

Protect Your Data with An Identity-Aware Network

What is EpiForce VM?

Apani[®] EpiForce[®] VM helps an organization accelerate adoption of server virtualization by securing virtual machines (VMs), physical servers and clients on their network from a centralized management console. EpiForce VM security software delivers access control and policy-based encryption, both based on identity, to protect critical data and communications from intruders. Working at the network layer, EpiForce VM deploys logical security zones that are transparent to users and applications, enabling security zones to be quickly deployed and efficiently managed from a central console. Unlike access control appliance-based solutions that rely on physical locations and IP addresses, EpiForce VM creates an *identity-aware network* that delivers security to mixed physical and virtual data centers independent of these requirements.

EpiForce VM: Building an Identity-Aware Network

VPNs, remote workers and web applications render traditional network perimeter defenses ineffective, leaving internal networks vulnerable to attack.

According to industry analyst Gartner, “adding identity awareness to a network enables visibility into user behavior and adds another layer of protection for critical resources”.^{*} EpiForce VM allows an organization to create an identity-aware network that protects data and network communications by isolating users, servers, clients and mission critical data into security zones, regardless of system platform or physical location. Access to these zones is based on policy and traffic is selectively encrypted. EpiForce VM provides flexibility and efficiency not available with traditional network security solutions.

To maximize the benefits realized by virtualization, an identity-aware network helps large organizations impose dynamic, yet secure policies across all platforms in their data centers. Organizations no longer need to face a trade-off between the operational benefits of virtualization and maintenance of strong security. The complexity of a silo approach to securing their data center is avoided. Organizations are better positioned to satisfy regulatory compliance standards that require network segmentation without physically reconfiguring the network and minimize audits by reducing the attack surface. EpiForce VM delivers an identity-aware network through two disciplines: logical security zones and policy-based encryption, both based on identity.

^{*}“Introducing the Identity-Aware Network”, Lawrence Orans, Gartner, 10 December 2008/ID Number: G00162947

At a Glance

EpiForce VM security software enables an organization to create an identity-aware network across VMs, physical servers and clients to protect critical network data and communications from intruders.

Only EpiForce VM allows you to:

- 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.
- Secure network traffic through policy-based encryption of data in motion based on identity to protect all data communications - virtual and physical.
- Maintain security policy when VMs are created or migrated to prevent an unprotected VM from being deployed.
- Protect data across mixed data centers running a variety of operating systems on disparate platforms without the cost or difficulty of modifying applications or network configurations.
- Automatically reconfigures security policy if a VM is restarted, preventing a security gap.

EpiForce VM is ideal for:

- Enabling guest networking/contractor isolation
- Achieving legal and regulatory compliance (e.g. PCI DSS)
- Safeguarding legacy applications
- Facilitating information security in mergers and acquisitions
- Controlling network administrator access

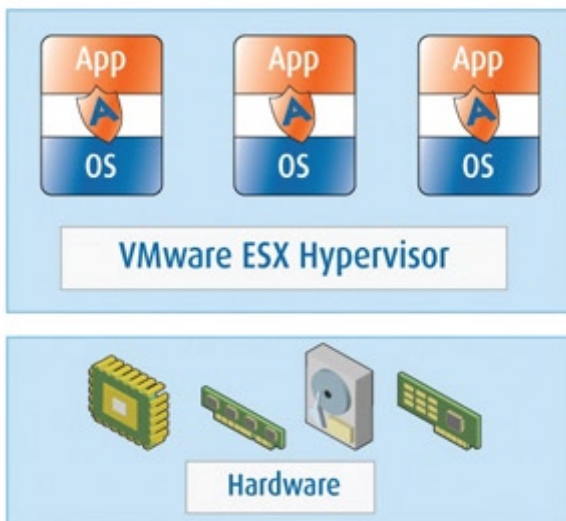
Logical Security Zoning and Policy-Based Encryption Based on Identity

Logical security zones offer a superior, software-based alternative to traditional network segmentation. Security zones enable flat networks to be separated into isolated security communities without reconfiguring the network and without regard to platform or the physical location of computers. Users, VMs, physical servers and clients are assigned membership into one or more logical security zones, creating a flexible, layered security approach within the network. Logical security zones can be based on users, user groups, applications, IP addresses, ports, geographic regions – almost any factor.

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.

Simpler, More Flexible Alternative

EpiForce VM is designed for the reality that an organization has legacy systems, virtualized servers and everything in between. The static nature of a hardware solution renders it inappropriate for the operational flexibility of server virtualization. A virtualization specific software security appliances does not account for the rest of the physical data center. EpiForce VM addresses this dilemma by providing a single console to deploy and manage security policy for both virtual and physical systems in a data center.



EpiForce Protected Virtual Machine

In a VMware ESX Server, EpiForce agents are installed on each VM to deliver strong identity-based access control and encryption of data in motion.

Features & Benefits

Operations

Logical Security Zoning

Control access to resources by isolating users, virtual or physical servers and clients into one or more private communities without regard to their physical or virtual location. For increased flexibility, zones may be based on users, user groups, IP addresses or ranges, ports and geographic regions - almost any factor.

Identity and Secure Policy Enforcement **New!**

Policies can be set to grant user or system access to one or more logical security zones or to deny “un-trusted” user or system access. User authentication uses Kerberos tickets and system authentication uses digital certificates so both user and system authentication are cryptographically secure.

Policy-Based Encryption of Data in Motion

Network data communications between users and virtual or physical systems may efficiently be secured through policy-based encryption of data in motion. Secure, IPsec “supported” data encryption algorithms DES, 3DES, AES-128 or AES-256 are used.

Preventive Jump-Off **New!**

A single EpiForce Agent on a Microsoft Windows or Citrix XenApp Terminal Server can control multiple remote users and their security policies to prevent “jump-off” or unauthorized access to critical data on a network.

Policy Persistence

Security policy remains persistent, regardless of the physical location of a user, virtual or physical server or client. In the event of a location change, the security policy follows the user or system and requires no additional administrative action. Agents also automatically reconfigure security policy when a VM is restarted avoiding a security gap. Other security solutions lack this feature and pose a security risk.

Distributed Architecture

To maintain high availability, EpiForce VM software was designed with a distributed architecture that allows multiple instances of management components to be installed to maintain fault tolerance. Policies are enforced between servers and clients themselves, eliminating the bottlenecks and single points of failure common in appliance-based solutions like firewalls, VLANs and NAC.

Unprotected Host Support

Servers, clients, printers and other devices that do not have Enforce VM installed may be included in logical security zones to control access to those critical resources.

Minimal Performance Impact

VeriTest, an independent testing lab, found that EpiForce VM imposes a minimal impact to CPU utilization and typical network traffic flows.

Management and Reporting

Centralized Management Interface

Policies are easily deployed and managed from a centralized console with a user-friendly graphical user interface (GUI) from anywhere on the network. A management console may also be installed in the data center or remote offices to allow flexibility in central office, regional branch or organizational unit management.

VM-Enabled Admin Console

Install EpiForce VM Admin Console on one or more VMs, physical machines or both, increasing greater administrator flexibility.

Activity Logging

Penetration attempts, operational status, IPsec protocol status and an audit trail of key management and encapsulation protocols are just a few of the key activities stored in standard Syslog and Microsoft Windows Events Log formats.

Management Reporting Integrated with Third-Party Tools

Administrators can generate reports on security activities such as client software alerts, configurations, exceptions and system status through open software or standard tools such as Splunk and Crystal Reports. Data used for these reports are obtained from Syslog and Microsoft Windows Event Logs.

Dynamic Real-Time Policy Management **New!**

Administrators can quickly make immediate policy changes on-the-fly to meet urgent needs.

Role-Based Delegation of Admin Privileges

Security administrators may deploy security policy by delegating administrator privileges to five roles including Super User, Account Management, System Settings, Operations, Audit and Read-Only to maximize flexibility.

Powerful Administrator Workflow

Administrators can use 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.

Installation and Interoperability

Cross-Platform Support **New!**

EpiForce VM Agents support Windows, UNIX and Linux platforms, including VMware vSphere (VMware ESX Server, vMotion and vCenter Server) and LPAR IBM, providing the flexibility to secure complex heterogeneous enterprise environments. Legacy operating systems or platforms can be protected with an EpiForce Guardian Security Appliance.

Microsoft Active Directory (AD) Synchronization **New!**

To deliver simplified administration and secure identity verification, user IDs from Microsoft Active Directory (AD) are synchronized with EpiForce VM.

Network Layer Transparency

EpiForce VM functions at the network layer to be transparent to users and applications, avoiding time-consuming user training or physical changes to the network. Legacy applications can easily be secured, eliminating the cost, time and incompatibilities associated with rewriting applications.

Broad VPN Client Support **New!**

EpiForce VM communications over a VPN is accomplished through UDP encapsulation enabling compatibility with VPN client software from vendors such as Cisco, Check Point and Nortel. This allows extended coverage of security policies to remote locations.

Enterprise-Class Security

Security and zoning policies have been tested and can scale to more than 300,000 agents. Therefore, EpiForce VM is able to meet the expanded needs of fast growing organizations who want to protect their security solution investment.

Auto Install Support

EpiForce VM Agents can be customized to install on thousands of systems remotely through standard remote installation tools. This feature streamlines deployments and saves considerable time.

Auto Registration Support **New!**

Systems with agents may have security policies configured through a pre-designed image to allow them to automatically add themselves to EpiForce VM. This eliminates data entry time and the possible errors associated with that activity.

EpiForce VM Platform Support - Physical and Virtual (exceptions noted)

Admin Console

Microsoft Windows Server 2003 R2 Enterprise Edition (32-bit x86)
Microsoft Windows XP Professional, Service Pack 2 & Service Pack 3 (32-bit x86)

Admin Server

Microsoft Windows Server 2003 R2 Enterprise Edition (32-bit x86)
Sun Solaris 10 (64-bit SPARC)*

Database

Microsoft Windows Server 2003 R2 Enterprise Edition (32-bit x86) MySQL 4.0
Sun Solaris 10 (64-bit SPARC), Oracle 10.2**

Agent

Microsoft Windows Server 2003 R2 Enterprise Edition and Terminal Server (32- & 64-bit x86, 64-bit Itanium)
Microsoft Windows XP Professional, Service Pack 2 & Service Pack 3 (32-bit x86)
Microsoft Windows 2000 Professional Service Pack 4 & Terminal Server (32-bit x86)
Citrix XenApp on Microsoft Windows Server 2003 R2 Enterprise Edition
Red Hat Enterprise Linux 5 Advanced Platform (64-bit x86) • Red Hat Enterprise Linux 4 Advanced Server (AS) (32- & 64-bit x86)
Red Hat Enterprise Linux 3 Advanced Server (AS) (32-bit x86)
Sun Solaris 10 (64-bit SPARC***)* • Sun Solaris 9 (64-bit SPARC***)* • Sun Solaris 8 (64-bit SPARC***)*
HP-UX 11i v2 (64-bit, Itanium)* • HP-UX 11i v1 (64-bit)* • IBM AIX 5.3 (64-bit, POWER) • IBM AIX 5.2 (64-bit, POWER)*

VPN Client through UDP Encapsulation

Cisco VPN Client v4.8 on Microsoft Windows XP Professional and Home Editions with Service Pack 2 and Service Pack 3
Nortel VPN Client on Microsoft Windows XP Professional and Home Editions with Service Pack 2 and Service Pack 3
Check Point VPN-1 Pro Server and Secure Client, NGX (R60), office mode on Microsoft Windows Professional and Home Editions with Service 2 and Service Pack 3

Virtualization

VMware vSphere • VMware ESX Server v3.5 • VMware VMotion • VMware vCenter Server (formerly VMware VirtualCenter)
Logical partition (LPAR) on IBM AIX 5.3

Clustering

Microsoft Cluster Server (MSCS) (64-bit x86)*
Symantec Veritas Cluster Server (VCS) Storage Foundation for Oracle RAC (SFRAC) 4.1 MP1, SOE 1.3.1 on Solaris 8 SPARC Update 1 (64-bit)*

Network Adapter Teaming

Microsoft Windows Server 2003 R2 Enterprise Edition IP Teaming on HP ProLiant (32-bit)
Red Hat Enterprise Linux 5 Advanced Platform (64-bit x86) • Red Hat Enterprise Linux 4 Advanced Server (AS) NIC Bonding (32-bit x86)
IBM AIX 5.3 on EtherChannel (64-bit)*

Load Balancing

F5 BIG-IP**

* Physical machines only ** Refer to F5 Tech Note on Apani download website *** Does not support sun4m and sun4d architectures

Technical Specifications

Authentication	x.509v3 certificate-based 128-bit AES with verification using Digital Signature Standard (DSS)
Security Standards	IPsec, IKE, x.509v3
IPsec Data Encryption	DES, 3DES, 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 (IKE) protocol (ISAKMP / Oakley), Diffie-Hellman Key Exchange Base, Identity Protection and Aggressive Mode Exchange
Scalability	Supports up to 300,000 agents