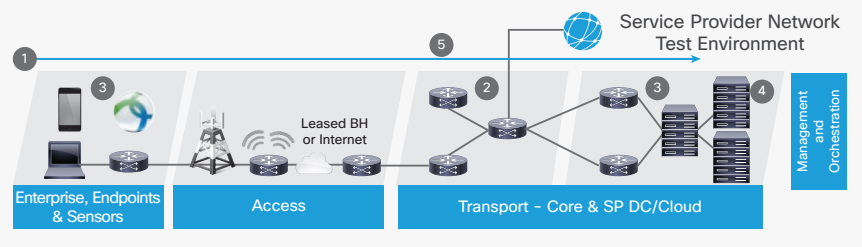
Test 5: Superior Performance and Greater Business Continuity

The final test simulated a large-scale cloud data center environment to validate carrier-class performance, scalability, and resiliency while running a catalog of security services. The Cisco security capabilities exceeded requirements for the most demanding service provider cloud and NFV environments.

Validated Threat-Centric Security for Service Providers

The telecommunications industry information company Light Reading commissioned an independent test lab, the European Advanced Networking Test Center (EANTC), to evaluate Cisco's threat-centric security solutions for service provider cloud and NFV environments.

The testing validated that Cisco's security architecture delivers comprehensive threat-centric security that protects across the entire attack continuum: before, during, and after an attack. Furthermore, it tested firewalls, VPNs, next-generation intrusion prevention systems (NGIPS), and URL filtering virtually within the network or running on the Cisco Firepower™ 9300 Security Appliance. The common orchestration capability was used to turn on software features across the service provider network and data center or cloud.



Next Steps

Contact Cisco sales for more information. Find out more at Service Provider Security Solutions.

C45-737650-00 08/16