

Secure Networks™: Trusted End-System Solution

Trusted End-System Solution Benefits

- **Uniquely provides protection** against vulnerable end systems at every LAN interface
- **Mitigates risk associated with new users or devices** attaching to the network by automatically quarantining “non-trusted” end systems
- **Improves network availability and overall productivity** by quickly isolating vulnerable end systems before they affect other users
- **Provides centralized management** to consistently enforce security policies, optimize IT resources and quickly configure new users or devices
- **Automated, system-level control lowers cost** of administration, implementation and troubleshooting
- **Integrates with leading endpoint security applications** to further strengthen network security and protect investments

Protecting the Infrastructure from Vulnerable End Systems

IT administrators know that many workstations and other networked devices connect to the corporate infrastructure without the latest security updates. These end systems are vulnerable to malicious attacks that could compromise critical resources, leading to business disruption and revenue impairment. Enterasys’ Trusted End-System (TES) solution uniquely addresses this challenge, enhancing your organization’s overall security posture to maximize network availability and business productivity.

The Trusted End-System solution allows you to deploy cost-effective end-system admission control for every LAN-connected user. TES is part of the family of Secure Networks solutions that integrate advanced security and management features to centralize and automate granular control of the entire network infrastructure.

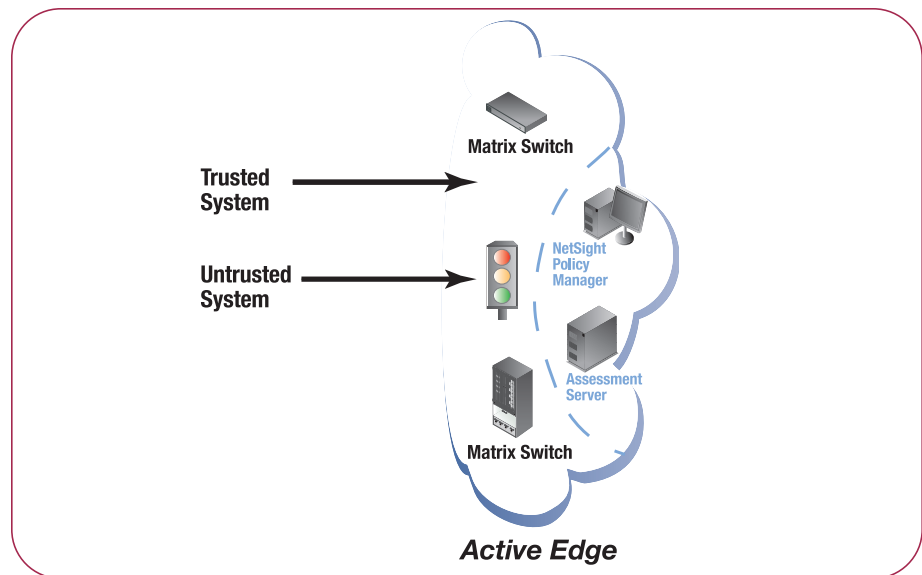
With a Trusted End-System solution, you can not only minimize the disruption caused by vulnerable network devices but ensure seamless access for trusted users with up-to-date security profiles. It also provides effective protection against more sophisticated network threats by automatically quarantining suspect devices, greatly simplifying the deployment of security updates. There is no requirement for user interaction with this process. TES leverages the power of centralized, policy-based management, so it is easy to deploy and administer.

The Foundation of a Trusted End System

The Trusted End-System solution ensures that only devices with correct and up-to-date security credentials are granted access to the corporate IT infrastructure. TES determines the security level of each networked device as it attempts to connect by examining parameters such as security application configuration, operating system patch level and anti-virus signature revision. End systems that fail this verification may be vulnerable or already compromised, so they are quarantined until the necessary corrective actions have been taken. The TES solution is centrally configured and controlled for consistent enforcement of security policies, optimization of IT resources and scalability to quickly add new users or devices as needed.

Enterasys has developed two complementary approaches to the Trusted End-System solution to meet the needs of all types or sizes of enterprises. The **Agent-Based Trusted End System** is designed for interoperability with leading-edge endpoint security applications from Zone Labs and Sygate. Zone Labs “Integrity” and Sygate “Secure Enterprise” security software products have been certified by Enterasys Networks Security Response Team for interoperability within a Secure Networks infrastructure.





Security policy rules and profiles are defined and distributed using the NetSight™ Atlas Policy Manager application. When a user or device attempts to connect to the network, the end system is assessed via the Zone Labs or Sygate security agent. The results of this evaluation are forwarded to an Assessment Server and Authentication Server to determine the level of trust. If the results of both authentication and security assessments are positive, the Matrix™ switch will permit network access in conformance with security policies. If the results of the security assessment are negative, the user or device is assigned a Quarantine Role until the corrective actions have been taken.

The **Network-Based Trusted End-System** solution complements the agent-based approach. It does not require a security agent to reside on each connecting device, making it particularly useful for organizations such as universities that often cannot control the number or type of end systems accessing the network. Once again, NetSight Atlas Policy Manager defines the end-system security requirements. When a user or device first attempts to connect to the network, its credentials are passed to an Authentication Server while the end system is scanned using vulnerability assessment and operating system patch assessment tools. This process is used to determine if that device meets the requirements for a trusted end system.

What Sets Enterasys' Trusted End System Solution Apart

The Trusted End-System solution minimizes the disruption caused by networked devices with incorrect or out-of-date security configurations. It effectively protects the network from vulnerable end-user driven workstations, laptops and PDAs, as well as automated, self-running end systems such as surveillance cameras and IP phones that can introduce security threats to the infrastructure. TES protection is seamless and transparent for trusted business users.

Importantly, the Trusted End-System solution is designed to enhance already installed Secure Networks solutions, and can be deployed with a relatively cost-effective upgrade. A range of associated professional services are also available to assist with the rapid configuration and optimization of the TES solution.

Like all Enterasys Secure Networks solutions, the Trusted End-System solution was developed using open standards to interoperate in multi-vendor environments for simplified deployment, inherent scalability and greater overall investment protection.

To Learn More

Learn how Enterasys' Secure Networks solutions 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 enterasys.com/secure-networks.

Matrix, NetSight and RoamAbout are trademarks or registered trademarks of Enterasys Networks. All other products or services mentioned are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.

All contents are copyright © 2004 Enterasys Networks, Inc. All rights reserved.

Lit. #9013712 7/04