ECI THE ELASTIC NETWORK

NFV

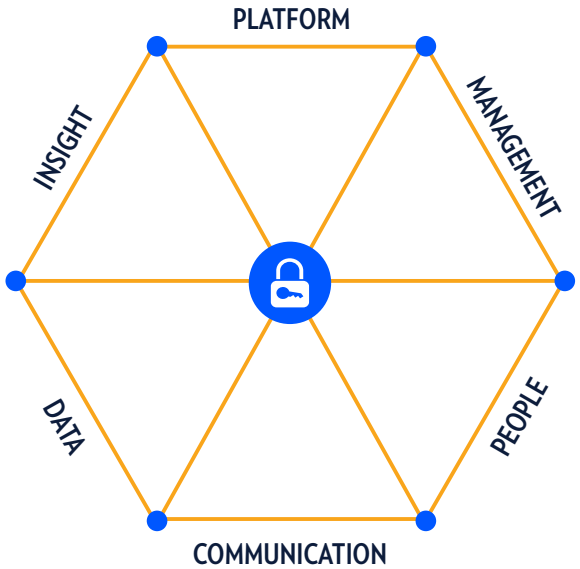
CYBER SECURITY APPLIANCE*

Until recently, network customers have been purchasing assorted services, each running on a dedicated appliance, and connected to the organizational network. ETSI recognized the complexity and cost consequences of this trend, and the need to provide quick and time to market network solutions. So, they defined the Network Function Virtualization (NFV) standard to address and simplify it. NFV allows these customers to use a single platform to run all of these applications and services. This significantly reduces the associated Capex and Opex of the hardware mix, energy consumption, labor, and more.

Introduce	Utilize	Offer	Increase
new cyber security services	NFV on ECI cyber appliance	cyber security value-added services	revenues and reduce costs (CAPEX/OPEX)

ECI's Cyber Security Appliance is a new NFV platform, designed as a standalone solution for multivendor-based networks. The NFV approach replaces traditional purpose-built equipment with an elastic, robust, and generic platform.

The NFV appliance is furnished with generic x86-based engines and a virtualization environment that can be configured remotely and run a variety of applications. The ECI holistic 'Hexagon' security paradigm provides the most suitable cyber security solution. It is designed with a central point of control featuring intelligent, real-time, aggregated views for a total unified IT/operational network.



***ECI customers running on the NEPTUNE platform can obtain a proprietary single T-slot card that supports the same capabilities as the NFV appliance.**

Security applications supported

The NFV appliance supports service chaining, a highly effective "horizontal" traffic steering function. This capability channels the traffic to pertinent Virtual Network Functions (VNFs) only, saving considerably on network security application resources. The following is a synopsis of the powerful security apps supported by the appliance:

Firewall

The firewall controls incoming and outgoing network traffic, based on an applied set of rules. Simultaneously, it creates a barrier between a trusted secure network and a non-trusted network. This provides a multilayer protection firewall suite, including five security gates, between the public and private networks. Each security gate supports intelligent security technologies suited to a specific layer including MacSec capabilities, IPSec, NAT, header analysis, user ID, data validation, full-session state management, IP/Port/User-based ACL, integrated, and URL awareness. This offering is part of our alliance with Checkpoint and our solution implements their Next Generation Threat Prevention for multilayered security protection.

L2 encryption

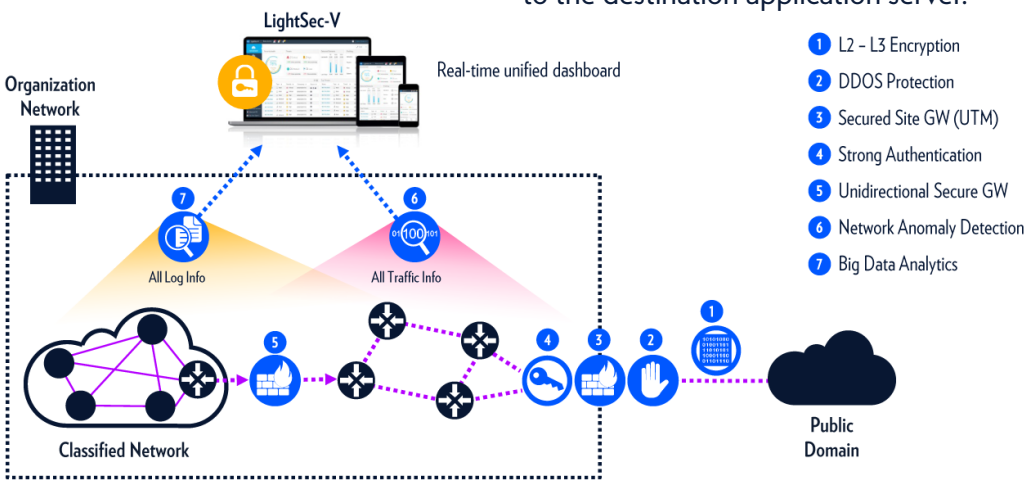
Layer 2 Encryption delivers data confidentiality and integrity for sensitive data-in-motion in shared environments, preventing one tenant from monitoring the network traffic or attacking the virtual servers of another tenant. Furthermore, it allows the data owner or a trusted third party to control the encryption keys (AES-256) without having to share them with the infrastructure provider. The virtual application protects one or more virtual servers and links by enforcing the encryption and isolation policies specified in the centralized key and policy management system for the ECI cyber solution.

L3 encryption (IPSec)

IPsec is a protocol suite for securing IP communications by authenticating and encrypting each IP packet of a communication session. IPsec can be used to protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). It also supports network-level peer authentication, data origin authentication, data integrity, and data confidentiality (encryption), plus replay protection.

Front-end perimeter

The front-end perimeter is a dual-node patented approach for protecting your infrastructure from a less secure network. This eliminates the need to deploy reverse-proxy solutions or maintain incoming firewall ports. It also improves the security of the networks and simplifies network configuration, thereby reducing operation, administration, and management (OAM) costs. The solution has two-tier deployment architecture, comprising an external and internal node. The external node serves as a front-end to all services published. This node ensures that only legitimate session data can traverse the internal network. It operates without opening **any** ports within the external firewall. The role of the internal node is to deliver the session data to the internal network from the external node, scan it using various application-level security techniques, and then pass it on to the destination application server.



SSH interception

The front-end perimeter implements a patented dual-node approach for securing the network from the outside, or as a standalone SSH Proxy. This method eliminates the need to store sensitive data in another network (e.g. DMZ), to deploy reverse-proxy solutions, or to maintain incoming firewall ports. The solution improves the security of enterprise networks and simplifies network configurations. This reduces OAM costs considerably. The solution features a two-tier deployment architecture, comprising an external node and an internal node. The role of the external node is to serve as a front-end to all services published. This node ensures that only legitimate session data can traverse into the internal network. It functions without opening any ports within the external firewall. The role of the internal node is to pull the session data into the internal network from the external node. It scans the data using various application level security techniques, and passes it on to the destination application server.

Block application level attacks are prevented by inspection and control of the incoming traffic on the application layer to detect and mitigate virus, trojan, and malware attacks. This is performed both on clear channels and encrypted channels, such as HTTPS.

SCADA IPS/IDS

This is a fast and optimized pattern-match mechanism that provides:

- Enhanced state awareness, deep per-packet inspection
- Quick identification of common signatures within the packet
- Signature matching based on a programmable set of rules
- Ability to load any rule/signature at runtime without affecting traffic
- Dynamically updating signatures, and
- Focus on MODBUS, DNP3, BACnet, and additional SCADA protocols
- A fully-agnostic engine
- Real-time insights of cyber security and operational incidents

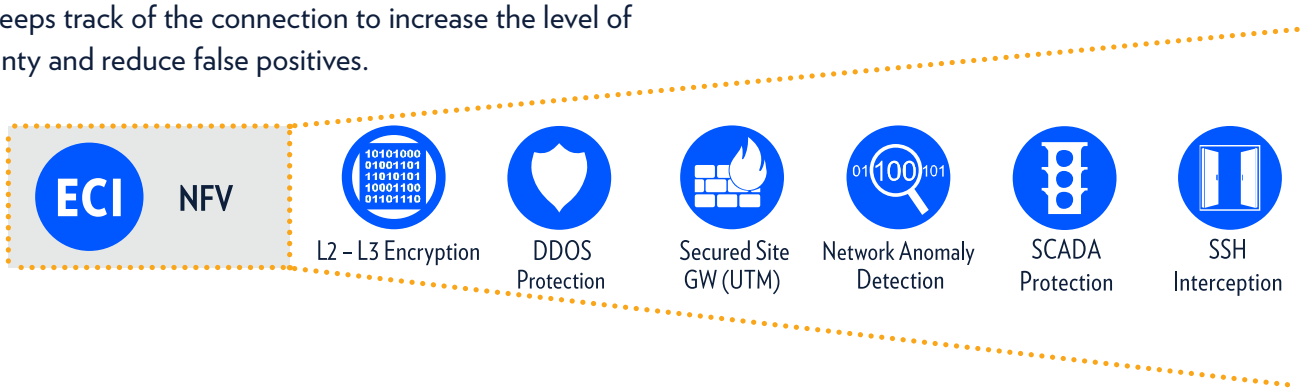
SCADA IPS/IDS quickly filters out the vast majority of traffic that is clearly harmless (identifying simple signatures at a low CPU cost). Traffic marked as suspicious (common attack signature detected) is forwarded for further analysis. SCADA searches deeper in the packet and keeps track of the connection to increase the level of certainty and reduce false positives.

SCADA anomaly detection

The ECI cyber network Anomaly Detection (AD) solution for the SCADA sector is much more extensive than just an IDS/IPS. One of its features is based on a genuine engineering approach. It employs a combination of scenario and anomaly detection techniques, determined to discover threats within the SCADA network.

The SCADA AD solution also includes the following key features:

- A powerful anomaly detection engine, which provides the only situational aware solution on the market
- A fully-agnostic engine
- Real-time insights of cyber security and operational incidents
- Investigation and forensic capabilities
- An intuitive UI, which provides simplified navigation capabilities
- Deep Packet Inspection (DPI) of industry protocols: DNP3, Modbus, 61850, 60870-5, ICCP, C37.118, TCP/IP, SSH, DNS, ICMP, OPC, and HTTP.
- Automatic asset discovery and management



EPAD – End Point Anomaly Detection

End Point Anomaly Detection (EPAD) is an agentless engine that accurately detects sophisticated cyber-attacks, such as Advanced Persistent Threat (APT), without flooding the IT department with inconclusive 'gray' findings. This process begins by collecting indicators from workstations, servers and the network. EPAD then persistently mines the collected data in order to detect the presence of malicious activity, using a comprehensive set of automated analysis processes. Afterwards, to minimize the number of ambiguous cases, analysts at the Security Operation Center (SOC) investigate suspicious activities and items.

DDoS protection

This is a real-time, behavioral-based attack mitigation device that protects the organization infrastructure, preventing network and application downtime, application vulnerability exploitation, malware spread, network anomalies, information theft, and other emerging cyber attacks. It constitutes a world-class security solution including Distributed Denial of Service (DDoS) mitigation and SSL-based protection to fully protect applications and networks against known and emerging network security threats. These include denial of service attacks, DDoS attacks, internet pipe saturation, attacks on login pages, attacks behind CDNs, and SSL-based flood attacks. Our DDoS protection scheme comprises:

- Dedicated hardware that protects without affecting legitimate traffic
- A comprehensive set of security modules
- Accuracy of inline or out-of-path (OOP) deployment
- Centralized attack management, monitoring, and reporting

Network anomaly detection

This breach detection and remediation solution comprises one or more network appliances (physical and/or virtual), together with software modules. They connect passively to the primary network switches of your internal network and find compromised endpoints and stolen credentials proactively, and proceed to flag and remediate them. The solution works in a three-step iterative process to identify and mitigate attacks, as follows:

- **Detect** - The appliance passively monitors traffic in the enterprise network and profiles the behavior of each user/endpoint in the network. Without requiring any configuration or signatures, it detects subtle behavior deviations of users and endpoints, based on behavior and peer history within the organization.
- **Illuminate** - An agentless endpoint analysis module further investigates traffic anomalies, automatically scans suspected endpoints, and collects host-level indicators to identify the origin of suspicious activities. This unique combination of network-centric detection and endpoint analysis, augmented by cloud-based threat intelligence, provides your security team with actionable incidents with an extremely low false positive rate.
- **Remediate** (with detailed alerts and reports) - The actionable information generated for each breached endpoint enables efficient triage and remediation. The solution purposely keeps the number of alarms (and false positives) to a low manageable number, so that breaches can be mitigated efficiently and quickly by IT security practitioners. This can be executed early in the attack life cycle, before any real damage can be achieved.

Big data and machine-learning cyber analytics

By making sense of terabytes of current and historical data without any predefined rules or heuristics, this solution provides a cyber-analyst toolbox that includes:

- Sophisticated and generic machine-learning algorithms, able to discover patterns and covert adversary activity from within terabytes of security logs.
- Canned visualized dashboard and reports, including investigation queries that provide security analysts with fast results, while allowing them to leverage their specific expertise and the current security measures of the enterprise. Complements our NFV solution.

Management system

Security challenges in today's organization environment are diverse. Threats to critical systems exist in both IT and OT (Operations Technology) environments, on all protocol levels. The sheer amount of notifications, systems and alarms, causes false positives and increases the chance of a successful breach or attack.

ECI's LightSEC-V™ solution addresses these challenges by displaying all critical information on a single dashboard, enabling security managers to clearly pinpoint the sources of attack. The LightSEC-V's unified dashboard presents a clear picture of all detected security threats throughout the entire network, including production and operations networks. The result – dependable prevention of attacks and breaches sometimes even before they cause down-time or damage. **LightSEC–V provides:**

LightSEC-V: Real-time management for real-time security

LightSEC-V, a member of the LightSEC family of products, is an intelligent, multi-vendor, multi-service, web-based system for the management and visualization of cyber security events. It provides 'at-a-glance' aggregated views of calculated threats from many security systems, such as: big data cyber analytics (BDCA), front-end perimeter protection, SCADA, Endpoint and Network anomaly detection, advanced breach detection, Layer 1/2/3 Encryption, DDoS protection, advanced DPI, unidirectional gateway, firewall, SCADA firewall, advanced GRC (compliance), and session recording.

LightSEC-V: Key advantages and features

- Unified Dashboard - The dashboard gathers the relevant data, events and incidents on a single integrated display. It offers the following benefits:
  - Provides a one-stop shop for cyber security alerts by gathering data from multiple systems including network and security systems and from all layers
  - Shows the 'big picture' by presenting an updated cyber status of your environment
  - Delivers centralized real time cyber reports and notifications
  - Offers visibility from any device, including mobile phones and tablets
- Aggregated Events - from multiple security subsystems and cyber engines, are analyzed and graded into significant main alerts:
  - Allows drill-down and simple navigation to discover and pinpoint root causes
  - Supplies automatic learning engine with no need for signature updates or pre-defined heuristics
  - Provides a smooth flow of information between main and sub-systems (in GUI dashboard)
- Calculated threats are presented in a user friendly manner
- Centralized, real time view of the cyber security status of the IT combined with the operations network
- Future-proof growth flexibility (adding/removing third-party widgets and aggregated components)

Specifications

HARDWARE

Equipment Options	• Standalone appliance • x86 NFV card hosted on a Transport Slot (TS) on the NPT 1020/1021/1050/1200/1800 (future) chassis
CPU	• Intel® Xeon® E3-1105Cv2 • 4 Cores • 8 Threads
RAM	• 16 GB (2 x 8GB) on Dual-Channel, DDR3 • Clock: 1600MHz on Single DIMM per Channel
Storage	• BIOS: 8MB • Configuration/LOG Memory: 32 GB SSD
Interfaces	• Appliance: 8 x 1Gbps SFP • Card: 4 x 1Gbps SFP • Traffic • Debug Terminal/COM: Serial COM • Debug/Configuration USB
Size	• Appliance: 1U • Card: 1 NPT Transport Slot (TS)

ENVIRONMENTAL

Operating Temperature	0°C ÷ +50°C
Humidity	5% to 95%

MANAGEMENT

Cyber Management System	LightSEC
Network Management System	LightSoft

POWER

Appliance	• -48 V DC • 220V AC
Card	• -48 V DC from backplane • 40W Max per slot

*Specifications subject to change without notice

Contact us to discover how ECI's holistic LightSEC solution can secure your business

ABOUT ECI

ECI is a global provider of ELASTIC network solutions to CSPs, utilities as well as data center operators. Along with its long-standing, industry-proven packet-optical transport, ECI offers a variety of SDN/NFV applications, end-to-end network management, a comprehensive cyber security solution, and a range of professional services. ECI's ELASTIC solutions ensure open, future-proof, and secure communications. With ECI, customers have the luxury of choosing a network that can be tailor-made to their needs today – while being flexible enough to evolve with the changing needs of tomorrow. For more information, visit us at www.ecitele.com