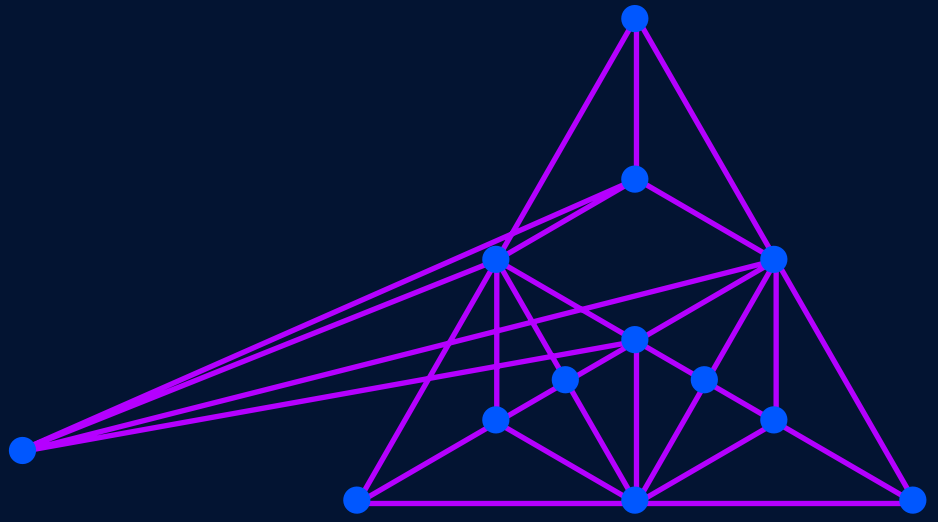
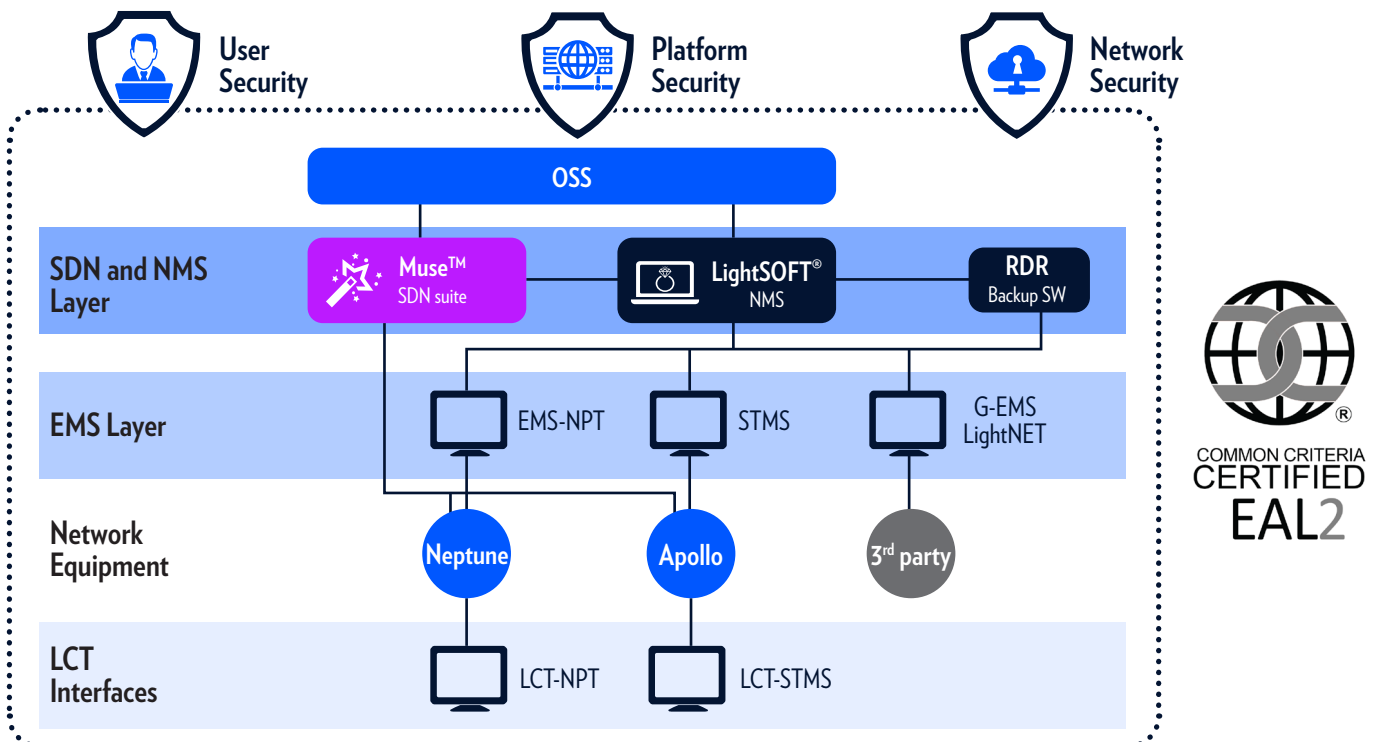


PORTFOLIO SECURITY



TOTAL PROTECTION FROM THE NETWORK UP

Packet and optical networks are configurable today with a few button clicks. Without proper protection, it can be just as easy to misconfigure or bring the network down, whether inadvertently or maliciously. To ensure that this does not occur, ECI provides multiple layers of comprehensive security throughout its product portfolio, from network and element management systems to the network equipment itself. Role based-access control (RBAC) extends to operations personnel as well as end-customers using CNM portals. Transport Layer Security (TLS) secures all intersystem links and the underlying operating systems are hardened. In addition, ECI networking products offer advanced security features, like encryption or network slicing, which the operator can use for internal purposes or offer to end-customers as a service.



ECI PRODUCT PORTFOLIO SECURITY APPROACH

Neptune packet networking and Apollo optical networking product families reside at the core of ECI's portfolio. LightSOFT® NMS manages both families end-to-end via their respective EMS. Muse delivers advanced SDN capabilities, like 5G network slicing control.

User and platform security protects against erroneous or malicious use of networking or management capabilities. At the same time, Neptune and Apollo deliver their own value-added networking security features. This brochure highlights major aspects of this comprehensive approach.



USER SECURITY

User security ensures that only authorized operations users can access ECI's management and control systems and regulates their capabilities. Notable features include:

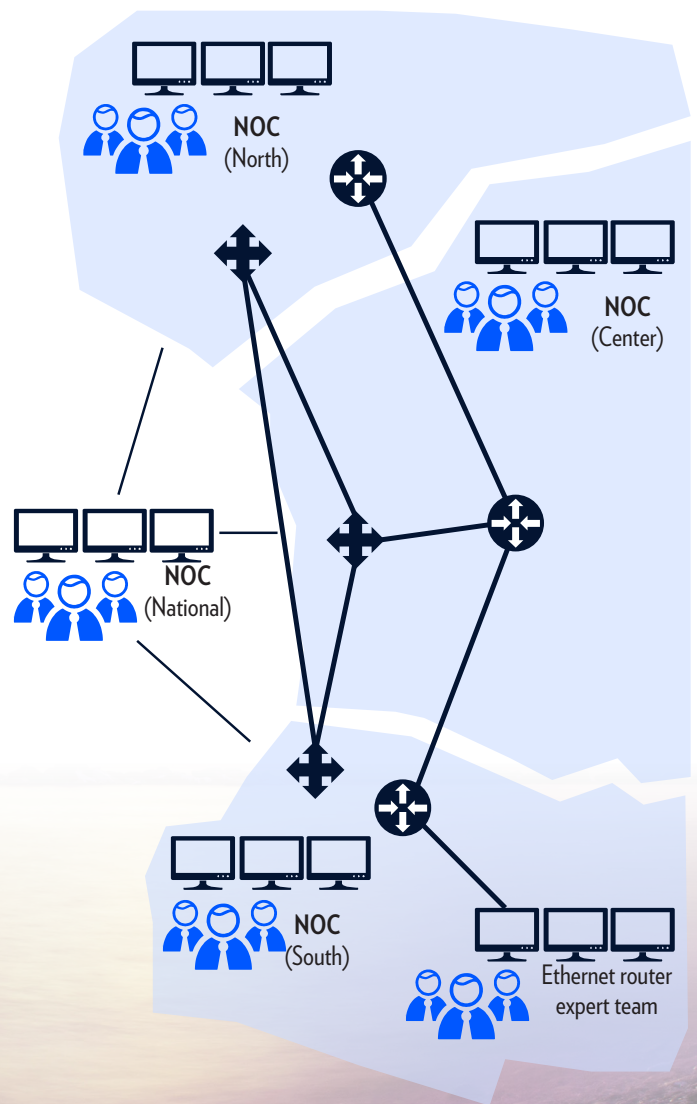
Authorization and authentication – Centrally-administered RADIUS or LDAP based applications safeguard user access.

Two-factor authentication option – A combination of password knowledge and physical possession of a smart card significantly increases access security.

User profile management – Role-based access control (RBAC) manages the span of network domains that users can access and the range of functional control capabilities that they can exercise within those domains. Customizable prebuilt profiles for major operational categories, such as configuration, provisioning, and maintenance facilitate the creation and management of profiles for individual users or user groups.

Enhanced security – Additional controls provide added security, beyond access authorization and profiles. These include items, such as login attempt monitoring and lockouts, activity filtering, activity monitoring and logging, and file and mail restrictions.

Customer network management – Application of all the above controls to end-customers enables them to manage their transport services or subnetworks through a CNM portal. Customers gain the satisfaction of controlling their domains directly, while the network operator has the assurance that this control is isolated from interfering with other resources.





PLATFORM SECURITY

Platform security operates at a system level that is independent of users. It hardens communication links and underlying operation systems against improper use or hacking and ensures data integrity. Notable features include:

Secure communication links – Transport Layer Security (TLS) cryptographic protocols protect all intersystem links in the ECI transport ecosystem, ensuring privacy between the communicating entities. This includes links among Muse, LightSOFT, networking equipment, and remote databases. Additional capabilities are IP port blocking and special authorizations for remote sessions.

Hardened operating systems – All OSs of Muse, LightSOFT, and Neptune and Apollo EMSs have been hardened to protect against misuse through a range of methods. These include disabling unnecessary system services, added levels of user authorizations, and special measures like firewalls, IP Tunneling, VPNs, RAS, and NAT.

Database security – Access to management and control databases is secured, locally and remotely, via credentials that restrict access to specified application and operating system domains. For added security, aliasing is available, which hides database connection string details from data-source definitions.

Geographic redundancy – Remote Database Replication (RDR), a field-proven flexible redundancy mechanism, provides full network management backup capabilities for disaster recovery. It is configurable for a wide variety of topologies for different geographic infrastructure distribution, security needs, and available budgets for standby mirror hardware.

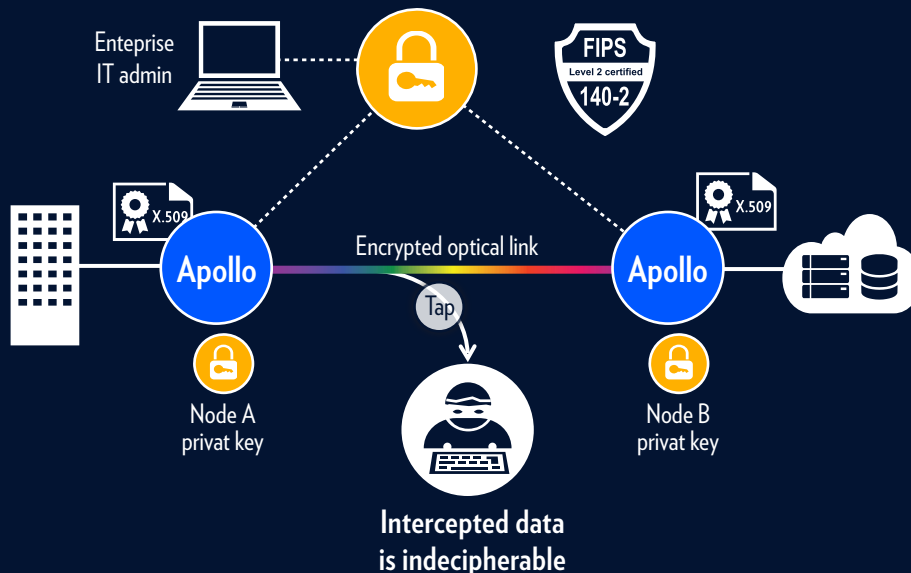
Development security – ECI employs a secure Software Development Life Cycle process. This includes automatic static security code analysis on all ECI and 3rd-party software. It also analyzes and manages possible security vulnerabilities of open-source components.



NETWORKING SECURITY

ECI's networking products offer advanced security features that network operators can use for internal purposes or provide to end-customers as a service.

Layer 1 Optical Encryption (L1OE) – The only way to protect against fiber tapping is by encrypting the optical bit stream. Apollo L1OE can be applied selectively at a per-service level, or to an entire wavelength, without adding any delay to the bit stream. Apollo can also extend key administration to Enterprise IT to apply to their optical services or links without telco involvement.

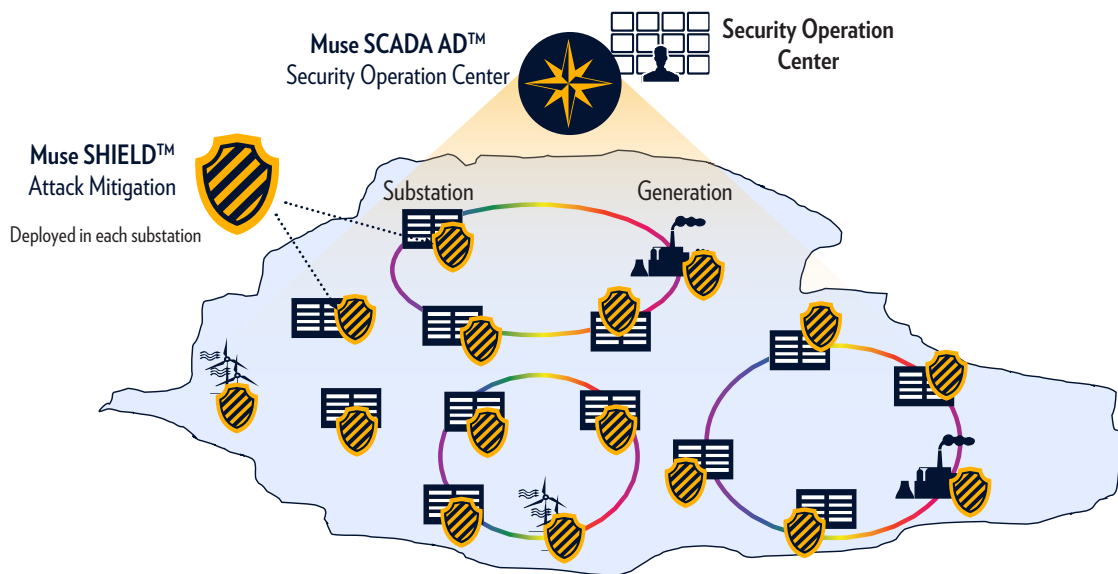


Packet Networking Security – Neptune provides multiple mechanisms to protect the integrity of the packet network and the contents of the packets themselves:

- **Access Control Lists (ACL)** protect routers by specifying permissions, such as a list of restricted IP addresses from which the user can access a specific device, or a list of IP addresses that the user is allowed to access within the network.
- **Layer 2 MACsec encryption** provides data origin authentication, data confidentiality, and data integrity for secure transport of media access control services among business locations over the public WAN.
- **VPN security** protects users from attacks or loss of data privacy through comprehensive filtering and segregation. The contents of packets classified to a specific VPN are not visible to other VPNs, providing sniffing or snooping protection.
- **Port-based Network Access Control (PNAC)** authenticates devices, wishing to attach to a LAN or WLAN.
- **Broadcast Storm Control** halts extremely heavy levels of incoming broadcast traffic, typically encountered under DoS attacks, giving network operators an opportunity to pinpoint and resolve the source of the problem.
- **Dynamic ARP inspection** protects against Address Resolution Protocol (ARP) spoofing and certain man-in-the-middle attacks, by intercepting and discarding ARP packets with invalid IP-to-MAC address bindings.

Security Isolation through Network Slicing – Muse manages hard and soft slicing technologies within Neptune and Apollo, including FlexE, VPNs, dedicated queues, and ODUflex. These are used to create virtual subnetworks dedicated to customer segments or service classes with a high degree of isolation from intrusion and other network traffic. Network slicing is particularly important to support performance guarantees for the different 5G service types, such as ultra-reliable low-latency communications.

Virtualized Operations Technology (OT) Security – Muse manages a suite of security VNFs that deliver operational technology security, such as SCADA anomaly detection, for utilities and other critical infrastructure enterprises. The VNFs run on both Neptune plug-in and standalone COTS NFVi.



ECI's approach to total protection of its product portfolio provides network operators with peace of mind that their networks are protected against inadvertent user errors and malicious attacks.

Contact us to find out how our ELASTIC networks can help your business grow

ABOUT ECI



ECI is a global provider of ELASTIC network solutions to CSPs, critical industries, and data center operators. With the advent of 5G, IoT, and smart everything, traffic demands are increasing dramatically, and network operators must make smart choices as they evolve their infrastructure. ECI's Elastic Services Platform leverages our programmable packet and optical networking solutions, along with our service-driven software suite and virtualization capabilities, to provide a robust yet flexible solution for any application. ECI solutions are tailored for the needs of today, yet flexible enough to meet the challenges of tomorrow. For more information, visit us at www.ecitele.com