

Secure Networks

Leveraging the Network Infrastructure as an Integration Point for Security Intelligence and Capability

How Can Secure Networks Benefit Your Business?

- Minimizes exposure to internal and external threats: theft, business disruption, negative publicity
- Integrates security pervasively; it's not bolted on
- Ensures cost-effective acquisition and operation for a lower TCO
- Integrates with existing IT infrastructure

How Can Secure Networks Benefit Your IT Organization?

- Provides central control and enforcement of enterprise security policy
- Automates prevention, detection, response
- Minimizes false positives
- Centralizes management for faster reaction times
- Offers distributed enforcement and granular control, deployed globally
- Scales easily to accommodate a dynamic network environment

A New View of Network Security

In today's world there are more threats to your IT infrastructure and systems than ever before. At Enterasys, we understand that the security of your enterprise network is directly tied to the success of your business.

To protect the assets of the business properly, security can't be an afterthought; it must be holistically integrated into the entire network infrastructure. You must adopt an end-to-end approach that anticipates risks before they occur, using pervasive mechanisms that automatically keep up with changing conditions. Such networks can actually enable the business to grow and change dynamically. Instead of "network security," IT can provide true Secure Networks.

We define Secure Networks as an approach that leverages the network infrastructure as an integration point for all security intelligence and capability. The network has the unique opportunity to be this unifying factor because of its pervasive presence, its ability to provide control over individual devices and people, and its inherent independence and immunity from corruption at the computing and application layers of the IT system.

Secure Networks Solutions

Some of the solutions that help deliver a Secure Network include:

Dynamic Intrusion Response Solution.

Secure Networks' Dynamic Intrusion Response Solution proactively detects abnormal behavior on the enterprise network and intervenes to quarantine the offending user or deviant device. Dynamic Intrusion Response isolates and categorizes each security vulnerability, identifies the source of that vulnerability and automatically reconfigures the network to eliminate the potential threat.

Secure Open Convergence Solution.

Secure Networks' Secure Open Convergence Solution provides the foundation for successfully building a standards-based converged network environment to support IP telephony, Storage-over-IP and other critical applications.

Acceptable Use Policy Solution.

Secure Networks' Acceptable Use Policy Solution is a unique, policy-based system that allows the network to provision required business services to users automatically while preventing undesirable and malicious traffic from entering the infrastructure.



Secure Application Provisioning Solution. Secure Networks' Secure Application Provisioning Solution applies Quality of Service to applications and services based on an organization's business rules and policies—and on the business role of the user accessing the application or service—to ensure improved business processes and enhanced security.

Secure Data Center Solution. Secure Networks' Secure Data Center Solution is a unique policy-based solution that allows for the administration of specific security and Quality of Service policies associated with data center assets and applications.

Secure Guest Access Solution. Secure Networks' Secure Guest Access Solution enables an organization to offer guest access thanks to a fundamental process of recognition through which the network “sees” whether the user connecting to the network infrastructure is an employee, or other “trusted user,” or a visitor, and then assigns access accordingly.

Single Sign-On Solution. Secure Networks' Single Sign-On Solution enables users to access different systems—including the operating system, network and individual applications—with one password, for a system that is less complicated to administer and less cumbersome to use.

What Sets Enterasys Secure Networks Apart?

- Embedded security from the core to the edge delivers superior threat mitigation with increased operational efficiency
- Reduces operating expenses and capital expenditures
- Begins with a holistic view of security, while security appliance vendors focus on compliance, privacy, or business
- Defines security policy at the network core, then enforces detection and response at the network edge; a secure edge is the best defense against DDOS attacks
- Scales to address the vulnerabilities posed by new network access technologies
- Offers consistent management interfaces, simpler deployments, and reduced dependence on scarce security resources

To Learn More

To find out how Enterasys' Secure Networks can help you respond to evolving threats, increase operational efficiency, and reduce deployment complexity, call your Enterasys sales representative or an authorized Enterasys partner, or visit the web at **enterasys.com**