ECI THE ELASTIC NETWORK

SECURE DATA COMMUNICATION NETWORK

MULTI-TIER PROTECTION AGAINST MULTI-DIMENSIONAL THREATS

Your data communication network (DCN) is vital to your enterprise, carrying the information that powers your business applications and services to end-customers. You must secure the network as well as the applications and data it supports against a wide range of threats, aimed at intrusion, disruption, and theft – originating from both external and internal sources. Moreover, you must accomplish this while maintaining network ease-of-use.

ECI tackles this multi-dimensional challenge with a powerful and modular suite of security tools. These are applied using two main principles, segmenting the problem space into manageable geographic domains and threat classes, and linking local security instantiations with a global view. When combined with a complete lifecycle approach that covers planning, implementation, and ongoing support, ECI is able to create a unique and comprehensive DCN security solution tailored your enterprise's needs.

Powerful modular security suite

Segmentation into virtual domains

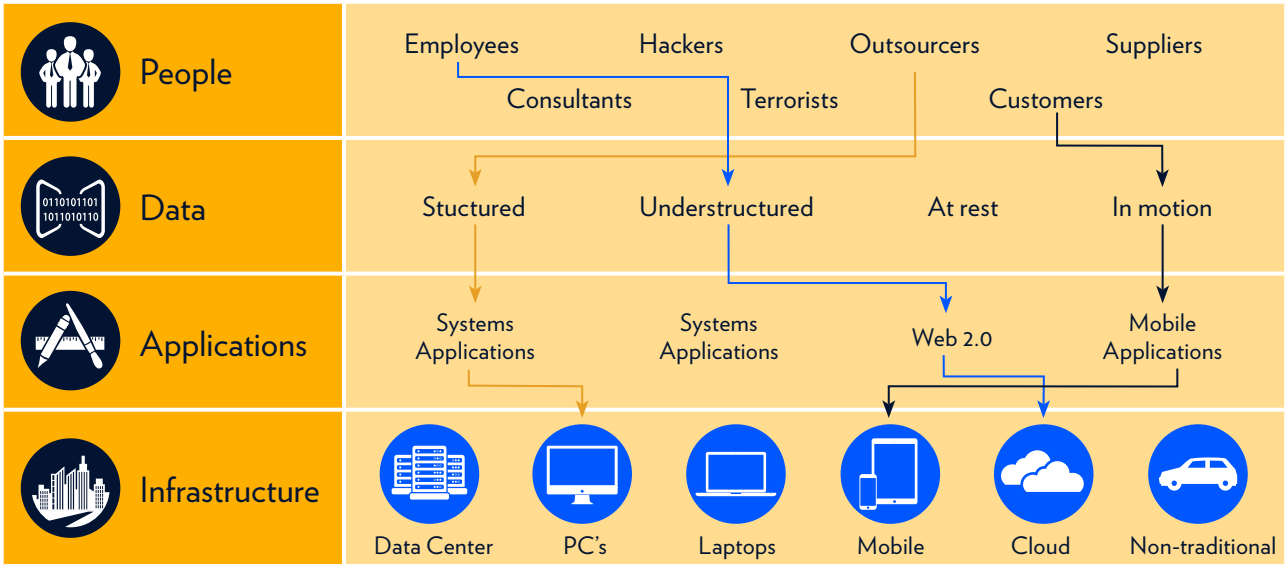
Linked local plus global security

Customization and lifecycle services

MULTI-DIMENSIONAL THREATS

The complexity of modern data communications networks produces multiple vulnerabilities. These leave DCNs open to sources of attacks that can be woven together in different ways encompassing people, data, applications, and physical devices. There are three typical categories of attack to defend against:

- Black – Outside agent attack from outside the DCN
- Gray – Outside agent from within the DCN
- Red – Inside agent attack from within the DCN



REQUIRES A MULTI-DIMENSIONAL SOLUTION

This multidimensional complexity creates a need for a comprehensive and segmented security approach, which provides multilayer protection and can intercept threats at various points in the attack chain.

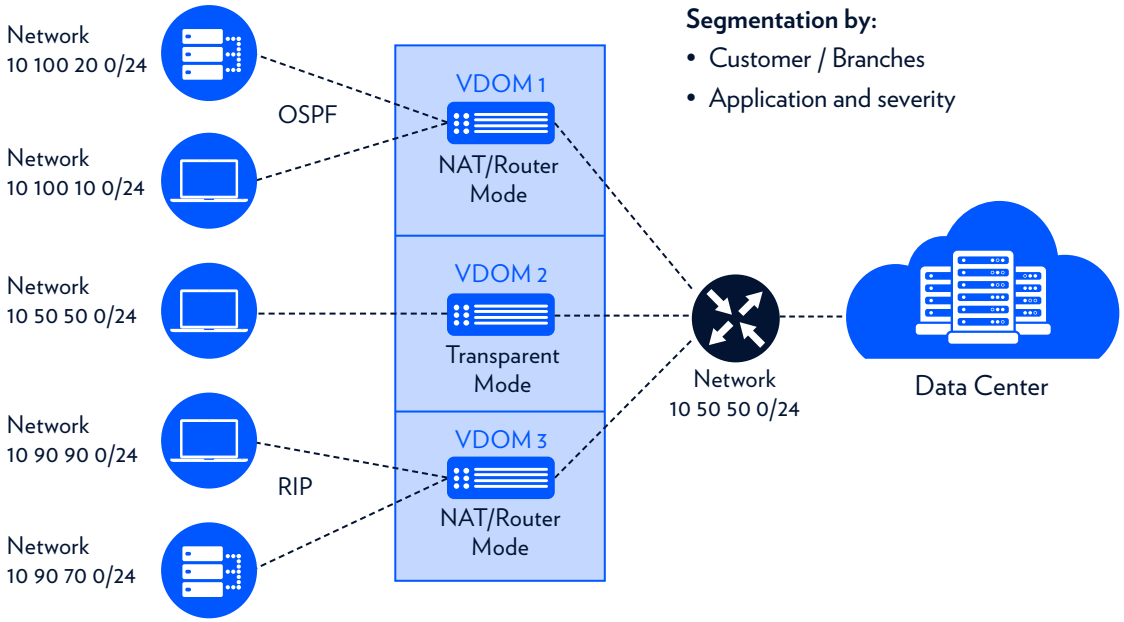
ECI's security solution starts with a multidimensional toolset, covering three broad categories:

- Multilayer encryption to protect the data in transit from interception, including L1 optical encryption, L2 MACsec, and L3 IPsec.
- Universal threat management (UTM) tools that mitigate attacks at both the data and application layers.
- Analysis, forensics and management tools to detect threat and attack patterns early on, so that proactive steps can be taken before a serious attack is launched.

DIVIDE AND CONQUER – SEGMENTATION INTO VIRTUAL DOMAINS

ECI's approach starts with breaking up the DCN into virtual domains (VDOMs). A VDOM can cover physical entities like branch offices or sets of customers, or be applied to abstract entities like types of applications, or classes of threats. The suite of cyber security tools can then be applied per VDOM in a variety of ways, for example:

- To separate duties and enforce security policies that preserve network access to specific users/resources
- To monitor activity per user, application, circuit - providing the system administrator with full network and application visibility per segment and per user
- To enforce advanced security mechanisms beyond firewall on specific network segments (IPS, AV, APP CONTROL, VOICE SECURITY, etc.)



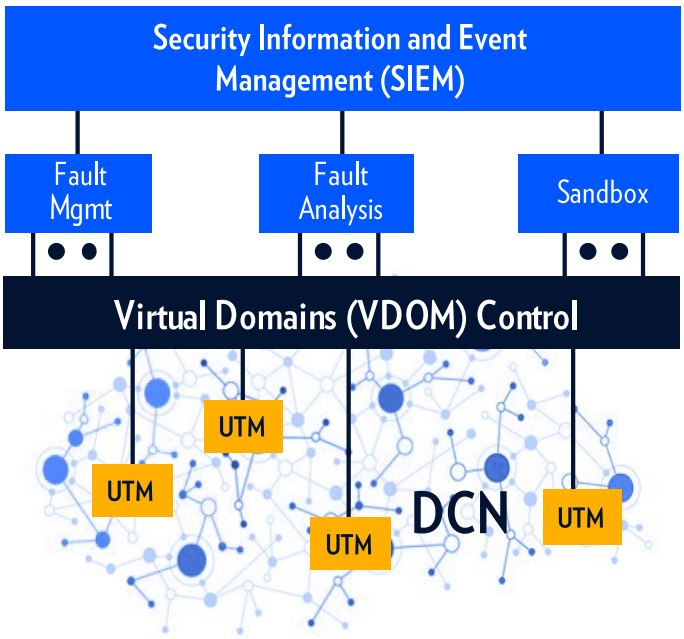
Each VDOM can implement its own application aware firewall with its own enforcement rules.

The benefits of this approach is manageability, allowing a security administrator to allocate the appropriate resources as needed, and have an ability telescope in and out when analyzing problems. It also supports regulatory compliance that often demands segmenting a network and providing different levels of security based on the underlying organizational mission set.

MICRO MACRO WORKING TOGETHER – LOCAL SECURITY WITH A GLOBAL VIEW

The second half of ECI's approach is to combine local security with a global view. ECI unifies and deploys cyber at the communications point-of-access to Enterprise facilities to mitigate attacks before they can cause harm. This is combined with a centralized system that eliminates the guesswork in identifying cyber security threats. It collects, validates, correlates, and analyzes information from point-of-attack applications and sensors, and presents threat insights in a visually intuitive and actionable manner, providing forensics in real time. Based on the centralized view, the policies of the local attack mitigation systems are also adjusted.

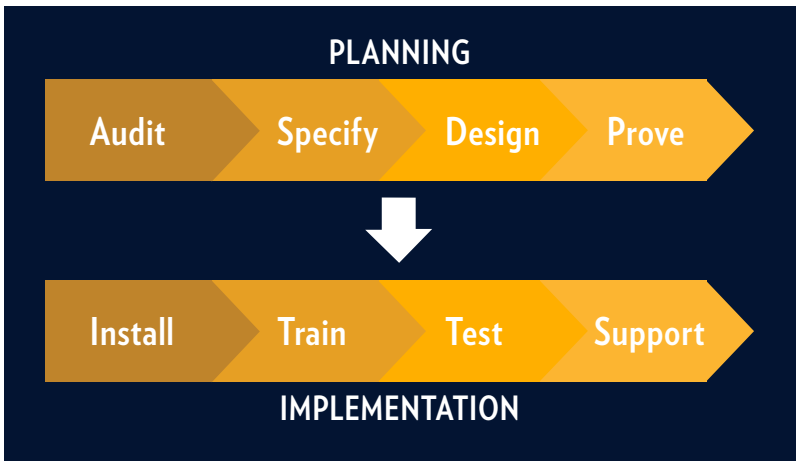
Finally, because cyber threats are continually changing requiring, ECI's solution includes a sandbox capability to test out new tools and approaches before applying them live in your network.



CUSTOMIZATION AND LIFECYCLE SERVICES

Just as important as the DCN security technologies, is the process by how the solution crafted and implemented. ECI provides complete lifecycle services through the planning and implementation phases, and ongoing support for the operational system.

ECI provides a DCN security solution that is tailored to the unique needs of your enterprise.



Contact us to find out how ECI can secure your Enterprise DCN

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