

Secure Networks™: Peer-to-Peer Security Solution

Peer-to-Peer – Managing the Risk

Today's colleges and universities must deal with the constant struggle of providing an open, collaborative learning environment while protecting students, faculty, administration, guests and IT systems from a growing number of risks. The network communication technologies that have accelerated collaboration and learning are also used in the illegal distribution of copyright-protected content. To face these challenges, higher learning institutions must apply technologies that enforce the institution's policies regarding the use of the network and distribution of content across that network. The technology chosen must also function to predict, prevent and automatically respond to other threats to the university such as worms, viruses and spyware.

Enterasys Networks can secure any network from any vendor. Secure Networks, an architecture from Enterasys, provides key technologies that solve not only the peer-to-peer file swapping legal liability issues, but can also be leveraged to solve other security challenges at the institution. Enterasys delivers Secure Networks to ensure the integrity and performance of IT services and the higher education users that rely on them. Enterasys embeds security technologies directly into the network fabric itself to respond to threats proactively, increase operational efficiency, reduce deployment complexity, and scale as the network expands over time. Security is no longer just bolted on, but pervasively integrated throughout the wired and wireless infrastructure.

Dynamic Response is a solution derived from the Secure Networks architecture. Dynamic Response leverages the architectural elements "Detection," "Location," "Access Control" and "Respond & Remediate." In the event of unauthorized peer-to-peer traffic occurring on the network, Dynamic Response isolates and

categorizes each security incident, identifies the source and automatically reconfigures the network to mitigate the threat. Using Dynamic Response, the campus network can be protected against content-sharing violations and other front-of-mind security risks such as spyware and rapidly spreading worms and viruses.

In deploying a Dynamic Response solution, the institution reduces the exposure of its educational and administrative resources to internal and external threats by opportunistic hackers/predators seeking to disrupt daily operations, host illegal/inappropriate content or steal personal information. Dynamic Response is an embedded security architecture that proactively addresses security exposures and complements already deployed security appliances without major reconfigurations or disruption to the network or user community.

Secure Networks Benefits

- Reduces complexity and risk by embedding active, automated security into the network fabric
- Maps acceptable use policy to network implementation
- Improves visibility into the network as a single entity for faster trouble resolution
- Provides secure/reliable access to internal and external users based on their roles within the organization
- Delivers automation and system-level control to lower the cost of administration, implementation and troubleshooting
- Enables application growth and expansion
- Increases productivity through improved access to data/applications

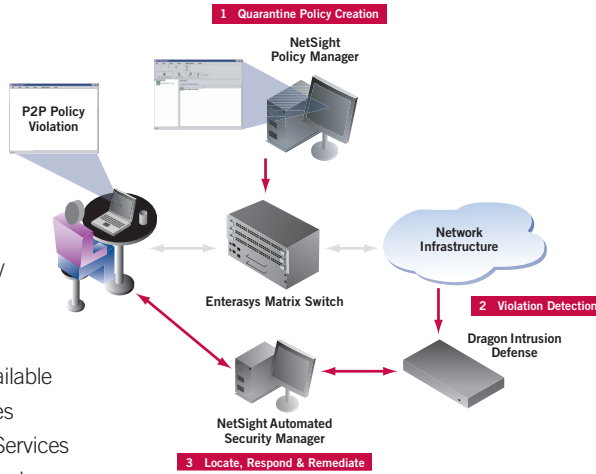
Major U.S. University Case Study

- Offers students an alternative to illegal file sharing via a licensed service
- Implemented Dynamic Response solution for control of peer-to-peer traffic
- Violators are warned via Web interception of event
- Violations are tracked—a third violation disables access pending administrative review

**There is nothing more important
than our customers.**

The Foundation of Dynamic Response

The network or security administrator creates customized policies that determine the network's response to each type of security event. Enterasys' NetSight® Policy Manager is used to classify both network users/groups and available infrastructure services, and defines the rules that determine how services are made available to each user/group. Enterasys provides default configurations, but all Rules, Services and Roles are fully customizable through a policy configuration wizard.



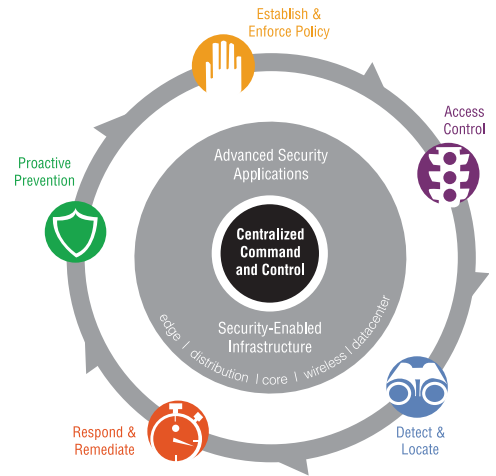
Security threats are detected by Enterasys' Dragon® Intrusion Prevention/Defense or any third-party security event detection product. Dragon diagnoses and categorizes each security incident, and reports them to the Enterasys NetSight Automated Security Manager. Using sophisticated algorithms and intelligent network mapping, NetSight Automated Security Manager determines the precise network location of the non-compliant user or device, and initiates the predefined action to fix the problem. This demonstrates the power and unique capabilities of the Dynamic Response solution. By implementing an automated configuration change, the non-compliant user or device is removed from the network, quarantined, or otherwise controlled. This capability extends across multiple vendors and multiple network technologies.

Privacy Concerns

Many higher education institutions struggle with balancing the privacy of students with the compliance requirements mandated by law. The Enterasys solution can be configured to monitor protocols, applications, content or all three. One institution may consider the use of a peer-to-peer protocol a violation of policy, while another may allow the protocol but inspect the content. The monitoring and detection options are flexible to meet the established acceptable use policies of each institution. Additionally, the Enterasys Dynamic Response solution may be configured to log and report on as much or as little of the data, person or location of the event as the institution requires as part of its compliance auditing efforts. Enterasys delivers a flexible and open architecture to automatically sense and respond to network security threats.

What Sets Enterasys Dynamic Response Apart

Enterasys Matrix™ switches, Dragon Intrusion Prevention/Defense and NetSight network management applications have been built with the embedded Secure Networks features that enable sophisticated threat isolation and resolution. Dynamic Response is the perfect complement to the firewalling, packet inspection and patch management protections already deployed in most higher education networks. The Enterasys solution is unique in its ability to automate the critical process of locating the exact source of a detected security violation and enabling the appropriate response to be applied.



Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2006 Enterasys Networks, Inc. All rights reserved. Enterasys is a registered trademark. Secure Networks is a trademark of Enterasys Networks. All other products or services referenced herein 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.



Delivering on our promises. On-time. On-budget.