



EpiForce: Protecting Personal Information

What is EpiForce?

Apani® EpiForce® is a software-based, cross-platform server isolation solution that enables two critical disciplines—logical security zoning and policy-based encryption of data in motion. EpiForce is a distributed, centrally managed solution that is transparent to users, applications and infrastructure—making it quicker to deploy and less costly to manage than hardware-centric solutions.

Single Solution: Physical and Virtual Servers

EpiForce Security software delivers cross-platform server isolation for both virtual and physical environments with a single solution. Cross-platform server isolation eliminates vulnerabilities within the corporate network by isolating servers, endpoints and business critical data into security zones for networks supporting physical and/or virtual servers, regardless of their platform or physical location. Access to these zones is strictly based on policy, and communications between the computers in them are optionally and selectively encrypted. Cross-platform server isolation provides flexibility and efficiency not available with traditional network security solutions, and it proactively mitigates risk in the event of a breach.

Logical Security Zoning

Logical security zones offer a superior, software-based alternative to traditional network segmentation accomplished with network firewalls, VLANs and some NAC variations. Zones enable flat corporate networks to be separated into isolated security communities without reconfiguring the network and without regard to the physical location of computers. Servers and endpoints are assigned membership into one or more logical security zones, creating a flexible, layered security approach within the corporate network. Logical security zones can be based on application, IP address, port, and user group—almost any factor.

Benefits

- Increase flexibility with logical security zones and policy-based encryption of data in motion.
- Centrally manage all EpiForce resources with only a few mouse clicks.
- Extend the life of legacy applications by supporting physical and virtual
- Deploy and manage security • policies on VMs, physical servers and clients from a centralized console.
- Create logical security zones containing VMs, physical servers and clients that control access based on user and system authentication.
- Automatically reconfigures security policy if a VM is restarted, preventing a security gap.

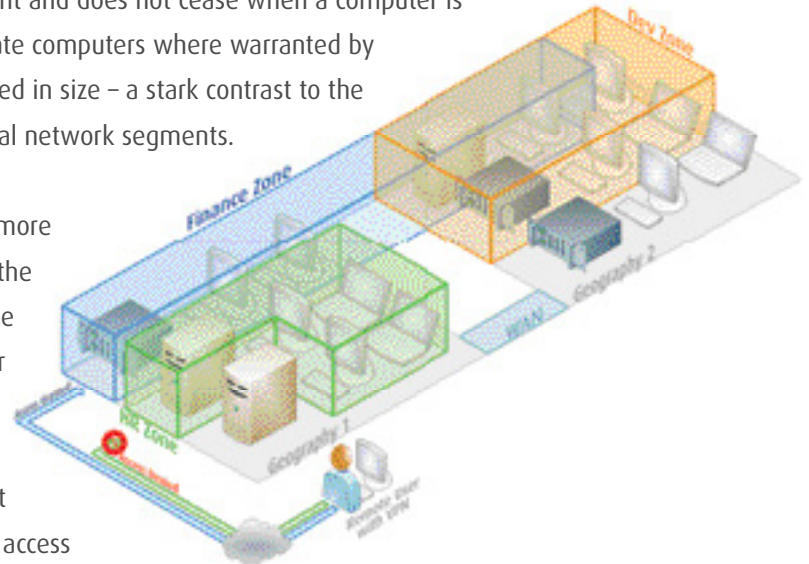
EpiForce is ideal for:

- Enabling remote worker/contractor isolation
- Achieving legal and regulatory compliance
- Safeguarding legacy applications
- Facilitating data security in mergers and acquisitions

With EpiForce, logical security zones can be spanned across physical and virtual environments, and computers can belong to one or many zones. Inclusion in a logical security zone is persistent and does not cease when a computer is physically relocated, providing organizations the flexibility to locate computers where warranted by business demands. Logical security zones can be virtually unlimited in size – a stark contrast to the constraints of available ports on a switch or a firewall in traditional network segments.

Logical security zones are centrally administered through one or more administration consoles, enabling zones and security policies for the entire EpiForce deployment to be modified with only a few mouse clicks. Administration can be delegated and workflow enabled for approving and committing policy changes.

Logical security zones can be created, moved or modified without the need to physically reconfigure the network. EpiForce controls access to logical security zones and dictates which systems can communicate with each other – at the machine or port level.



Logical security zones enable layered security without regard to platform or physical location.

Policy-Based Encryption of Data in Motion

Policy-based encryption of data in motion offers a superior alternative to the rigid encryption approaches common in link encryptors, network firewalls and personal firewalls. Policy-based encryption of data in motion secures communications between servers and/or clients based on policies dictated by the security administrator.

Apani EpiForce takes a unique two-pronged approach to encryption – delivering an efficient, low-overhead encryption mechanism and enabling security administrators to selectively deploy encryption policy at the port level. This approach allows EpiForce to strike an optimal balance between communications security and application performance, while reducing overall bandwidth requirements due to encryption. Policy-based encryption of data in motion offers a superior alternative to the rigid all-or-nothing encryption approaches common today. It secures communications between users, VMs, physical servers and clients based on policies dictated by the security administrator.



Policy-based encryption offers efficient and selective encryption at the port level.

Features & Benefits

Management and Reporting

Centralized Management Interface

Deploy and manage security policy for all EpiForce-enabled servers and endpoints from a single administration console. One or more administration consoles can be utilized simultaneously, enabling the flexibility to manage centrally, regionally or by business unit.

Role-Based Delegation of Admin Privileges

Maximize flexibility in operationalizing security policy by delegating administrator privileges to five roles including Super User, Account Management, System Settings, Operations, Audit and Read-Only.

Powerful Administrator Workflow

Utilize powerful workflows to create, submit, approve and commit security policy. All administrator actions are tracked as Change Sets and entered into the workflow process. Committed changes are deployed based on user-defined schedules.

Detailed Management Reporting

EpiForce offers 29 detailed management reports to ensure broad visibility into administrators, client software alerts, configurations, exceptions and system status.

Enhanced Alert and Activity Logging

Monitor operations of all client software through real-time alerts on penetration attempts, operational status, IPSec protocol status and an audit trail of key management and encapsulation protocols. EpiForce stores activity logs in standard Syslog and Windows Events Log formats.

Automated, Mass Software Upgrades

Deliver and execute EpiForce client software upgrades for all servers and endpoints with only a few mouse clicks. User-defined distribution servers ensure efficient software upgrades without overburdening the network or Admin Servers.

Installation and Interoperability

Cross-Platform Support

EpiForce client software is available for a broad range of operating systems, providing the flexibility to secure complex heterogeneous enterprise environments common in large companies. Legacy operating systems can be protected with EpiForce Guardian appliances.

Network Layer Transparency

EpiForce operationalizes IPSec at the network layer and is transparent to existing infrastructure and software applications. Legacy applications can easily be secured, eliminating the cost, time and incompatibilities associated with rewriting applications.

Broad VPN Client Support

EpiForce is compatible with VPN client software from leading vendors including Cisco.

Auto Create and "Push" Install Support

EpiForce enables thousands of servers and endpoints to be added and assigned default security policy at once, streamlining initial and incremental deployments. Client software can be deployed through most standard "push" installation packages such as Microsoft SMS or custom scripts.

Operations

Logical Security Zones

Isolate servers and endpoints into one or more private communities without regard to their physical location. Logical security zones can be based on IP addresses or ranges, ports, geographic regions and user groups – almost any factor. Logical security zones can be spanned across physical and geographic boundaries and can be sized for almost any application.

Policy-Based Encryption of Data in Motion

Efficiently secure communications between servers and endpoints based on port-level policy. Policy-based encryption is highly scalable, maximizes application performance and minimizes bandwidth requirements. EpiForce combines strong encryption and data integrity using industry-standard protocols.

Distributed Architecture

EpiForce is a distributed architecture with policy enforced between servers and clients themselves, eliminating the bottlenecks and single points of failure common in hardware-based solutions like firewalls, VLANs and NAC.

Policy Persistence

Security policy deployed by EpiForce remains persistent, regardless of the physical location of a server or endpoint. When a machine is moved, the security policy goes with the machine and does not require any policy changes or administrative action.

Customizable Failover Procedures

Granular and customizable failover procedures enable more flexibility to deploy EpiForce into normal business processes.

Support for Unprotected Hosts

Enforce policy for servers, endpoints and devices that don't have EpiForce installed, allowing printers and other devices to be included in logical security zones.

On-Demand Policy Distribution

Facilitate large deployments and the extension of EpiForce to servers and endpoints that have minimal disk and memory resources.



EpiForce Requirements and Specifications

Platforms Supported

EpiForce Management (Admin Server & Database)	<ul style="list-style-type: none"> • Windows 2003 Standard Edition, SP2 • Windows 2003 Standard Edition (x86-64) • Windows 2003 Standard Edition, R2 (x86-64) • Windows 2003 Enterprise Edition, SP2 • Windows 2008 Enterprise Edition (x86-32) • Windows 2008 Enterprise Edition, R2 (x86-32)
Admin Console	<ul style="list-style-type: none"> • Windows XP, SP2 or SP3 (x86, 32-bit) • Windows 2003 Standard Edition, SP2 • Windows 2003 Enterprise Edition, SP2

EpiForce Agent Requirements

Microsoft Windows <ul style="list-style-type: none"> • Windows XP SP2 or SP3 (x86-32) • Windows 2003 Standard Edition, SP2 (x86-32 and x86-64) • Windows 2003 Enterprise Edition, SP2 (x86-32 and x86-64) • Windows 2008 Standard Edition (x86-64) • Windows 2008 Standard Edition, R2 (x86-64) • Windows 2008 Enterprise Edition (x86-64) • Windows 2008 Enterprise Edition, R2 (x86-64) 	Linux <ul style="list-style-type: none"> • RedHat Enterprise Linux 3.0 (x86-32) • RedHat Enterprise Linux 4.0 (x86-32 and x86-64) • RedHat Enterprise Linux 5.0 (x86-64)
IBM <ul style="list-style-type: none"> • IBM AIX 5.3 (POWER, 64-bit) • IBM AIX 6.1 (POWER, 64-bit) 	Community Enterprise Operating Systems <ul style="list-style-type: none"> • CentOS 5 (x86-64)
Solaris <ul style="list-style-type: none"> • Solaris 8 (64-bit SPARC) • Solaris 9 (64-bit SPARC) • Solaris 10 (64-bit SPARC) 	HP <ul style="list-style-type: none"> • HP-UX 11i v1 (64-bit PA-RISC) • HP-UX 11i v2 (64-bit Itanium)

For complete requirements and compatibility information, visit www.apani.com

Technical Specifications

Authentication	x.509v3 certificate-based 128-bit AES with verification using Digital Signature Standard (DSS)
Security Standards	IPsec, IKE, x.509v3, PKCS
IPsec Data Encryption	DES, 3DES (168-bit key), AES-128, AES-256
IPsec Data Integrity	HMAC SHA-1, and HMAC MD5
Certificate Authority	Embedded x.509v3
Connection Authentication	x.509v3 certificate-based with verification using the DSS, automatic certificate management between communicating Admin Server and Agents.
Key Management	Automatic key generation and updating using IPsec standard Internet Key Exchange protocol (IKE, formerly ISAKMP / Oakley), Diffie-Hellman Key Exchange Base, Identity Protection and Aggressive Mode Exchange
Scalability	Supports up to 100,000 agents per zone