SANS INSTITUTE

ROADMAP To Security Tools & Services

5th EDITION SUMMER 2001

To order your free white papers and get more information
www.sans.org/tools.htm

PentaSafe
www.pentasafe.com

Solutionary
reliable, responsible e-security
www.solutionary.com

infoExpress
www.infoexpress.com

netForensics.com
www.netforensics.com

XYPRO
www.xypro.com

NSEC
NETWORK SECURITY CORP.
www.networksecuritycorp.com

ubizen
we secure e-business.
www.ubizen.com

Network I·C·E
www.networkice.com

netIQ
www.netiq.com

CHECK POINT
Software Technologies Inc.
We Secure the Internet.
www.checkpoint.com

CONSUL
risk management
www.consul.com

WP WHITE PAPERS

PentaSafe
Building a "human firewall" to protect information assets.

Solutionary, Inc.
How to Protect Information: A Comprehensive Guide to Securing Networks and Systems.

InfoExpress, Inc.
Enforcing Security Policies for Remote Users.

netForensics
Web Security Takes a Seat in the Boardroom.

XYPRO Technology
Securing NSK Communications with Software Based Encryption.

Network Security Corp
Managed Intrusion Detection: Monitoring and Detecting Malicious Activity.

Network ICE Corp.
Protocol Analysis vs Pattern Matching.

NetIQ Corporation.
Step by Step Guide to Selecting the Right Security Solution.

Check Point Software
Why Choose Integrated VPN/Firewall Solutions over Stand-alone VPNs?

CONSUL Risk Management
Securing the Enterprise.

1 Active Content Monitoring / Filtering

Once connected to the internet, an individual or organization undertakes a degree of risk from computer viruses, malicious Java or Active-X, and more. Tools that perform active content monitoring examine material entering a computer/network for potentially damaging content, cross-referencing what they scan with continuously updated definition libraries. The impacts of allowing malicious content to enter a network unchallenged can vary from suffering mild annoyances to extended network downtime and loss of stored material.

Some Of The Tools

- WP SuperScout Email Filter – SurfControl, Inc.
- WP SuperScout Web Filter – SurfControl, Inc.
- v-Go Single Sign-On – Passlogix, Inc.
- WebShield for Nokia Appliance – Nokia
- NetSecure Mail – NetSecure Software
- ConsoleServer 3200 – Lightwave Communications
- Pelican SafeTnet – Pelican Security
- Sendmail Secure Switch – Sendmail, Inc.
- Trend InterScan VirusWall – Trend Micro

2 Intrusion Detection – Host Based

A host-based intrusion detection system is software that monitors a system or application' log files. It responds with an alarm or a countermeasure when a user attempts to gain access to unauthorized data, files or services.

Some Of The Tools

- WP VigilEnt Security Agents for W2K, NT, UNIX and iSeries/AS400 – PentaSafe, Inc.
- WP ActiveGuard – Solutionary, Inc.
- WP ManTrap – Recourse Technologies, Inc.
- WP Tripwire for Servers – Tripwire, Inc.
- WP XYGATE Merged Audit – XYPRO Technology
- WP NFR (HIP) Host Intrusion Protection – NFR Security
- WP Security Manager – NetIQ Corporation
- WP Entercept – Entercept Security Technologies
- CyberWallPLUS – Network-1 Security Solutions
- Intruder Alert – Symantec
- Harvester – farm9.com
- RealSecure – ISS
- Centrax – CyberSafe Corporation
- PReCis - Insession Technologies

3 Firewalls

A firewall is a system or group of systems that enforces an access control policy between two networks.

Some Of The Tools

- WP CyberGatekeeper – VPN Policy Enforcer – InfoExpress, Inc.
- WP CyberArmor – Enterprise Personal Firewall – InfoExpress, Inc.
- WP SuperScout for Check Point Firewall-1 -SurfControl, Inc.
- WP SuperScout for Microsoft ISA Server -SurfControl, Inc.
- WP BlackICE Defender – Network ICE Corp.
- WP VPN-1 SecureServer – Check Point Software
- WP FireWall-1 Gateway – Check Point Software
- WP PGP Gauntlet Firewall – PGP Security
- Raptor Firewall with Power VPN – Symantec
- Personal Ravlin II – RedCreek Communications
- CyberWallPLUS – Network-1 Security Solutions
- Nokia Firewall/VPN Appliance – Nokia
- Norman Personal Firewall – Norman Data Defense Systems
- ZoneAlarm – Zone Labs
- Tiny Personal Firewall – Tiny Software
- Cisco Secure Pix Firewall – Cisco Systems
- Praesidium eFirewall – Hewlett Packard
- WatchGuard LiveSecurity System – WatchGuard Technologies
- SunScreen – Sun Microsystems
- Sidewinder – Secure Computing
- Lucent Managed Firewall – Lucent Technologies

To order your free white papers and get more information
www.sans.org/tools.htm

4 Intrusion Detection – Network Based

A network-based intrusion detection system monitors network traffic and responds with an alarm when it identifies a traffic pattern that it deems to be either a scanning attempt or a denial of service or other attack. It is quite useful in demonstrating that "bad guys" are actually trying to get into your computers.

Some Of The Tools

- WP ActiveGuard – Solutionary, Inc.
- WP ManHunt – Recourse Technologies, Inc.
- WP NFR (NID) Network Intrusion Detection – NFR Security
- WP BlackICE Sentry – Network ICE Corp.
- WP Check Point RealSecure – Check Point Software
- snort – Marty Roesch
- NetProwler – Symantec
- RealSecure – ISS
- SecureNet Pro – Intrusion.com
- Harvester – farm9.com
- RealSecure for Nokia – Nokia
- Dragon IDS – Enterasys Networks
- Anzen Flight Jacket for NFR – Anzen Computing
- Centrax – CyberSafe Corporation
- Cisco Secure Intrusion Detection System – Cisco Systems
- Shadow – The SANS Institute
- OpenView Node Sentry – Hewlett Packard

5 Authorization

Authentication answers the question of "Who are you?" whereas Authorization addresses the question of "Are you allowed to do that?" Policy-based authorization servers allow applications, usually web servers. an ability to centralize authentication and authorization tasks. A Security Manager defines authentication methods (e.g. passwords) users and access controls. Each time a user wishes to access a resource the application queries the authorization server, which refers to the policies and rules to answer the query.

Some Of The Suppliers

- WP XYGATE Encrypted FTP – XYPRO Technology
- WP XYGATE Access Control – XYPRO Technology
- WP MultiSecure Web/Guard – Ubizen, Inc.
- WP VACMAN Enterprise – VASCO
- Elara Suite – Transindigo
- GetAccess – enCommerce
- Authentor – Sentry Systems
- ClearTrust SecureControl – Securant Technologies
- Conclave / ReD I-Policy – RedCreek Communications
- SecureWay Policy Director – Tivoli
- DomainGuard – Hewlett Packard

6 Air Gap Technology

These hardware/software systems enable realtime data transfer between the Internet and back end systems, without opening holes in the firewall. Often Air Gap solutions enforce a physical disconnection between the production network and the outside world. They terminate all networking protocols, restricting access to application-layer data only, and perform application-specific content inspection behind the Air Gap.

Some Of The Tools

- e-Gap – Whale Communications
- Secure Directory File Transfer System – Owl Computing
- 2-in-1-PC – Voltaire Advanced Data Security
- Stop-It – RVT Technologies
- AirGap – Spearhead Technologies
- SecureSwitch – Market Central

7 Network Authentication

These tools take several approaches to improving the ability of you systems to differentiate between people who should and should not have access..

Some Of The Tools

- WP XYGATE Access Control – XYPRO Technology
- WP VACMAN Enterprise – VASCO
- Defender – Symantec
- Syntax Enterprise Services – Syntax
- TrustBroker – CyberSafe Corporation
- Cisco Secure Access Control Server – Cisco Systems

8 Security Appliances

These hardware/software combinations offer firewall and, sometimes, other services such as network load management, in a single purpose offering. Because they have very limited operating system functions, they are generally easier to manage, cheaper, and less subject to common hacker attacks than firewalls installed on general purpose UNIX or Windows NT computers.

Some Of The Tools

- WP NFR (SLR) Secure Log Repository – NFR Security
- WP PGP Gauntlet e-ppliances – PGP Security
- Dragon Appliance – Enterasys Networks
- Ravlin VPN Gateways – RedCreek Communications
- SecureCom PDS – Intrusion.com
- VelociRaptor – Symantec
- Resilience Continuous Availability Platform – Resilience
- SecureCom 8001 – Intrusion.com
- Nokia Firewall/VPN Appliance – Nokia
- Radguard – Radguard
- WebShield for Nokia Appliance - Nokia

9 Security Services: Penetration Testing

Consulting organizations simulate real-world hacking and social engineering attacks on an enterprise's network and systems to determine where weaknesses lie, and offer advice on how those weaknesses may be addressed in order to beef up security. Most use network-based vulnerability scanning tools listed elsewhere on this chart.

Some Of The Tools

- WP ActiveGuard – Solutionary, Inc.
- WP Penetration Testing – Network Security Corp.
- WP Web Application Testing – Network Security Corp.
- WP Ubizen Professional Services – Ubizen, Inc.
- WP CONSUL/Consultancy – CONSUL Risk Management
- WP Foundstone Professional Services – Foundstone
- Penetration Testing Services – Collins Consulting Group
- Thresher2 – farm9.com
- Cisco Secure Consulting Services – Cisco Systems
- Deloitte & Touche
- Ernst & Young
- KMPG Peat Marwick
- Lucent NetCare
- Tiger Testing
- IBM Recovery Systems

10 Authentication

Authentication is the process of determining whether someone or something is who or what it is declared to be. The most common form of authentication is the use of logon passwords, the weakness of which is that passwords can often be forgotten, stolen or accidentally revealed. The tokens in this category offer more stringent forms of authentication so that users need to both have something (the token) and know something (the PIN or password) to gain access.

Some Of The Tools

- WP XYGATE Key Management – XYPRO Technology
- WP Digipass – VASCO
- WP PGP E-Business Server – PGP Security
- WP VACMAN RADIUS Middleware – VASCO
- Penetration Testing Services – Collins Consulting Group
- Thresher2 – farm9.com
- Cisco Secure Consulting Services – Cisco Systems
- Deloitte & Touche
- Ernst & Young
- KMPG Peat Marwick
- Lucent NetCare
- Tiger Testing
- IBM Recovery Systems

11 Certificate Authority

A CA (Certificate Authority) is an organization that issues and manages security credentials and public keys for message encryption and decryption. This is an essential part of a public key infrastructure (PKI) because it manages the process of issuing and verifying the certificates used to grant people and systems access to other systems. These certificates include keys which help to strengthen authentication, privacy and non-repudiation.

Some Of The Tools

- VeriSign – VeriSign
- Norman Security Suite – Norman Data Defense Systems
- Mobile Trust – Certicom Corp.
- RSA Keon Certificate Server – RSA Security

12 File & Session Encryption

Encryption is a process through which data is transferred into a form whereby it cannot easily be intercepted and understood by unauthorized persons. Sophisticated computer algorithms are used to encrypt the files, then decrypt them when they are needed.

Some Of The Tools

- WP XYGATE Secure Client – XYPRO Technology
- WP XYGATE File Encryption – XYPRO Technology
- WP Stonegate – Stonesoft
- WP PGP Corporate Desktop – PGP Security
- PrivateArk Network Vault – Cyber-Ark Software
- f-Secure Filecrypto – Data Fellows
- Everlink Suite – Anyware Technology
- Norman Security Suite – Norman Data Defense Systems
- Security Builder – Certicom Corp.
- Safelan – G.T.G.I.

13 VPNs & Cryptographic Communications

A VPN or Virtual Private Network allows secure communications over the public internet. It saves money in organizations with large mobile workforces or many satellite offices reducing the need to use expensive private telephone networks.

Some Of The Tools

- WP VTCP/Secure Remote VPN/Extranet Solution – InfoExpress, Inc.
- WP Stonegate – Stonesoft
- WP VPN-1 – Check Point Software
- WP VPN-1 Secure Client – Check Point Software
- f-Secure VPN+ - Data Fellows
- SmartGate VPN – V-One
- Nokia Firewall/VPN Appliance – Nokia
- Ravlin VPN Gateways – RedCreek Communications
- Raptor Firewall with Power VPN – Symantec
- PPTP-RAS – Microsoft
- Cisco Secure Integrated VPN – Cisco Systems
- Defensor – CyberSafe Corporation

14 Secure Web Servers

These tools offer web services in environments that have been engineered to minimize the number of security holes.

Some Of The Tools

- WP VigilEnt Security Agents for Web Servers – PentaSafe, Inc.
- WP Tripwire for Web Pages – Tripwire, Inc.
- WP MultiSecure Web/Guard – Ubizen, Inc.
- WP StoneBeat WebCluster – Stonesoft
- WP Stonegate – Stonesoft
- WP VACMAN Enterprise – VASCO
- WP Security Manager – NetIQ Corporation
- WP Entercept – Entercept Security Technologies
- SecureStack – SecureWave
- NetSecure Web – NetSecure Software
- Webthority – Symantec
- CyberWallPLUS – Network-1 Security Solutions

15 Single Sign-On

These software packages allow users to get access to multiple computers and applications without learning many different passwords. Single sign-on tools generally do not change the underlying applications, but hide their differences through a layer of software.

Some Of The Tools

- WP MultiSecure Web/Guard – Ubizen, Inc.
- WP VACMAN Enterprise – VASCO
- Focal Point – Okiok Data
- Global Sign-On – IBM
- ReD 1-Access – RedCreek Communications
- Secure Single Sign-On – Systor Security Solutions
- TrustBroker – CyberSafe Corporation
- v-Go Single Sign-On – Passlogix, Inc.
- Norman Access Control – Norman Data Defense Systems

16 Web Application Security

Web application security is the protection of your web application and its resources from threats coming from the internet, such as stealing company assets, falsifying buy/sell transactions, getting private customer data and defacing the site. This is done by detecting and/or preventing the hacking techniques applicable to this domain, i.e. those which can be performed in the presence of firewalls and encryption.

Some Of The Tools

- WP VigilEnt Security Agents for BEA WebLogic – PentaSafe, Inc.
- WP Tripwire for Web Pages – Tripwire, Inc.
- WP MultiSecure Web/Guard – Ubizen, Inc.
- WP VACMAN Enterprise – VASCO
- WP Security Manager – NetIQ Corporation
- WP User Authority – Check Point Software
- WP Foundstone Professional Services – Foundstone
- WP Entercept – Entercept Security Technologies
- Appshield – Sanctum, Inc.
- CONTROL-SA – BMC Software
- AppScan – Sanctum, Inc

Some Of The Tools

Security Alert Consensus

SANS in collaboration with Network Computing now offers a definitive weekly summary of new alerts and counter-measures with announcements from: SANS, CERT, the Global Incident Analysis Center, the National Infrastructure Protection Center, the Department of Defense, Security Portal, Ntbugtraq, Sun and several other vendors. When you subscribe, by selection only the operating systems you support, you will receive a version of Security Alert Consensus tailored and customized to you needs.

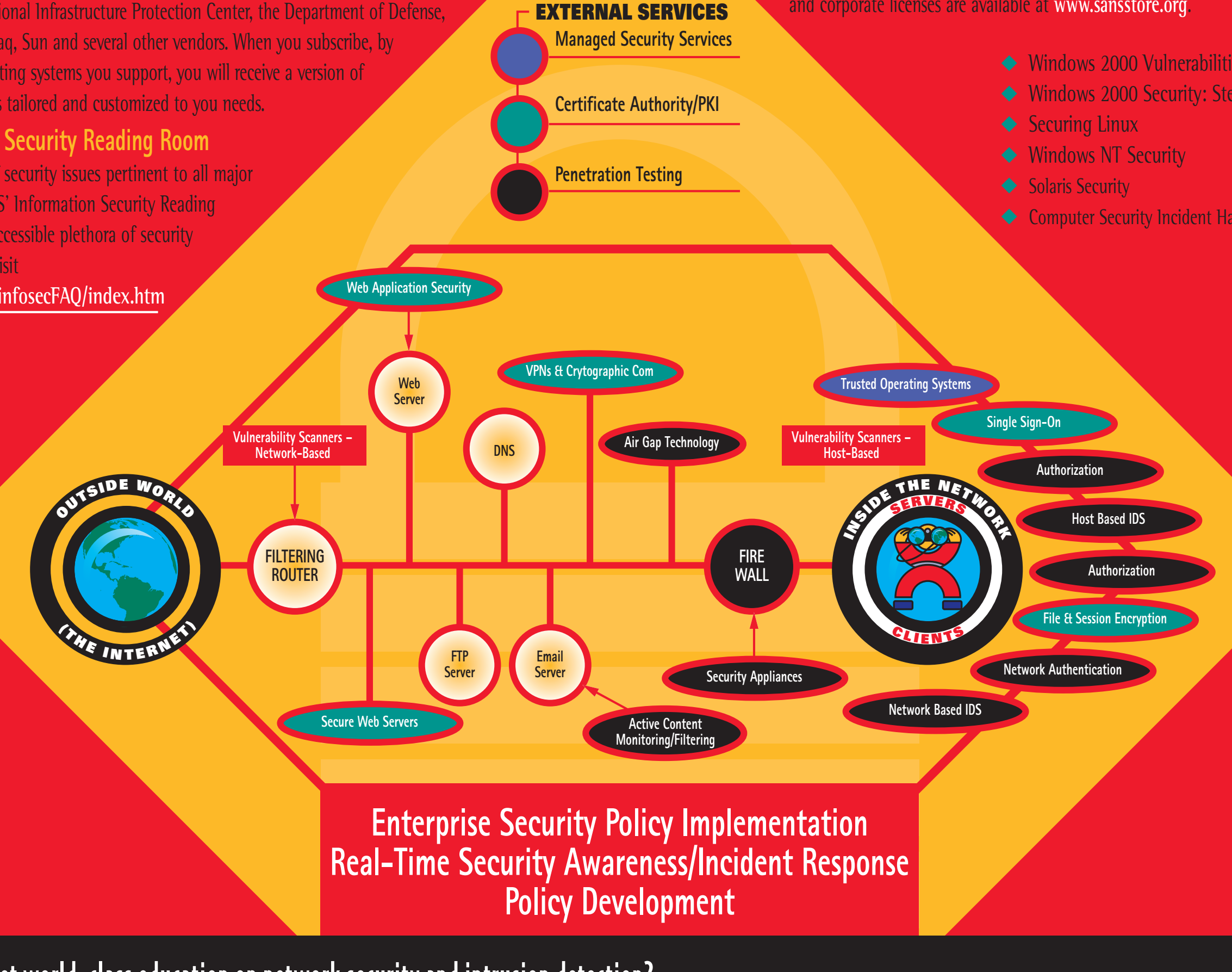
SANS Information Security Reading Room

Covering a vast array of security issues pertinent to all major operating systems, SANS' Information Security Reading Room offers a readily accessible plethora of security knowledge and news. Visit
http://www.sans.org/infosecFAQ/index.htm

SANS Consensus Research Documents

The industry's most experienced practitioners share their real-world knowledge to produce step-by-step guides to harden operation systems and solve other common security problems. More than 145 large and small user organizations participated in their creation and updating Individual and corporate licenses are available at www.sansstore.org.

- Windows 2000 Vulnerabilities and Solutions
- Windows 2000 Security: Step by Step
- Securing Linux
- Windows NT Security
- Solaris Security
- Computer Security Incident Handling



Enterprise Security Policy Implementation
Real-Time Security Awareness/Incident Response
Policy Development

Where do you get world-class education on network security and intrusion detection?

SANS Parliament Hill
Ottawa, Canada
August, 8-18, 2001

New England SANS
Boston, Mass.
September 5 -12, 2001

Network Security 2001
San Diego, CA
October 15-22, 2001

North Pacific SANS
Vancouver, Canada
November 15-20, 2001

SANS Cyber Defense Initiative - West Coast
San Franscisco
December 16-21, 2001

St. Johns SANS
Jacksonville, FL
August 20-25, 2001

SANS Scandinavia
Stockholm, Sweden
September 23-28, 2001

Great Lakes SANS
Chicago, Illinois
November, 5-10, 2001

SANS Cyber Defense Initiative - East Coast
Washington, DC
November 27-December 3, 2001

For additional event information and dates, go to:
http://www.sans.org

17 Vulnerability Scanners: Network Based

Software that simulates the behavior of attackers to learn which of as many as 600 possible weaknesses are present on the system being attacked.

Some Of The Tools

- WP ActiveGuard – Solutionary, Inc.
- WP bv-Control for Internet Security – BindView Corp.
- WP Security Analyzer – NetIQ Corporation
- WP CyberCop Scanner – PGP Security
- SAINT - World Wide Digital Security, Inc.
- Nmap – Fyodor
- SATAN – Wietsa Venema & Dan Farmer
- Internet Scanner – ISS
- NetRecon – Symantec
- Thresher – farm9.com
- NetSonar – Cisco Systems
- Nessus – Renaud Deraison & Jordan Hrycaj

18 Vulnerability Scanners – Host Based

These tools check the settings on our systems to determine whether they are consistent with corporate security policies. They are often used by auditors.

Some Of The Tools

- WP VigilEnt Security Agents for Windows 2000/NT, UNIX and AS/400 (iSeries) – PentaSafe, Inc.
- WP ActiveGuard – Solutionary, Inc.
- WP bv-Control for Windows 2000 & Active Directory, Novell NetWare, NDS/eDirectory, UNIX and OS/400 – BindView Corp.
- WP Security Analyzer – NetIQ Corporation
- WP CONSUL/zAudit – CONSUL Risk Management
- COPS – Dan Farmer
- Security Configuration Manager – Microsoft
- System Scanner – ISS
- SecurityAnalyst – Intrusion.com
- Database Scanner – ISS

19 Real-Time Security Awareness / Incident Response

RTSA allows the security manager to see what is happening across the enterprise among multiple vendor security products and sources in near real-time from a central console. RTSA helps reduce the number of personnel whose time must be devoted to monitoring multiple security products and sources.

Some Of The Tools

- WP VigilEnt Security Manager – PentaSafe, Inc.
- WP ActiveGuard – Solutionary, Inc.
- WP Incident Response – Network Security Corp.
- WP NetForensics – netForensics.com
- WP bv-Control Risk Management Suite – BindView Corp.
- WP Tripwire for Web Pages – Tripwire, Inc.
- WP SecurityWatch.com – Ubizen, Inc.
- WP Security Manager – NetIQ Corporation
- WP CONSUL/eAudit (CeA) – CONSUL Risk Management
- WP Foundstone Professional Services – Foundstone
- SCORPIAN – Security Automation, Inc.
- ISS Emergency Response Services – ISS
- CONTROL-SA – BMC Software
- Open e-Security Platform – e-Security, Inc.

20 Enterprise Security Policy Implementation

EPSI enables security managers to automate each step of security policy management from a central console including creating, editing, approving, publishing, distribution, education, compliance, reporting and maintenance. These tools enforce awareness, assess employee understanding, track incidents and measure compliance, which helps organizations improve management of IT risks without overburdening limited staff.

Some Of The Tools

- WP VigilEnt Policy Center – PentaSafe, Inc.
- WP Tripwire Manager – Tripwire, Inc.
- WP MultiSecure Web/Guard – Ubizen, Inc.
- WP ePolicy Orchestrator – PGP Security
- Living Policy – Intellitactics, Inc.

21 Enterprise Security Administration

Tools providing enterprise-wide security administration apply a given security policy across and entire organization, ensuring all users of that enterprises network will be subjected to the same rights and restrictions. These systems are especially valuable in grating new users access to all appropriate systems and, more importantly, removing users from all systems if they are terminated.

Some Of The Tools

- WP VigilEnt Security Manager – PentaSafe, Inc.
- WP CONSUL/eAudit (CeA) – CONSUL Risk Management
- WP CONSUL/zAudit – CONSUL Risk Management
- WP CyberGatekeeper – VPN Policy Enforcer – InfoExpress, Inc.
- WP bv-Control Risk Management Suite – BindView Corp.
- WP NetForensics – netForensics.com
- WP Stonegate – Stonesoft
- WP ICEcap Manager – Network ICE Corp.
- WP VACMAN Enterprise – VASCO
- WP File & Storage Administrator – NetIQ Corporation
- WP Directory & Resource Administrator – NetIQ Corporation
- Trend Virus Control System – Trend Micro
- SAFEsuite Decisions – ISS
- Enterprise Security Manager – Symantec
- RedCreek e-Director – RedCreek Communications
- Symark PowerBroker – Symark Software

22 Managed Security Services

Vendors providing managed security services assume a percentage of the security administration tasks for an enterprises' network, allowing administrators to concentrate on other job responsibilities.

Some Of The Tools

- WP ActiveGuard – Solutionary, Inc.
- WP Managed Firewall – Network Security Corp.
- WP Managed IDS – Network Security Corp.
- WP OnlineGuardian – Ubizen, Inc.
- WP Provider-1 – Check Point Software
- WP Sitemanager-1 – Check Point Software
- WP FoundScan – Foundstone
- WP PGP Firewall MSP – PGP Security
- WP CONSUL/Managed Security Monitoring – CONSUL Risk Management
- Vigilinx
- OneSecure
- Riptech, Inc.
- SANS Institute
- Veritect
- DefendNet
- SecureWorks
- Counterpane
- Ignyte
- XO
- Guardent
- TruSecure
- Securify

23 Security Services: Policy Development

Consulting organizations that have worked with many organizations have templates with which they can quickly establish for all aspects of computer security from acceptable use to email to extranets to PKI.

Some Of The Tools

- WP Information Security Policies Made Easy: Reference Library – PentaSafe, Inc.
- WP ActiveGuard – Solutionary, Inc.
- WP XYPRO Services – XYPRO Technology
- WP Security Policy Development – Network Security Corp.
- WP Security Policy Review – Network Security Corp.
- WP Foundstone Professional Services – Foundstone
- WP CONSUL/Managed Security Monitoring – CONSUL Risk Management
- WP CONSUL/Consultancy – CONSUL Risk Management
- Accenture
- PricewaterhouseCoopers
- Ernst & Young

24 Trusted Operating Systems

Because all other security mechanisms rely on the operating system, they can be disabled or circumvented by a successful attack on the o/s. Trusted o/s technology provides the only mechanism to protect the o/s itself from successful attack.

Some Of The Tools

- PrivateArk Network Vault – Cyber-Ark Software
- SecureEXE – SecureWave
- Nokia IPSO – Nokia
- Pitbull – Argus Systems Group
- Virtual Vault – Hewlett Packard

Recourse Technologies
www.recourse.com • 1-877-786-9633 • info@recourse.com
www.recourse.com

BIND VIEW
www.bindview.com

TRIPWIRE
www.tripwire.com

SurfControl
The Filtering Company
www.surfcontrol.com

NFR SECURITY
www.nfr.com

STONESOFT
Enabling the Secure, Highly Available Enterprise
www.stonesoft.com

VASCO
www.vasco.com

FOUNDSTONE
KNOW VULNERABILITIES
www.foundstone.com

PGP SECURITY
A Network Associates Company
www.pgp.com

entercept
SECURITY TECHNOLOGIES
www.entercept.com

WHITE PAPERS WP

Recourse Technologies
Securing your network infrastructure with threat management solutions.

BindView Corporation.
2001 - The Quest for Understanding Security Management.

Tripwire, Inc.
Data & Network Integrity (DNI)-Technology to Invoke Trust in IT - The Tripwire Solution, An IDC White Paper.

SurfControl, Inc.
Managing and Minimizing Email Risks.

NFR Security
Intrusion Detection Coverage: When to look at hosts and when to look at wires.

Stonesoft, Inc.
Enabling Your Business with a High Availability Enterprise Firewall.

Ubizen, Inc.
Securing e-Business at the Application-Level.

VASCO
Transparent, Strong Authentication Using Auto-Managed RADIUS Middleware.

Foundstone
Hands-On Incident Response for Windows.

PGP Security
Finding Your Way Through the VPN Maze: Making Sense of the Emerging VPN Market.

Entercept Security Technologies
The Future of Web Server Security.