Enterprise Security
Moving from Chaos to Control with Integrated Security Management

Yanet Manzano
Florida State University
manzano@cs.fsu.edu

Enterprise Security Challenges

- Implementing consistent enterprise wide security policies
- Maintaining OS environments (patch level updates)
- Firewalls at a consistent level of protection and permission
- Managing growth of user access to computer resources
- Monitoring and responding to security events (IDS)
- Protecting against new and more sophisticated viruses and blended threat

manzano@cs.fsu.edu
Security Managers Solutions

- Home grown or ad hoc security processes
  - Security processes conformed to technology in place
  - Labor-intensive procedures linked specific products
  - Fragmented security solutions

**Result:** inefficiencies inevitably plague day-to-day operations

**Solution:** design security processes and technology **based on** business requirements and a coherent management approach

**Problem:** too much to do + too little time + too few people

---

Security Management: Complex

- Mergers and acquisitions
  - highly complex, heterogeneous IT environments

- Rapid introduction of e-business applications
  - not always fit into a corporate standard for best security practices

- Growth of trusted users among partners, consultants, suppliers
  - must access core resources online on a regular basis

- Growing awareness of the necessity of host-based, and network or perimeter security measures
Enterprise Security Goals

- Moving from chaos to better management control requires organizations to re-think and re-organize traditional approaches to security management.

Growing consensus:
- Best practice essentials that involve four “consistent threads”
  - Integrated security policy management
  - Self-service and more efficient user provisioning
  - Business-driven controls of vulnerabilities and configurations
  - Event consolidation and control

Integrated Security Policy Management

Best practice essentials

**Needs:**

- Develop/adapt policies to meet industry, regulatory and audit requirements
- Implement policies quickly and effectively across the enterprise
- Translate into practical and enforceable technical controls that can be implemented across a heterogeneous IT infrastructure
- Verifying policies compliance more effectively
Self-service and more efficient user provisioning
Best practice essentials

Needs:
- Automating the provisioning of accounts
- Administering users more effectively and efficiently
- Enabling self-service to reduce help desk costs and enhance availability

Business-driven controls of vulnerabilities and configurations
Best practice essentials

Needs:
- Establish security baselines based on most appropriate configurations
- Automate the assessment of vulnerabilities based on latest threats
- Correct exposures immediately with automated controls and patch management tools
- Maintain security controls that are scalable, auditable and consistent across the enterprise
Event consolidation and control

Best practice essentials

**Needs:**

- Detect and prevent intrusions in real time from multiple sources
- Manage and analyze security events across the enterprise to improve resource allocation and decision making
- Provide rapid, coordinated response and appropriate forensic follow up to incidents

Enterprise Solutions Needs

**Solutions**

- provide automated and integrated management tools
- improve the effectiveness and efficiency of enterprise security posture

**Automation**

- assure consistent, streamlined administrative processes
- eliminate the need for additional headcount

**Integration**

- required to deliver consistent reporting and management across complex, heterogeneous IT environments
  - multiple operating systems, security devices, and dynamic web-based services and applications
VigilEnt Integrated Security Management

- NetIQ Solution

- Solutions provide tools to:
  - automate best practice security processes
  - integrating security management across multiplatform, heterogeneous IT environments

- Ensure security technology automates processes according to corporate security policies

- Integrates people’s roles with policy driven processes that are automated by proven technology

Key Areas of Security Management
Policy & Compliance Management

- provide built-in knowledge for creating, updating, distributing and tracking security policy compliance across the enterprise

- VigilEnt Policy Center
  - acts as the engine
  - security managers can extend their policies and standards out to their security technology infrastructure

- Content Modules
  - provide significant efficiencies in developing policies for highly regulated industries such as government agencies

Policy & Compliance Management

VigilEnt Policy Center

- contains a library of policies and standards
- allows security managers to assign policy standards based on roles
- certify people in roles have read and agreed to abide by the policy standards
- security policies and standards can be translated into groupings of technical and business rules
  - applied to the key technologies that protect information assets
Administration & Identity Management

- Automate the process for a wide variety of administrative tasks
  - self-service user password resets
  - password synchronization,
  - role-based user provisioning,
- eliminate expensive manual administration
- minimize downtime and business interruption
- Provide authorized users access to critical applications swiftly and securely 24x7

VigilEnt Password Manager:
- self-service for password resets via any online web browser
- automatic and consistent monitor and maintain password policy

VigilEnt User Manager
- secure and efficient manage user access to corporate applications from a common facility
- centralized user administration and automated user provisioning for heterogeneous platform environments
Administration & Identity Management

**Security Administration Suite**

- highly secure and automated delegation of Windows account administration
- planning, managing, troubleshooting and reporting for Windows Group Policy from central, easy-to-use console
- innovative Windows Active Directory permissions management capabilities:
  - powerful role-based security
  - auditing and advanced analysis

Administration & Identity Management

**File Security Administrator**

- delivers a complete file security management and reporting solution for Windows NT 4 and Windows 2000 environments

**Migration Suite**

- accelerates the transition between platforms while minimizing the impact on IT and user resources.
Many Organizations:
- where and how they are vulnerable?
- what information assets to protect?
- how to go about correcting exposures when found?
- Struggling to develop accepted practices for
  - establishing a baseline standard of protection
  - configuring and maintaining systems to meet standards

**VigilEnt Security Manager**
- automated centralize vulnerability management across heterogeneous systems
- proactively ensures system availability by establishing
  - security configuration baselines,
  - continuously auditing for security vulnerabilities
  - helping correct exposures
**Security Analyzer**

- provides a flexible, enterprise-scale vulnerability assessment solution for Windows, Solaris and Linux computers
- scans computers across the network for the latest vulnerabilities
- provides reports to help correct vulnerabilities and comply with company security policies.

**Incident & Event Management**

Helps solve business security problems:
- managing security events in real-time
- consolidating security event logs for effective log analysis
- managing multiple firewall reporting system
- improve efficiency and reduce staff time by
  - preventing intrusions
  - automating event management and response
Incident & Event Management

**VigilEnt Log Analyzer**

- provides archival and historical analysis of logs across the enterprise
- collects logs using a *distributed and hierarchical architecture*
  - Ex: OS, web servers, third-party event source
- normalizes logged events from disparate sources
  - enabling query and analysis of logs over a period of time
- archive logs and perform sophisticated *intrusion trend and forensic analysis*

Incident & Event Management

**Security Manager**

- provides real-time monitoring across multiple IDS, firewall and anti-virus devices of
  - security threats
  - intrusions and
  - policy violations
- delivers automated controls
  - do not require security knowledge for deployment and customization
Incident & Event Management

**Firewall Reporting Products**

- Provide essential info about activity around popular firewall appliance products in easy-to-interpret reports

- Use reports to:
  - Assess the state of network
  - Eliminate security threats and network abuses

---

**Conclusion**

- Policy-driven approach to managing info security
  - helps assure continuous policy compliance for people and technology across the enterprise

- Automate technology implementation and ongoing maintenance of key security management functions to
  - minimize personal | leverage the value of investments

- Comprehensive security management integration and coverage of heterogeneous e-business IT environments

- deliver the benefits of a common security infrastructure and architecture with superior functionality