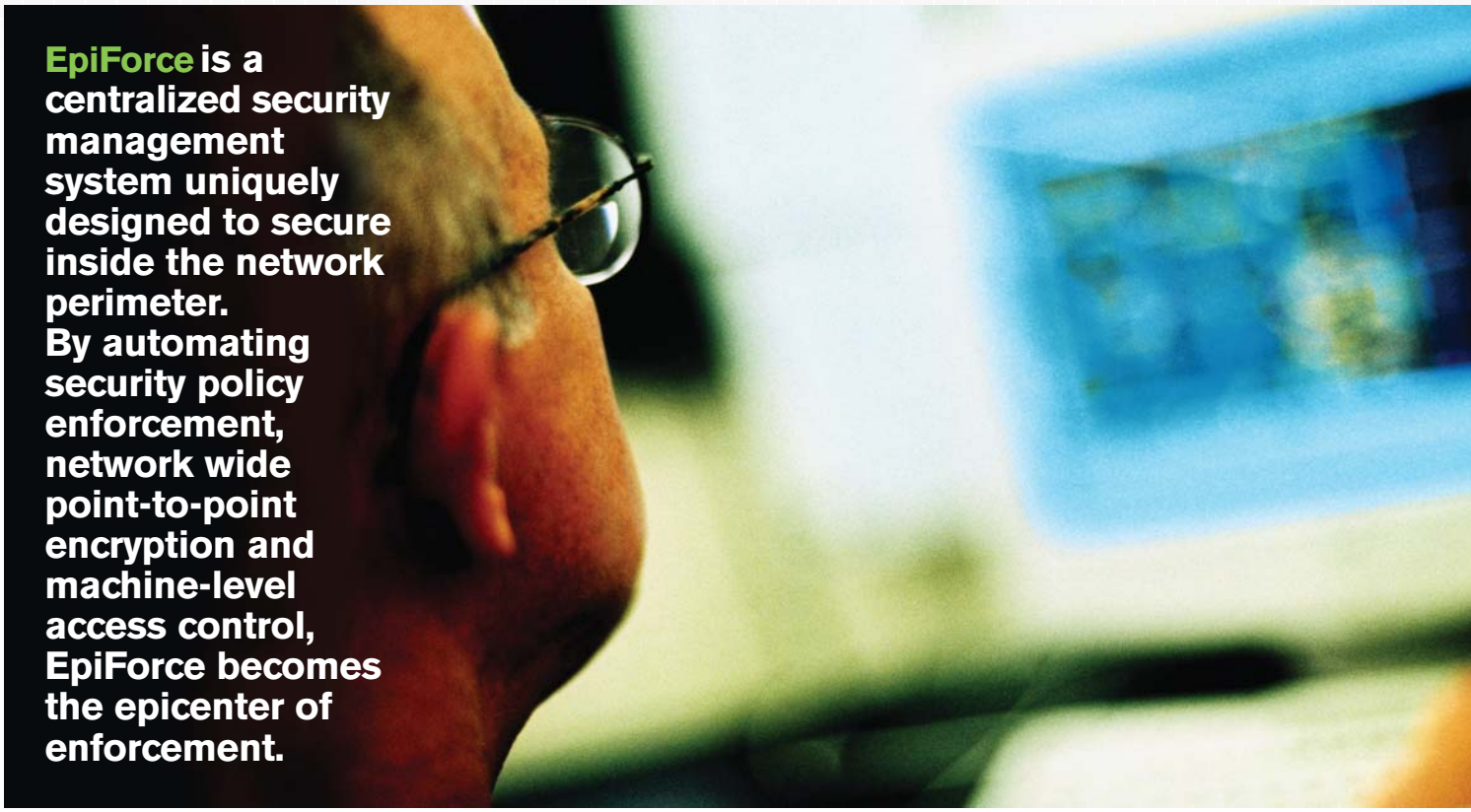
PRODUCT BROCHURE
VERSION 2.0

EpiForce

Securing Inside the Network Perimeter



EpiForce is a centralized security management system uniquely designed to secure inside the network perimeter. By automating security policy enforcement, network wide point-to-point encryption and machine-level access control, EpiForce becomes the epicenter of enforcement.

Things have changed for network managers – they must now secure inside the perimeter.

An attack can come from anywhere, at any time. There is no well defined network edge or perimeter, and it's often difficult to tell who should or should not be granted access to the network. An explosion in mobile computing and systems integration between both partners and suppliers has placed a premium on back office connectivity to anyone, from anywhere, through any device. Today's porous networks require a new approach to security.

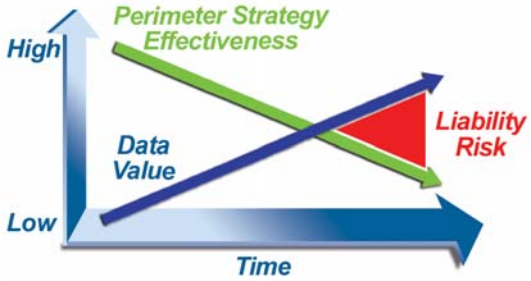
The loss of sensitive customer data is no longer just an IT headache, or a topic to be addressed privately within the confines of an IT department. Government regulations now demand immediate public notification of a security breach involving customer records, resulting in a loss of confidence from customers, investors and employees, translating into a reduction in market value.

Apani

EpiForce

THE SECURITY THREAT HAS EVOLVED

The security threat from inside the network perimeter is not new. According to CSI / FBI survey data, this vulnerability has contributed to at least half of all the network security incidents over the past 7 years. Yet, most security expenditures have been focused on the perimeter. A growing liability risk has emerged reflecting the increased likelihood of a data breach and the accompanying public disclosure, followed by customer, investor and employee loss of confidence.



IN 2005, JUST UNDER HALF THE MALICIOUS NETWORK ATTACKS WERE ORIGINATED INTERNALLY, AT AN AVERAGE LOSS PER THEFT INCIDENT OF OVER $355,000, AN INCREASE OF 111% OVER THE PRIOR YEAR.
2005 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY

THE GROWING POROUS NATURE OF TODAY'S NETWORKS

There is no question today that the perimeter is getting more porous. The network edge is difficult to identify, blurring the distinction between *inside* and *outside*.

THE 2005 AVERAGE LOSS PER UNAUTHORIZED ACCESS TO INFORMATION INCIDENT JUMPED 488% TO OVER $300,000.
2005 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY

THE INCREASED VALUE OF CUSTOMER DATA

Historically, customer data has had little value on the open market. Today the opposite is true, with records reaching as high as $100. Online auction sites, run by crime syndicates, facilitate distribution for stolen data, further acerbating the problem.

NETWORK ATTACKS HAVE BECOME MORE SOPHISTICATED

With the growing value of customer data, increased time and energy are now being expended targeting where valuable data is located.

SECURING INSIDE THE PERIMETER IS NOW ESSENTIAL – BUT HAS UNIQUE CHALLENGES

Customer and financial records' growing value coupled with the regulatory and business risks of a data breach necessitate better security surrounding these valuable assets. These records typically reside within the network perimeter. Now is the time to address this business liability.

The network inside the perimeter is a very different environment to that on the outside. It tends to be much larger scale and heterogeneous, with no convenient gateways to manage security. The applications environment is more complex and usually includes legacy applications that can not integrate security without expensive modification. This application environment frequently includes 'any-to-any' network configurations, creating significant challenges when it comes to restricting access.

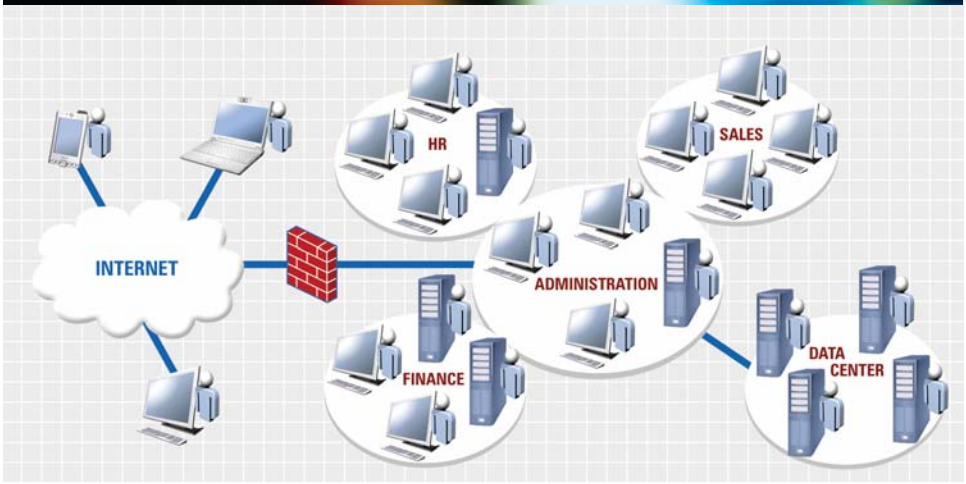
Existing perimeter-based technologies, such as firewalls and VPNs do not work well inside the perimeter as typical gateway designs cause bottlenecks, latency and bandwidth constraints. The network inside the perimeter is by design an open environment, and perimeter-based security technologies can not effectively secure it. What is needed is a new security element that works the way the network does. A horizontal security layer that is centrally managed, application agnostic and transparent to users. What is needed is EpiForce.

EpiForce creates logical security zones to allow easier, more flexible management and the creation of closed user groups.

A NEW APPROACH TO SECURING INSIDE YOUR NETWORK

EpiForce is an enterprise level application specifically designed to secure data in motion and protect data at rest within the network perimeter regardless of the application or OS platform. Operating at the network level, it will seamlessly co-exist with your existing perimeter defenses and is completely transparent to end users and applications. The agent-based software design is highly scalable for large distributed environments with automatic provisioning and real time policy updates, all controlled through a central management interface.

FLEXIBLE SECURITY ZONES



ENTERPRISE NETWORK SECURITY — FROM THE INSIDE OUT

EpiForce offers a unique combination of encryption, network segmentation and centralized policy management to secure inside the perimeter. By establishing security zones based on application access and usage policies, it is now possible to easily manage and enforce security policies to protect valuable customer and financial data.

EpiForce helps you cost effectively achieve regulatory compliance by:

- Securing data in motion and protecting data at rest across the whole network environment, regardless of scale, operating system or hardware
- Automating enforcement of security policies, providing a strong audit trail to demonstrate sensitive data is secure
- Documenting unauthorized attempts to access secured information, providing the necessary reporting to address audit and regulatory needs

A BEST PRACTICES FRAMEWORK

EpiForce addresses four critical components necessary to build a next generation network security framework. First, ensure each device connecting to your network is automatically identified and authenticated. Next, only grant access to authorized network devices. Third, logically segment your network into security zones to provide defense in depth to mitigate the impact of potential attack. Finally, ensure your monitoring capabilities can detect developing threats and provide the necessary reporting. EpiForce addresses each of these best practices through a single, software-based installation that is sufficiently scalable to support enterprise-class networks.

Apani

SUMMARY OF BENEFITS

REDUCE THE RISK OF A SECURITY BREACH:

Secure inside the network perimeter to significantly increase the effectiveness of a perimeter-based defense

- Centralized system provides easy management of security relationships
- Encrypts sensitive data in motion to greatly reduce the likelihood of theft
- Identifies and authenticates devices accessing protected data
- Dynamic network segmentation provides defense in depth, without moving cables
- Supports the entire environment irrespective of OS or hardware platforms

COST EFFECTIVE, EASILY MANAGED SYSTEM:

Automatically encrypts data in motion, enforces network security relationships and implements machine level access control

- Software-based design is compatible with existing security systems, so improved flexibility, performance and scalability, eliminating costly equipment purchases
- Transparent to end users and applications, avoiding costly software upgrades and end user training
- Modular system architecture enables easily phased deployment to meet the stringent and unique needs of global enterprise and government installations
- Enterprise class system capable of managing large scale environments

SATISFY IT SECURITY REQUIREMENTS OF REGULATORY COMPLIANCE:

Secure data transmittal, enforce access policy and maintain audit trail

- Flexible management architecture supports centralized, distributed or tiered administrative structure to enforce security policies based on your unique organ zational design
- Sensitive internal data flows are protected with point-to-point encryption
- Machine-level access control restricts unauthorized system access
- Automatic enforcement of security relationships and 'out of bounds' activity repor ing provides an effective audit trail to demonstrate compliance and reduce the cost of the audit

ABOUT APANI NETWORKS

Established in 2003, Apani Networks is the leading enterprise network security software provider focused on securing inside the network perimeter. EpiForce, the company's flagship product, provides a transparent security layer for networked applications by encrypting data in motion, enforcing machine-level access control and centrally managing security policy relationships. Apani enables corporate IT managers to quickly, automatically and cost effectively lock down their networks, while providing the security and audit trail necessary to demonstrate compliance to the wide range of regulations that affect enterprises today.

IN THE UNITED STATES ALONE, IT IS ESTIMATED THAT ABOUT 10 MILLION AMERICANS HAVE HAD THEIR PERSONAL INFORMATION PILFERED AND MISUSED, RESULTING IN ANNUAL LOSSES OF $5 BILLION TO CONSUMERS AND $48 BILLION TO BUSINESSES.
FEDERAL TRADE COMMISSION

Apani

www.apani.com

Telephone: +1 714 792 1800
Toll Free: 866 638 5625
Apani Networks
1800 E. Imperial Highway
Brea, California 92821