Dr. Myron L. Cramer
The Windermere Group

WINDERMERE

Windermere
2000 Windermere Court
Annapolis, Maryland 21401
410-266-1900

CIO interact 2004

Blair County Convention Center
One Convention Center Drive
Altoona, PA
March 28 – 29, 2004

Risk Management Round Table
Panel Issue # 4

How do you strike the balance between the drive, drive, drive to get things done in IT Departments, with the need to safeguard systems and applications?

WINDERMERE

Premise

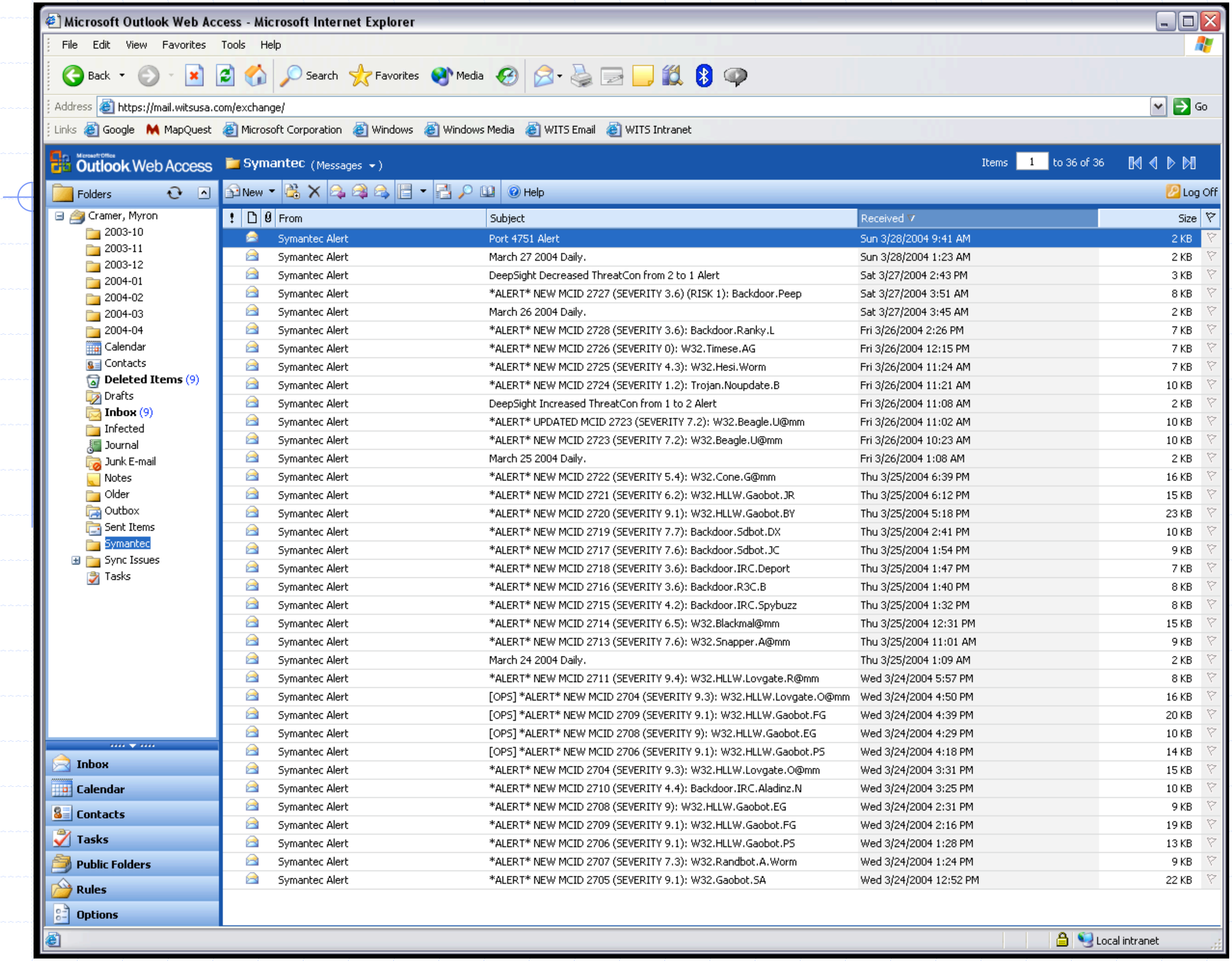
- **Security impedes IT functions**
  - User: Accounts, passwords, and privileges
  - Workstations: standardized baselines, operating systems, core applications
  - Network: Hook-ups, LAN’s, WAN’s
  - Servers: Hosts, corporate services
  - Firewalls: filters, proxies, remote access
- **Security adds no value to the IT business proposition**
  - Security is separate from IT capabilities
  - Protecting services does not add value

Today’s Environment

- **Viruses & Worms**
  - Mass mailing
  - Trojans
  - Distributed Denial of Service
  - Data Base Injections
- **Patches**
  - Windows Critical Updates
- **Internet Fraud**
  - Scams
  - Impersonation

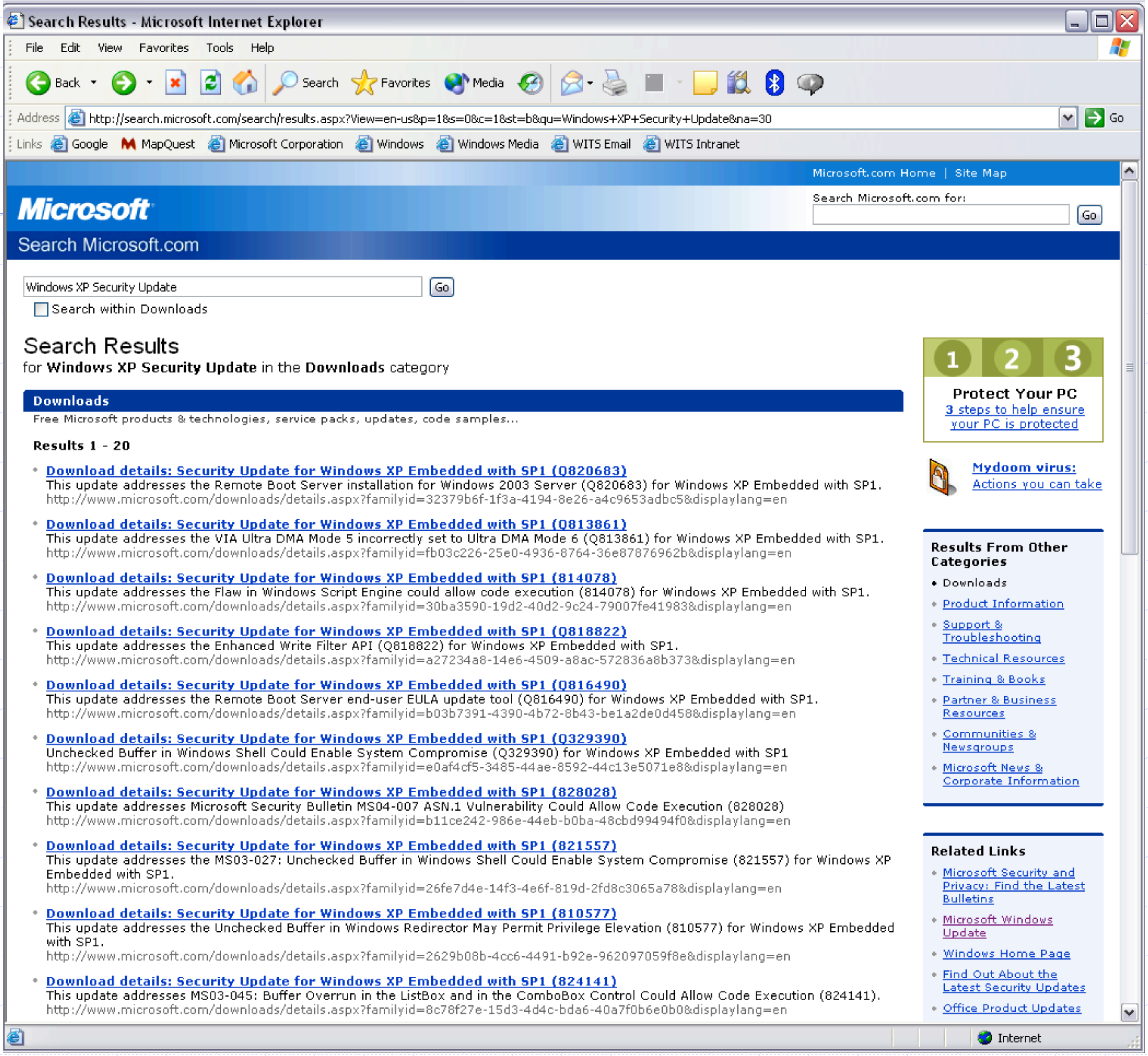
- **Information Theft**
- **SPAM**
- **Network Congestion**
- **System Outages**

How much can IT really get done without security to protect against these?



Address https://mail.witsusa.com/exchange/

From	Subject	Received	Size
Symantec Alert	Port 4751 Alert	Sun 3/28/2004 9:41 AM	2 KB
Symantec Alert	March 27 2004 Daily.	Sun 3/28/2004 1:23 AM	2 KB
Symantec Alert	DeepSight Decreased ThreatCon from 2 to 1 Alert	Sat 3/27/2004 2:43 PM	3 KB
Symantec Alert	*ALERT* NEW MCID 2727 (SEVERITY 3.6) (RISK 1): Backdoor.Peep	Sat 3/27/2004 3:51 AM	8 KB
Symantec Alert	March 26 2004 Daily.	Sat 3/27/2004 3:45 AM	2 KB
Symantec Alert	*ALERT* NEW MCID 2728 (SEVERITY 3.6): Backdoor.Ranky.L	Fri 3/26/2004 2:26 PM	7 KB
Symantec Alert	*ALERT* NEW MCID 2726 (SEVERITY 0): W32.Timese.AG	Fri 3/26/2004 12:15 PM	7 KB
Symantec Alert	*ALERT* NEW MCID 2725 (SEVERITY 4.3): W32.Hesi.Worm	Fri 3/26/2004 11:24 AM	7 KB
Symantec Alert	*ALERT* NEW MCID 2724 (SEVERITY 1.2): Trojan.Noupdate.B	Fri 3/26/2004 11:21 AM	10 KB
Symantec Alert	DeepSight Increased ThreatCon from 1 to 2 Alert	Fri 3/26/2004 11:08 AM	2 KB
Symantec Alert	*ALERT* UPDATED MCID 2723 (SEVERITY 7.2): W32.Beagle.U@mm	Fri 3/26/2004 11:02 AM	10 KB
Symantec Alert	*ALERT* NEW MCID 2723 (SEVERITY 7.2): W32.Beagle.U@mm	Fri 3/26/2004 10:23 AM	10 KB
Symantec Alert	March 25 2004 Daily.	Fri 3/26/2004 1:08 AM	2 KB
Symantec Alert	*ALERT* NEW MCID 2722 (SEVERITY 5.4): W32.Cone.G@mm	Thu 3/25/2004 6:39 PM	16 KB
Symantec Alert	*ALERT* NEW MCID 2721 (SEVERITY 6.2): W32.HLLW.Gaobot.JR	Thu 3/25/2004 6:12 PM	15 KB
Symantec Alert	*ALERT* NEW MCID 2720 (SEVERITY 9.1): W32.HLLW.Gaobot.BY	Thu 3/25/2004 5:18 PM	23 KB
Symantec Alert	*ALERT* NEW MCID 2719 (SEVERITY 7.7): Backdoor.Sdbot.DX	Thu 3/25/2004 2:41 PM	10 KB
Symantec Alert	*ALERT* NEW MCID 2717 (SEVERITY 7.6): Backdoor.Sdbot.JC	Thu 3/25/2004 1:54 PM	9 KB
Symantec Alert	*ALERT* NEW MCID 2718 (SEVERITY 3.6): Backdoor.IRC.Deport	Thu 3/25/2004 1:47 PM	7 KB
Symantec Alert	*ALERT* NEW MCID 2716 (SEVERITY 3.6): Backdoor.R3C.B	Thu 3/25/2004 1:40 PM	8 KB
Symantec Alert	*ALERT* NEW MCID 2715 (SEVERITY 4.2): Backdoor.IRC.Spybuzz	Thu 3/25/2004 1:32 PM	8 KB
Symantec Alert	*ALERT* NEW MCID 2714 (SEVERITY 6.5): W32.Blackmal@mm	Thu 3/25/2004 12:31 PM	15 KB
Symantec Alert	*ALERT* NEW MCID 2713 (SEVERITY 7.6): W32.Snapper.A@mm	Thu 3/25/2004 11:01 AM	9 KB
Symantec Alert	March 24 2004 Daily.	Thu 3/25/2004 1:09 AM	2 KB
Symantec Alert	*ALERT* NEW MCID 2711 (SEVERITY 9.4): W32.HLLW.Lovgate.R@mm	Wed 3/24/2004 5:57 PM	8 KB
Symantec Alert	[OPS] *ALERT* NEW MCID 2704 (SEVERITY 9.3): W32.HLLW.Lovgate.O@mm	Wed 3/24/2004 4:50 PM	16 KB
Symantec Alert	[OPS] *ALERT* NEW MCID 2709 (SEVERITY 9.1): W32.HLLW.Gaobot.FG	Wed 3/24/2004 4:39 PM	20 KB
Symantec Alert	[OPS] *ALERT* NEW MCID 2708 (SEVERITY 9): W32.HLLW.Gaobot.EG	Wed 3/24/2004 4:29 PM	10 KB
Symantec Alert	[OPS] *ALERT* NEW MCID 2706 (SEVERITY 9.1): W32.HLLW.Gaobot.PS	Wed 3/24/2004 4:18 PM	14 KB
Symantec Alert	*ALERT* NEW MCID 2704 (SEVERITY 9.3): W32.HLLW.Lovgate.O@mm	Wed 3/24/2004 3:31 PM	15 KB
Symantec Alert	*ALERT* NEW MCID 2710 (SEVERITY 4.4): Backdoor.IRC.Aladinz.N	Wed 3/24/2004 3:25 PM	10 KB
Symantec Alert	*ALERT* NEW MCID 2708 (SEVERITY 9): W32.HLLW.Gaobot.EG	Wed 3/24/2004 2:31 PM	9 KB
Symantec Alert	*ALERT* NEW MCID 2709 (SEVERITY 9.1): W32.HLLW.Gaobot.FG	Wed 3/24/2004 2:16 PM	19 KB
Symantec Alert	*ALERT* NEW MCID 2706 (SEVERITY 9.1): W32.HLLW.Gaobot.PS	Wed 3/24/2004 1:28 PM	13 KB
Symantec Alert	*ALERT* NEW MCID 2707 (SEVERITY 7.3): W32.Randbot.A.Worm	Wed 3/24/2004 1:24 PM	9 KB
Symantec Alert	*ALERT* NEW MCID 2705 (SEVERITY 9.1): W32.Gaobot.SA	Wed 3/24/2004 12:52 PM	22 KB



http://search.microsoft.com/search/results.aspx?View=en-us&p=1&s=0&c=1&st=b&qu=Windows+XP+Security+Update&na=30

Search Microsoft.com

Windows XP Security Update [Go]

□ Search within Downloads

Search Results

for **Windows XP Security Update** in the **Downloads** category

Downloads

Free Microsoft products & technologies, service packs, updates, code samples...

Results 1 - 20

- **Download details: Security Update for Windows XP Embedded with SP1 (Q820683)**
  This update addresses the Remote Boot Server installation for Windows 2003 Server (Q820683) for Windows XP Embedded with SP1.
  http://www.microsoft.com/downloads/details.aspx?familyid=32379b6f-1f3a-4194-8e26-a4c9653adbc5&displaylang=en
- **Download details: Security Update for Windows XP Embedded with SP1 (Q813861)**
  This update addresses the VIA Ultra DMA Mode 5 incorrectly set to Ultra DMA Mode 6 (Q813861) for Windows XP Embedded with SP1.
  http://www.microsoft.com/downloads/details.aspx?familyid=fb03c226-25e0-4936-8764-36e87876962b&displaylang=en
- **Download details: Security Update for Windows XP Embedded with SP1 (814078)**
  This update addresses the Flaw in Windows Script Engine could allow code execution (814078) for Windows XP Embedded with SP1.
  http://www.microsoft.com/downloads/details.aspx?familyid=30ba3590-19d2-40d2-9c24-79007fe41983&displaylang=en
- **Download details: Security Update for Windows XP Embedded with SP1 (Q818822)**
  This update addresses the Enhanced Write Filter API (Q818822) for Windows XP Embedded with SP1.
  http://www.microsoft.com/downloads/details.aspx?familyid=a27234a8-14e6-4509-a8ac-572836a8b373&displaylang=en
- **Download details: Security Update for Windows XP Embedded with SP1 (Q816490)**
  This update addresses the Remote Boot Server end-user EULA update tool (Q816490) for Windows XP Embedded with SP1.
  http://www.microsoft.com/downloads/details.aspx?familyid=b03b7391-4390-4b72-8b43-be1a2de0d458&displaylang=en
- **Download details: Security Update for Windows XP Embedded with SP1 (Q329390)**
  Unchecked Buffer in Windows Shell Could Enable System Compromise (Q329390) for Windows XP Embedded with SP1
  http://www.microsoft.com/downloads/details.aspx?familyid=e0af4cf5-3485-44ae-8592-44c13e5071e8&displaylang=en
- **Download details: Security Update for Windows XP Embedded with SP1 (828028)**
  This update addresses Microsoft Security Bulletin MS04-007 ASN.1 Vulnerability Could Allow Code Execution (828028)
  http://www.microsoft.com/downloads/details.aspx?familyid=b11ce242-986e-44eb-b0ba-48cbd99494f0&displaylang=en
- **Download details: Security Update for Windows XP Embedded with SP1 (821557)**
  This update addresses the MS03-027: Unchecked Buffer in Windows Shell Could Enable System Compromise (821557) for Windows XP Embedded with SP1.
  http://www.microsoft.com/downloads/details.aspx?familyid=26fe7d4e-14f3-4e6f-819d-2fd8c3065a78&displaylang=en
- **Download details: Security Update for Windows XP Embedded with SP1 (810577)**
  This update addresses the Unchecked Buffer in Windows Redirector May Permit Privilege Elevation (810577) for Windows XP Embedded with SP1.
  http://www.microsoft.com/downloads/details.aspx?familyid=2629b08b-4cc6-4491-b92e-962097059f8e&displaylang=en
- **Download details: Security Update for Windows XP Embedded with SP1 (824141)**
  This update addresses MS03-045: Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution (824141).
  http://www.microsoft.com/downloads/details.aspx?familyid=8c78f27e-15d3-4d4c-bda6-40a7f0b6e0b0&displaylang=en

1 2 3

Protect Your PC

3 steps to help ensure your PC is protected

Mydoom virus: Actions you can take

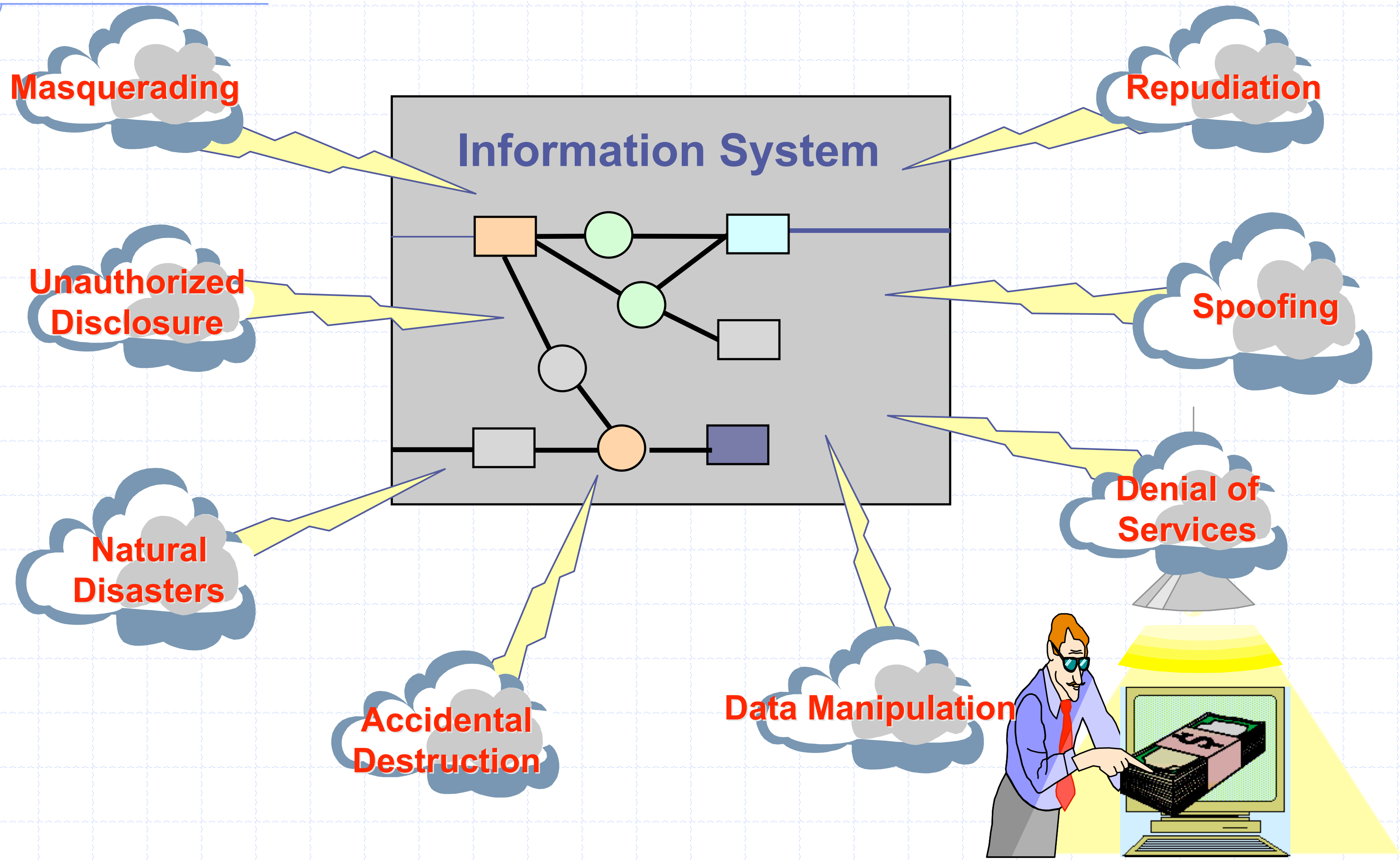
Results From Other Categories

- Downloads
- Product Information
- Support & Troubleshooting
- Technical Resources
- Training & Books
- Partner & Business Resources
- Communities & Newsgroups
- Microsoft News & Corporate Information

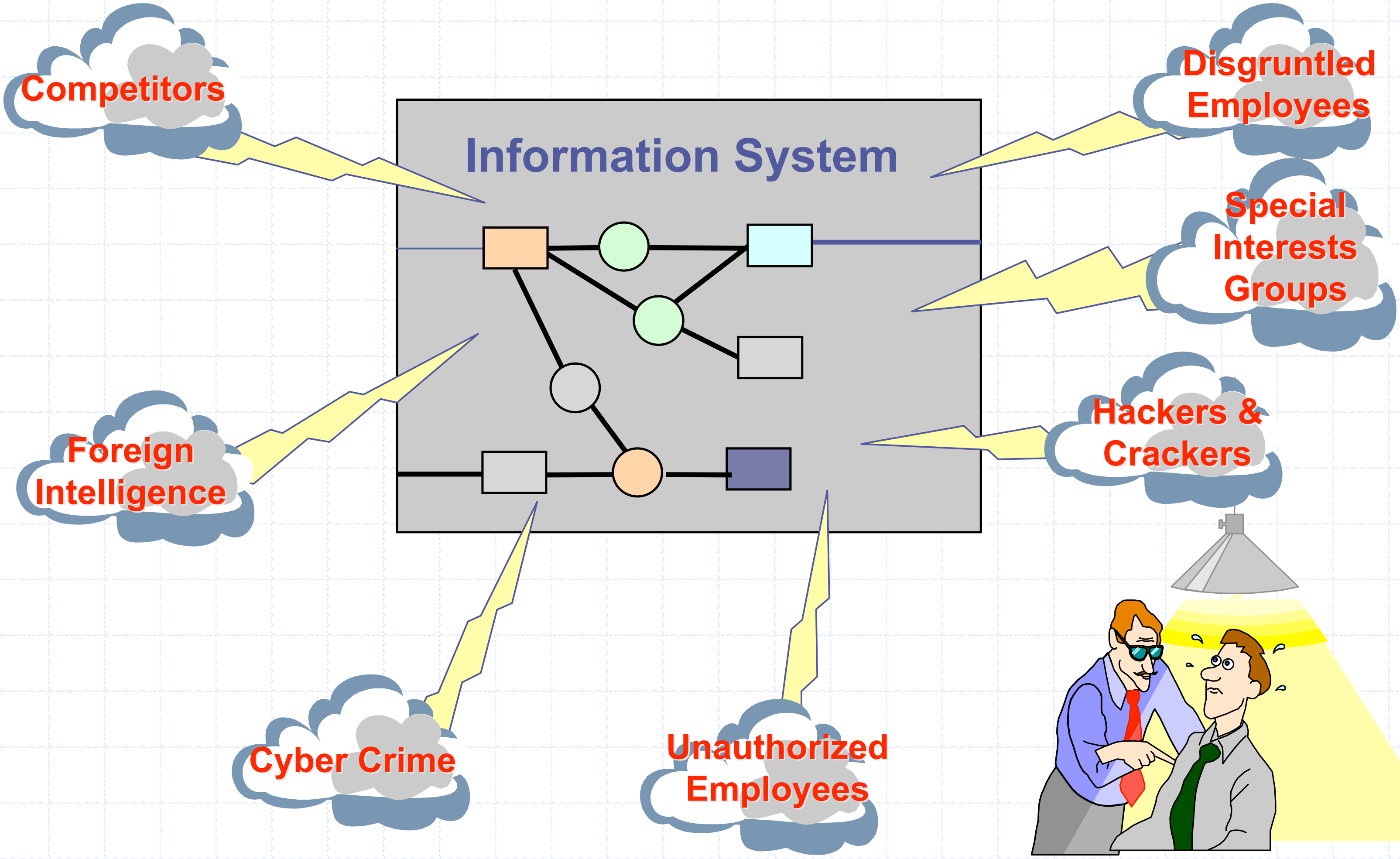
Related Links

- Microsoft Security and Privacy: Find the Latest Bulletins
- Microsoft Windows Update
- Windows Home Page
- Find Out About the Latest Security Updates
- Office Product Updates

Types of Threats



Who is a Threat?



Issue

- *How does information security fit in?*
- The perception that there is a conflict between getting IT done and security may be erroneous
- The real problem may be a failure of the information security solution

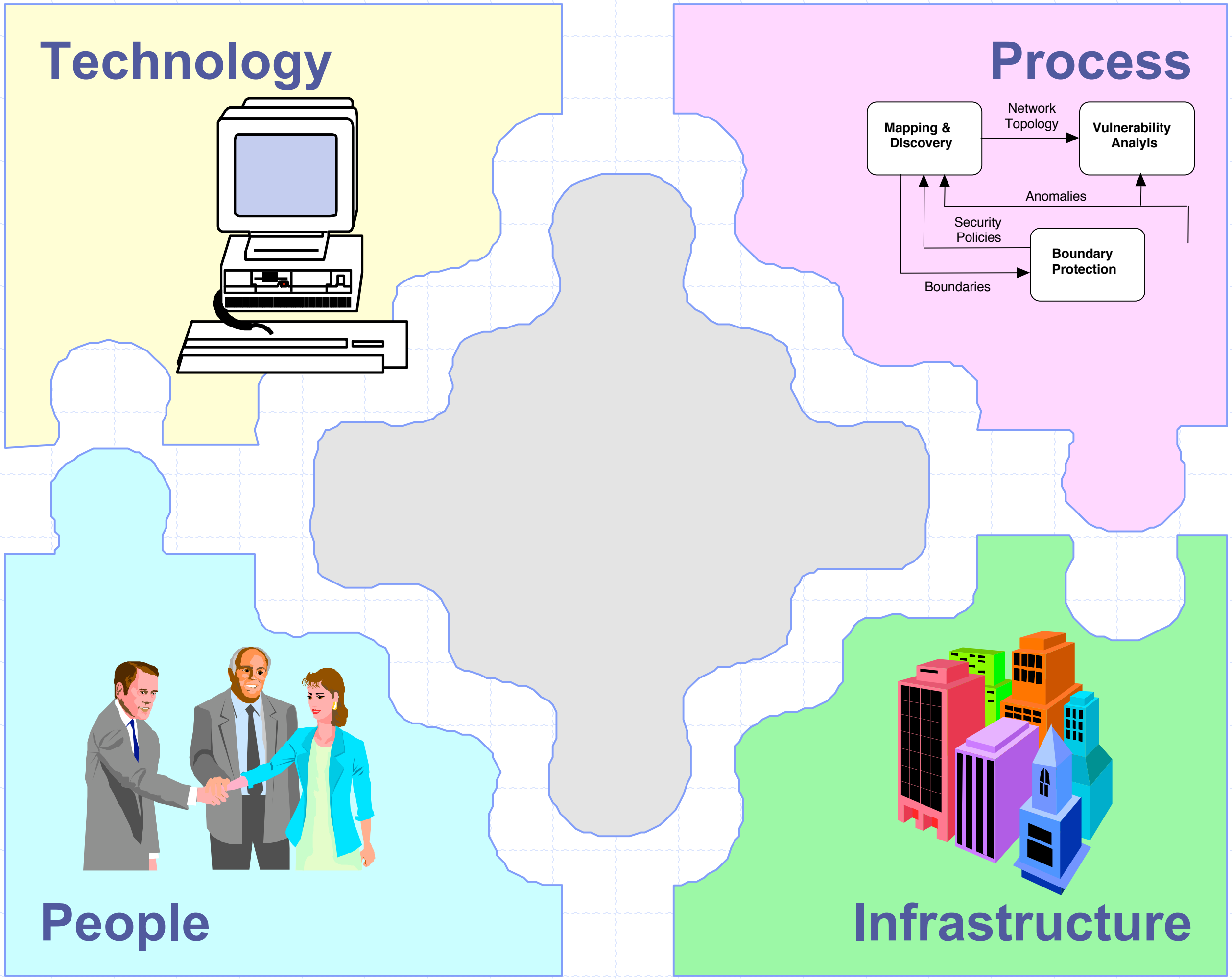
What can go wrong with the security solution?

- Inadequate information security architecture
- Wrong products
- Ineffective processes
- Unqualified people
- Inadequate infrastructure

What is a proper solution?

- Security should be part of the business proposition
- A proper security solution should enable and facilitate the use of IT
- Security should not impede IT

Solution Approaches



Technology

Process

Mapping & Discovery

Network Topology

Vulnerability Analyis

Anomalies

Security Policies

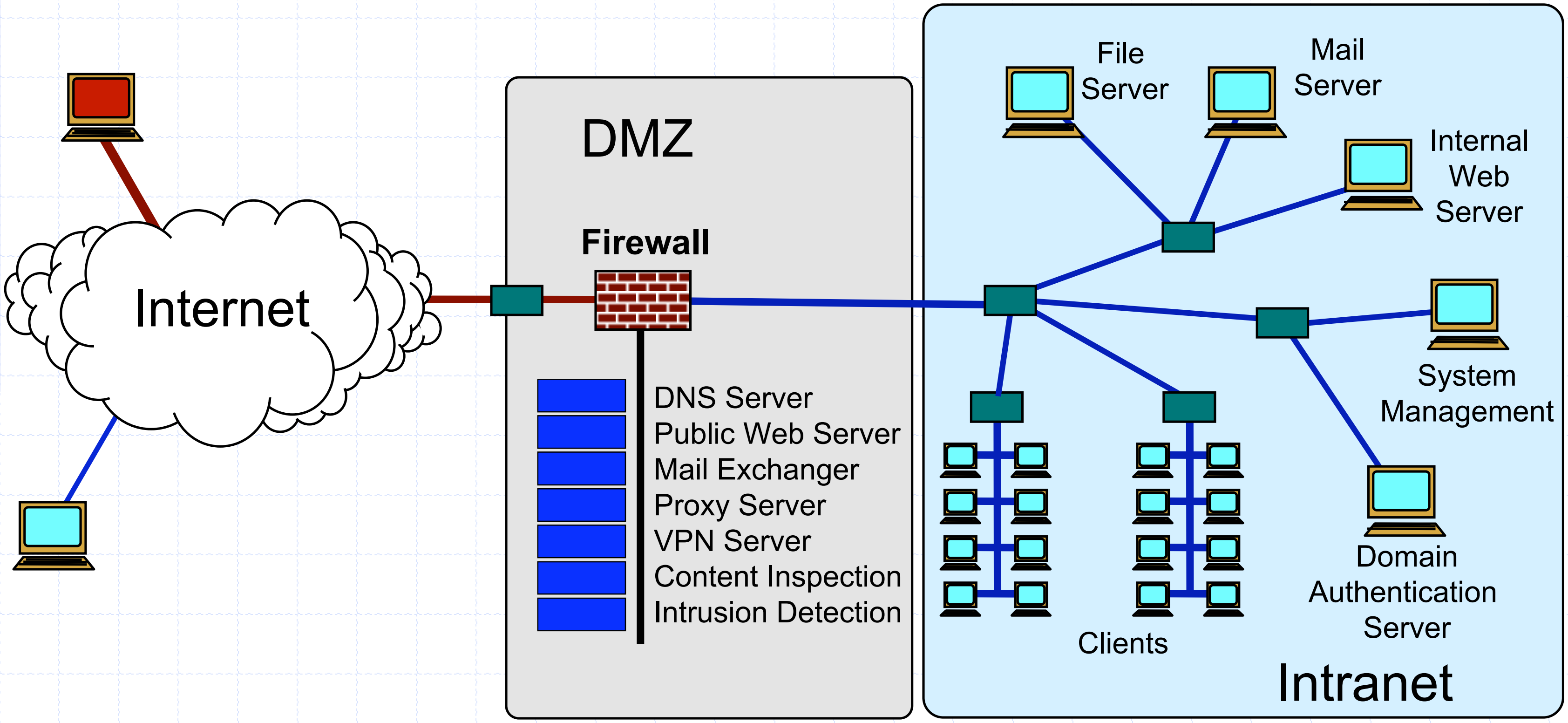
Boundary Protection

Boundaries

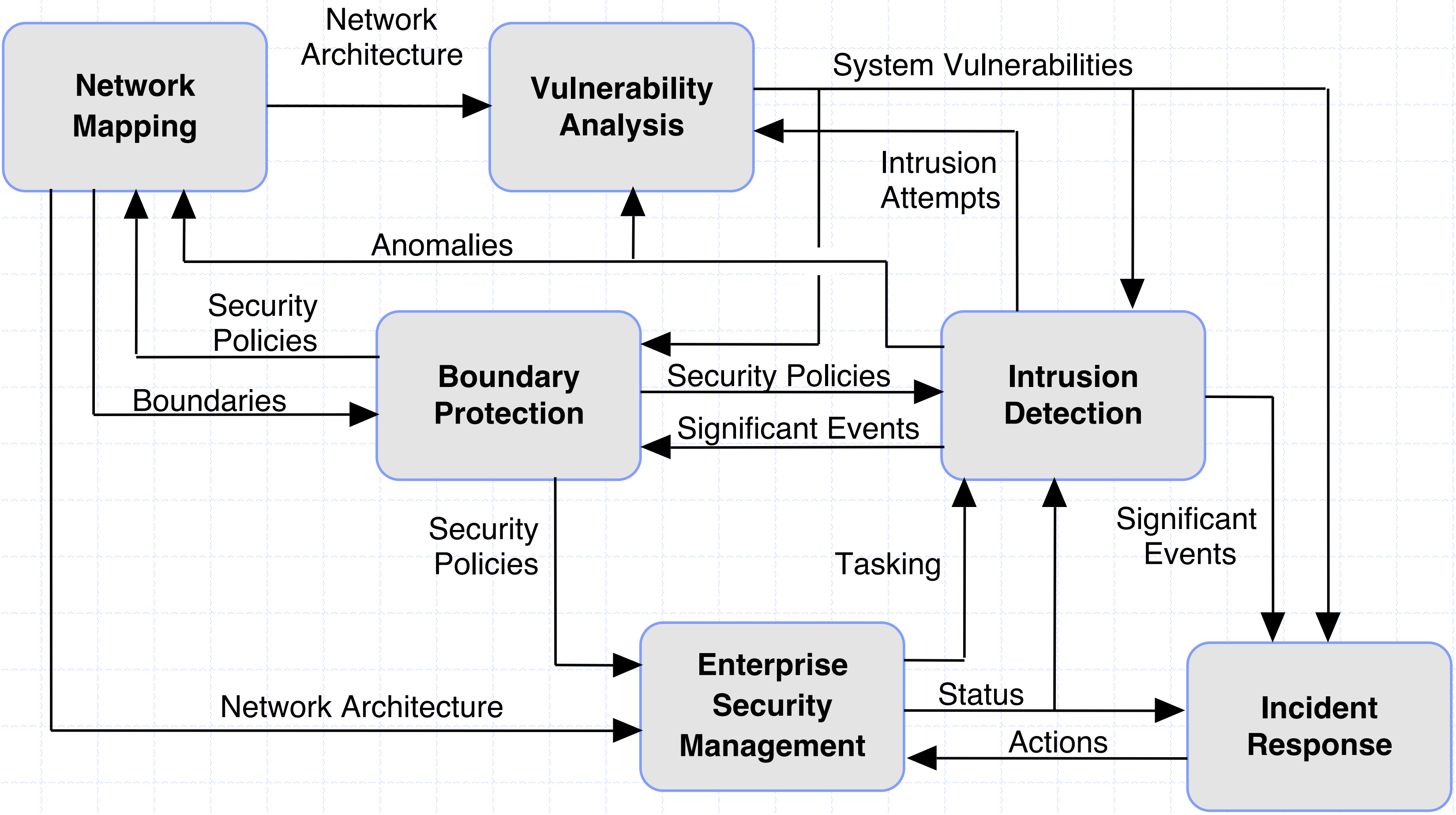
People

Infrastructure

Technology


Internet
DMZ
Firewall
DNS Server
Public Web Server
Mail Exchanger
Proxy Server
VPN Server
Content Inspection
Intrusion Detection
File Server
Mail Server
Internal Web Server
System Management
Domain Authentication Server
Clients
Intranet

Process



Network Mapping

Network Architecture

Vulnerability Analysis

System Vulnerabilities

Intrusion Attempts

Anomalies

Security Policies

Boundaries

Boundary Protection

Security Policies

Significant Events

Intrusion Detection

Security Policies

Tasking

Significant Events

Network Architecture

Enterprise Security Management

Status

Actions

Incident Response

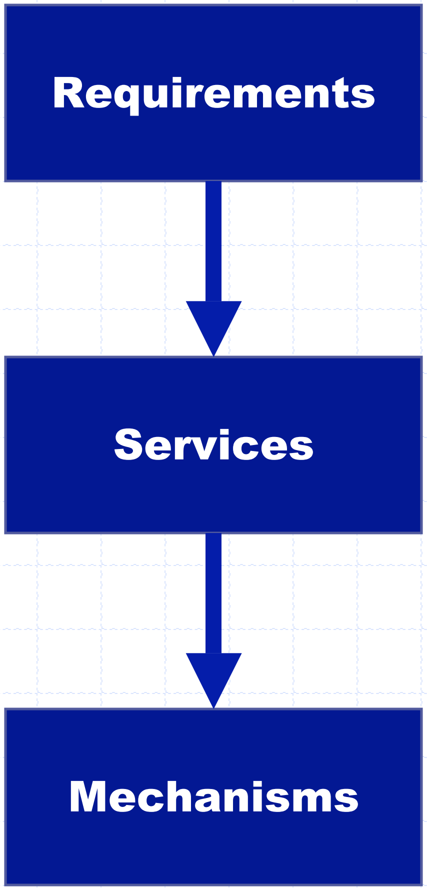
People

- **Experience**
  - Information security professionals
  - Previous clients
- **Certification**
  - Qualifications
  - Proficiency testing
- **Education**
  - Information systems
  - Networking
  - Application services
- **Training**
  - Information security seminars
  - Conferences

Infrastructure

- Facilities
- Physical Controls
- Video Monitoring
- Remote Management

Security Engineering Process



Requirements

Services

Mechanisms

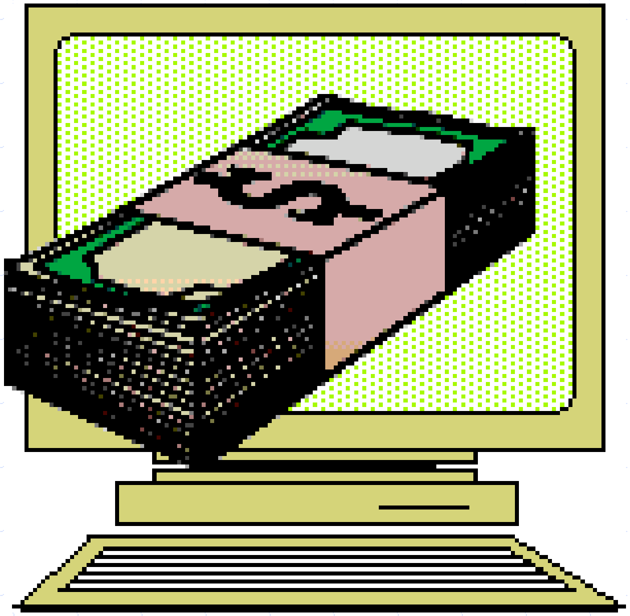
- **Policy**
  - Laws
  - Regulations
  - Agreements
  - Directives
- **Requirements Translation**
  - Operational Environment
  - Risk Exposures
  - User Communities
  - Information Administration
  - Security Specifications
- **Design**
  - Architectural Implementation
  - Product Performance Specification
  - Components Selection and Configuration

Information Assurance Requirements

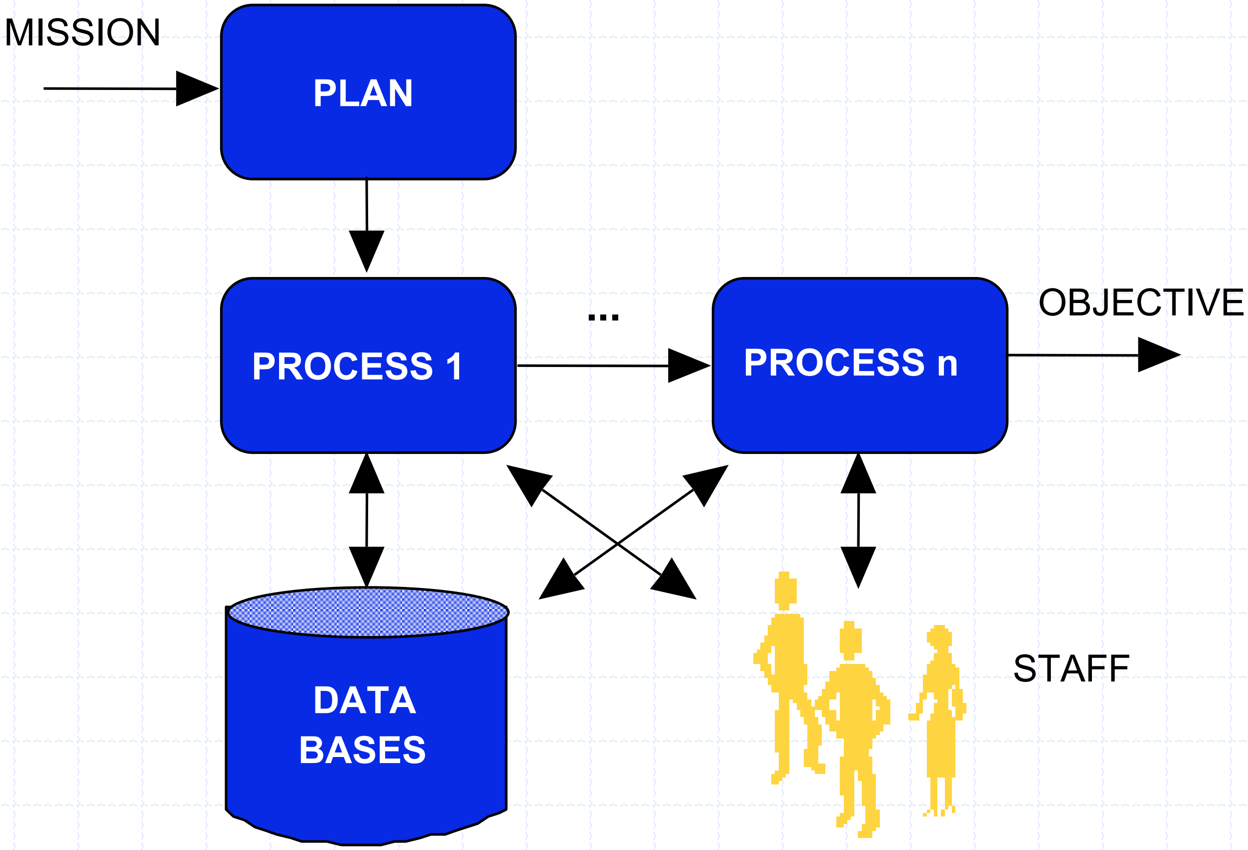
- **Confidentiality**
  - *Information is not disclosed to unauthorized users or processes*
  - Identification and authentication
  - Screen Lock
  - Labeling & Marking
  - Access Control
  - Separation of information & roles
  - Non-Repudiation
  - Audit
- **Integrity**
  - *Data or processes have not been altered or corrupted*
  - Configuration Management
  - Change Control
  - Malicious Code Protection
- **Availability**
  - *Information and information systems will be available to users*
  - Reconstitution
  - Continuity of Operations

Value of Information

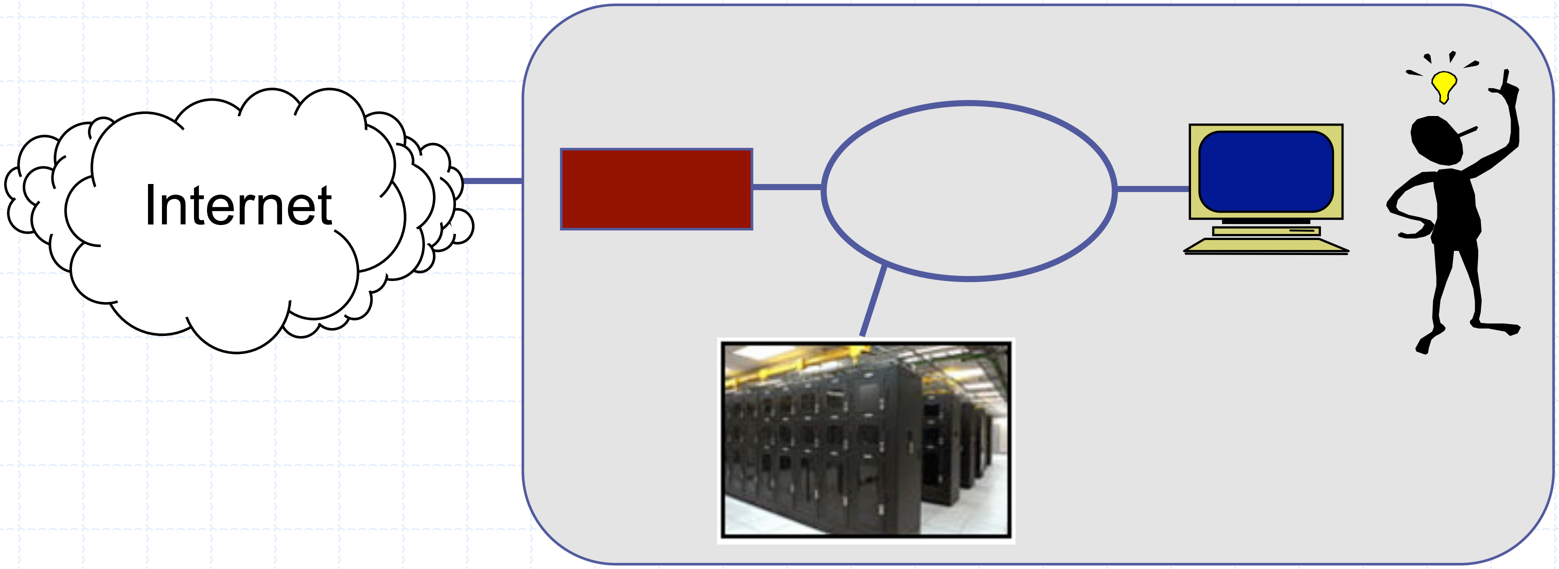
- Critical factor in the success of businesses and government
- Takes a wide variety of forms
- Each has a different value and different protection need



Types of Information

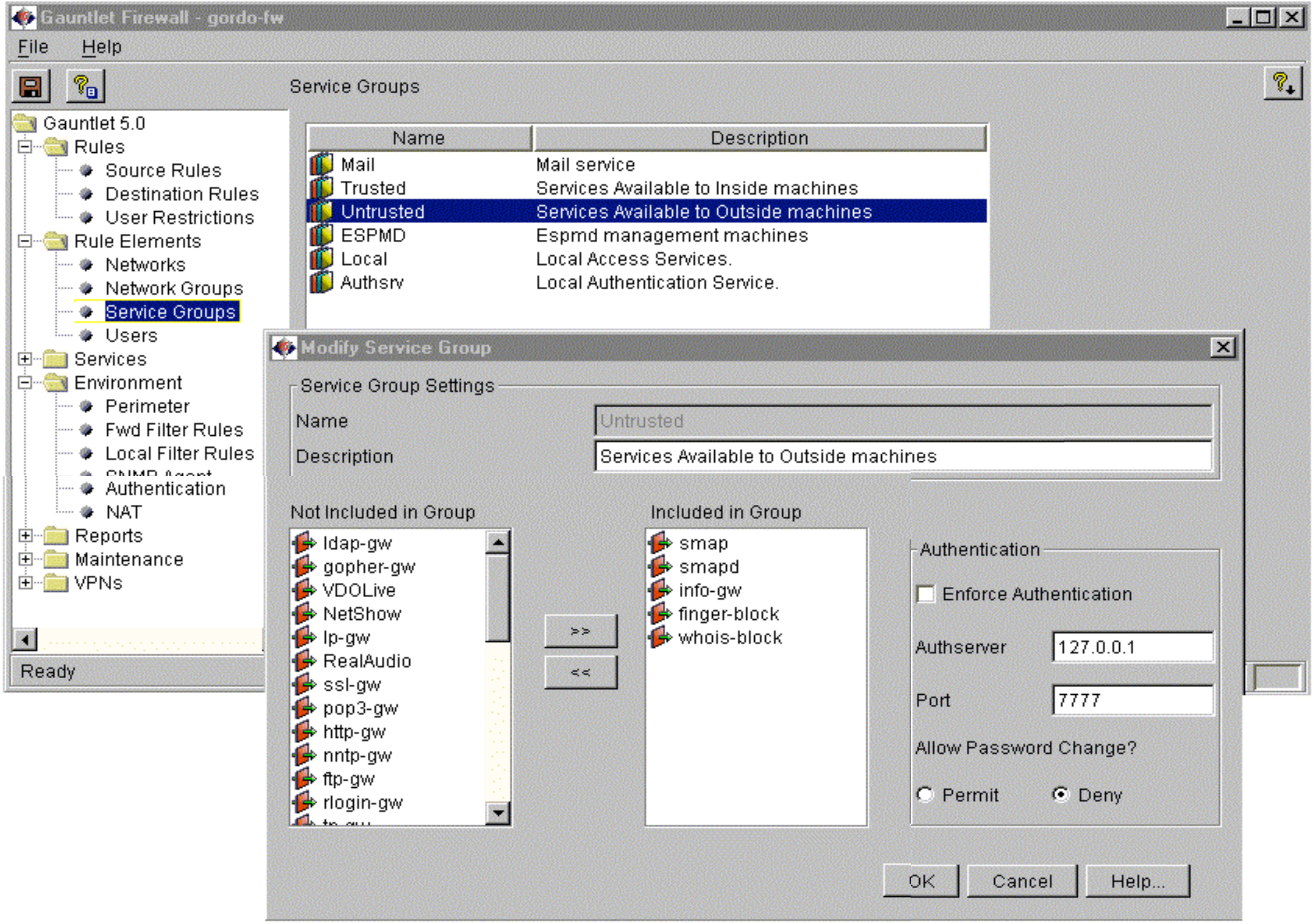


Solution Design



Boundary Servers Network Client Workstation User

Firewall



Service Groups

Name	Description
Mail	Mail service
Trusted	Services Available to Inside machines
Untrusted	Services Available to Outside machines
ESPMD	Espmd management machines
Local	Local Access Services.
Authsrv	Local Authentication Service.

Service Group Settings

Name: Untrusted

Description: Services Available to Outside machines

Not Included in Group:
- ldap-gw
- gopher-gw
- VDOLive
- NetShow
- lp-gw
- RealAudio
- ssl-gw
- pop3-gw
- http-gw
- nntp-gw
- ftp-gw
- rlogin-gw
- tn-gw

Included in Group:
- smap
- smapd
- info-gw
- finger-block
- whois-block

Authentication

□ Enforce Authentication

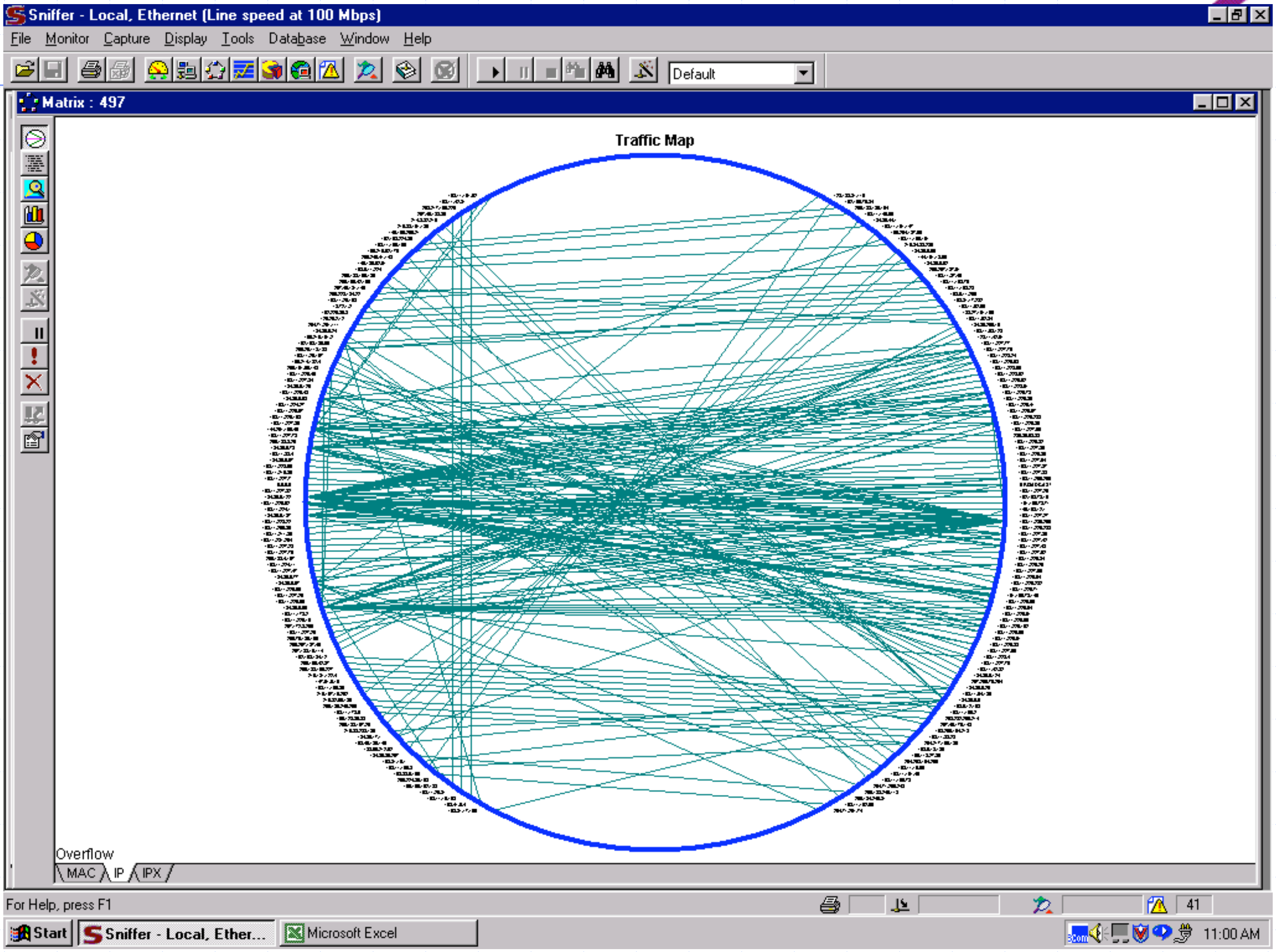
Authserver: 127.0.0.1

Port: 7777

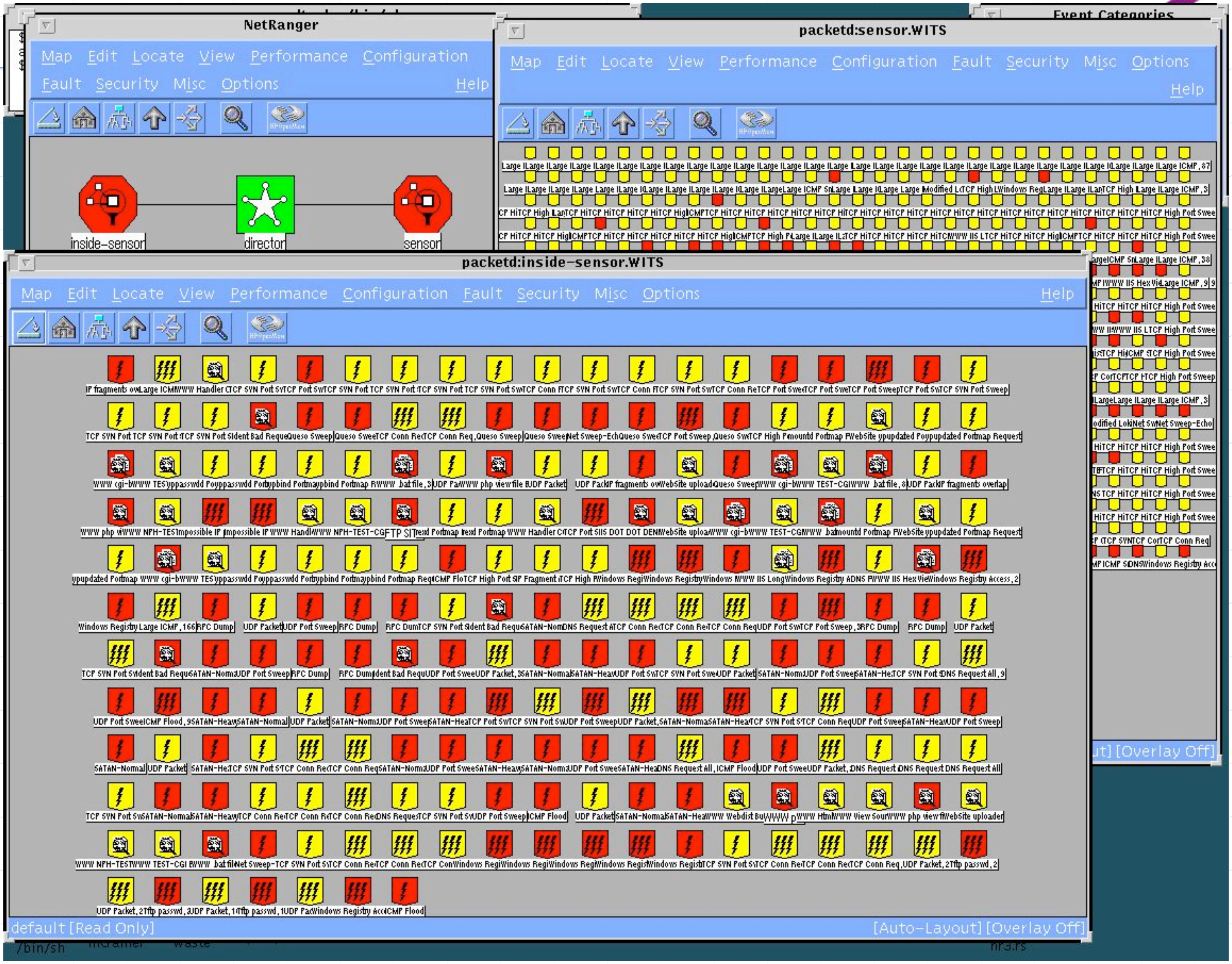
Allow Password Change?

○ Permit ● Deny

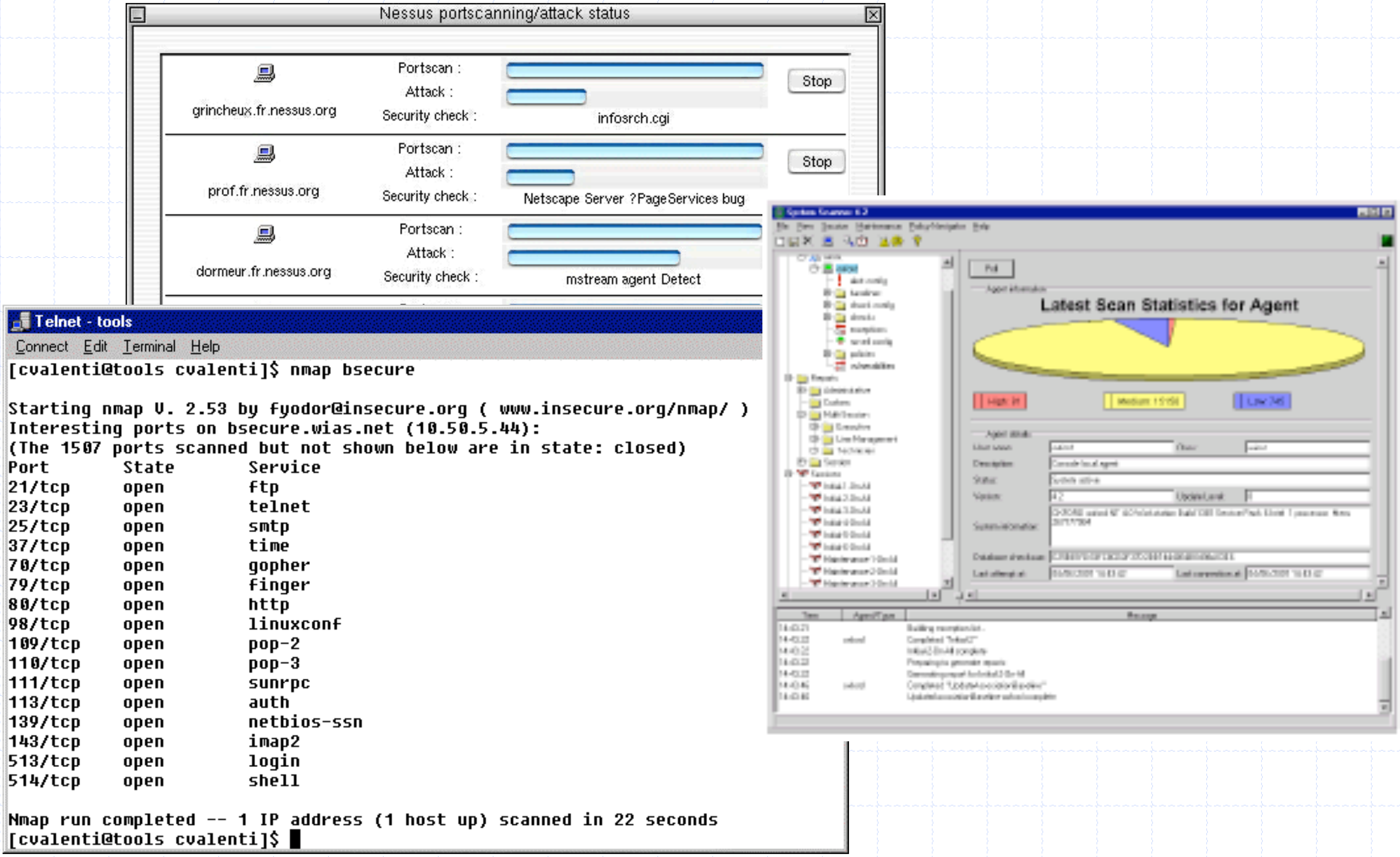
Network Discovery



Intrusion Detection


NetRanger
Map Edit Locate View Performance Configuration
Fault Security Misc Options Help
inside-sensor
director
sensor
packetd:sensor.WITS
Map Edit Locate View Performance Configuration Fault Security Misc Options
Help
Event Categories
packetd:inside-sensor.WITS
Map Edit Locate View Performance Configuration Fault Security Misc Options Help
default [Read Only]
[Auto-Layout] [Overlay Off]
/bin/sh

Vulnerability Scanning



grincheux.fr.nessus.org
Portscan :
Attack :
Security check : infosrch.cgi

prof.fr.nessus.org
Portscan :
Attack :
Security check : Netscape Server ?PageServices bug

dormeur.fr.nessus.org
Portscan :
Attack :
Security check : mstream agent Detect

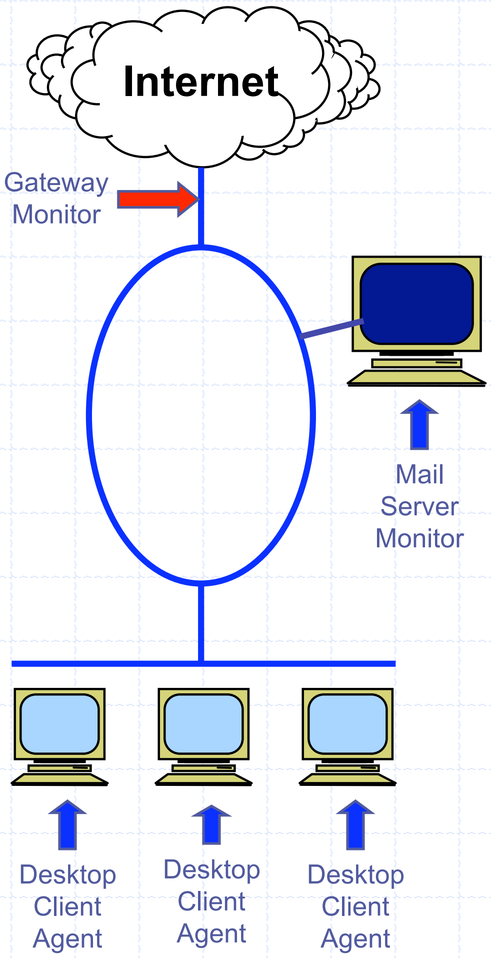
```
[cvalenti@tools cvalenti]$ nmap bsecure

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on bsecure.wias.net (10.50.5.44):
(The 1507 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
37/tcp     open        time
70/tcp     open        gopher
79/tcp     open        finger
80/tcp     open        http
98/tcp     open        linuxconf
109/tcp    open        pop-2
110/tcp    open        pop-3
111/tcp    open        sunrpc
113/tcp    open        auth
139/tcp    open        netbios-ssn
143/tcp    open        imap2
513/tcp    open        login
514/tcp    open        shell

Nmap run completed -- 1 IP address (1 host up) scanned in 22 seconds
[cvalenti@tools cvalenti]$ █
```

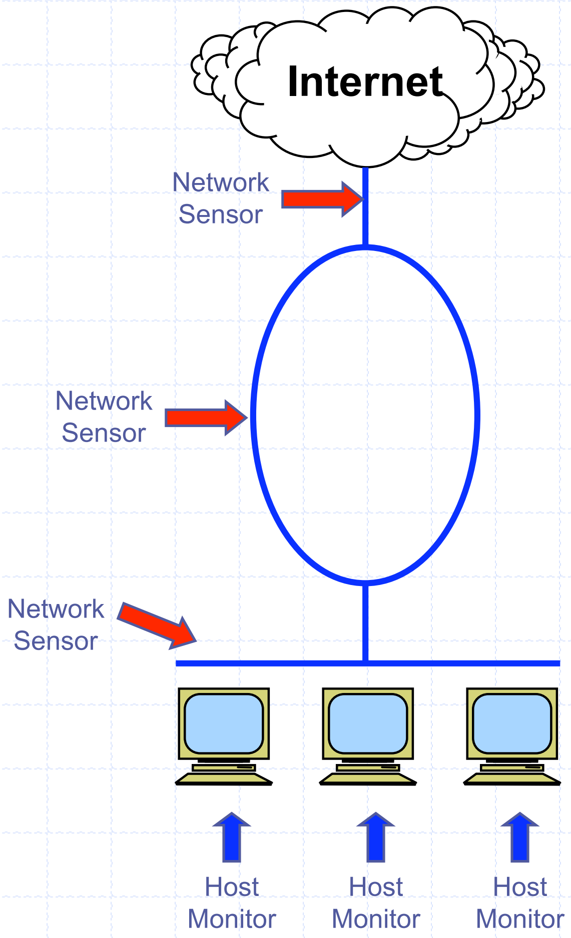
Anti-Virus Architecture

- **Integrating network and host protection provides layers of defense**
- **External Gateways:**
  - Inspection and detection of traffic
- **Mail Server:**
  - Virus detection and quarantine
- **Client agent:**
  - Desktops protection



Intrusion Detection Architecture

- Integrating network and host monitoring can provide the best of both approaches
- Network sensors at:
  - External gateways
  - Backbones
  - Server Subnets
- Host sensors on:
  - Critical servers
  - Potential targets

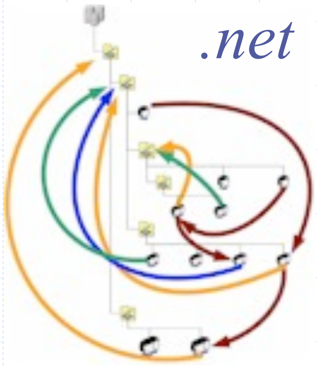


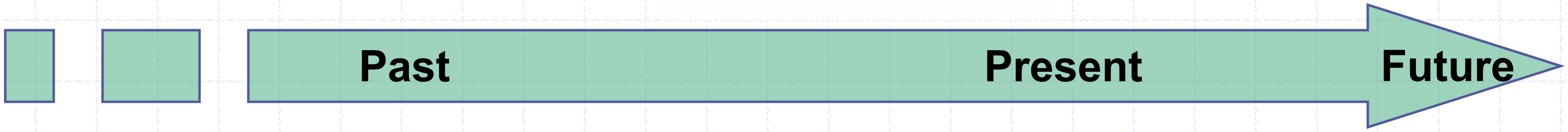
Challenges for Large Enterprises

- **Landscape Discovery**
  - Network topology
  - Role of legacy systems, services and users
  - Constraints of communications infrastructure
- **Dealing with Change**
  - Maintaining compatibility
  - Data center versus distributed computing base
- **Controlling Access**
  - Enabled extranet operations
  - Sharing information with partners and customers
  - Protecting intranet
- **Scalability**
  - Implementing security across a large enterprise
  - Supporting required user services
  - Maintaining cost-effective operations

Dealing with Change

- **Change Introduces new exposures**
- **Requires new approaches and new technologies**
  - Evolving Computing Models
  - Transitiona from Data Center to Distributed Computing to internet applications
  - Wireless & Mobile Computing
  - Collaborative services

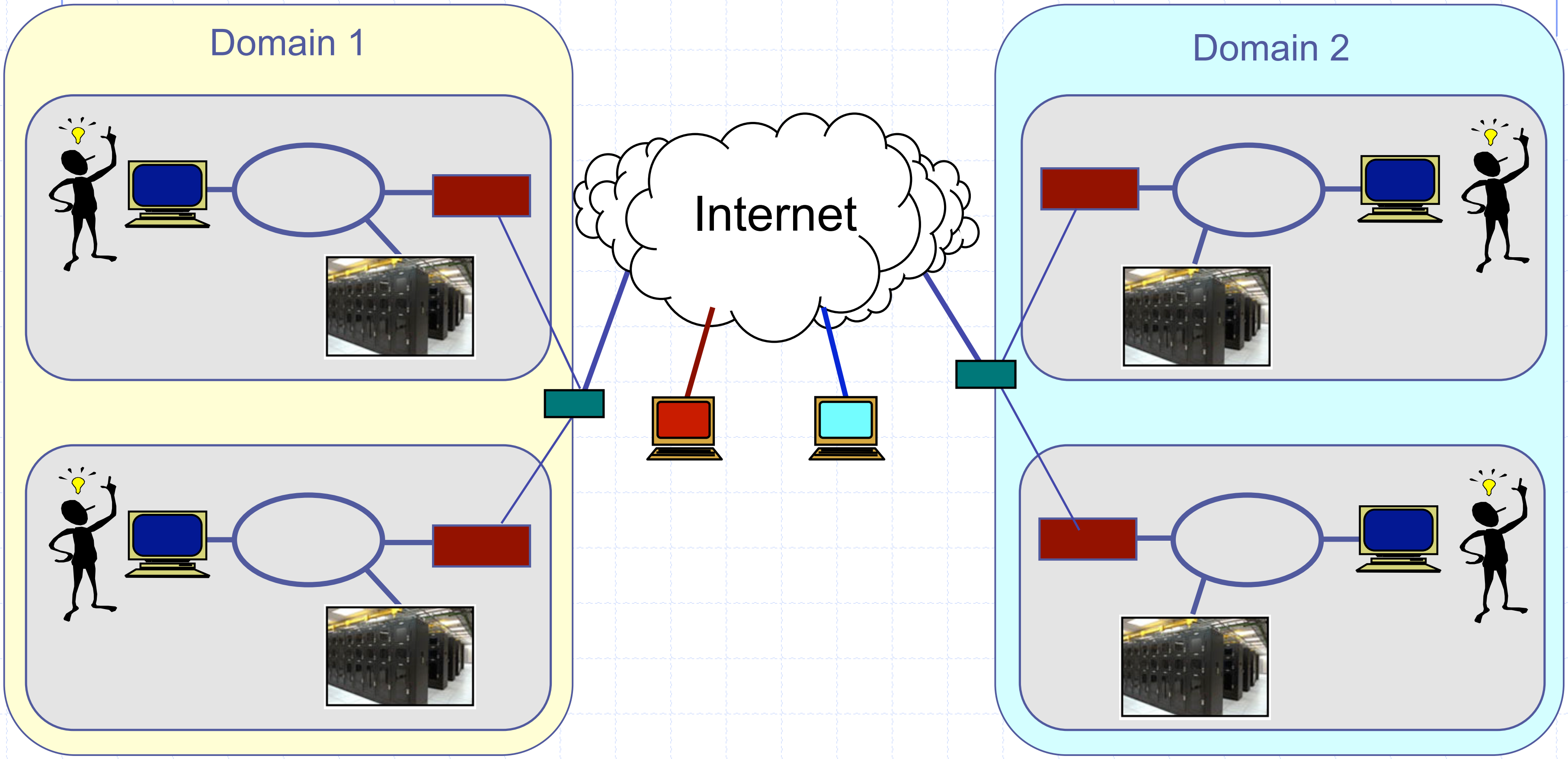




Time

Controlling Access

- *Supporting overlapping Communities of Interest*



Scalability

- **Network-based components**
  - Leverage network to distribute services to all connected users
- **Host-based components**
  - Where visibility and access is required to individual workstations
  - Requires administration of client configurations
- **Managed Services**
  - Outsourced operational support solutions