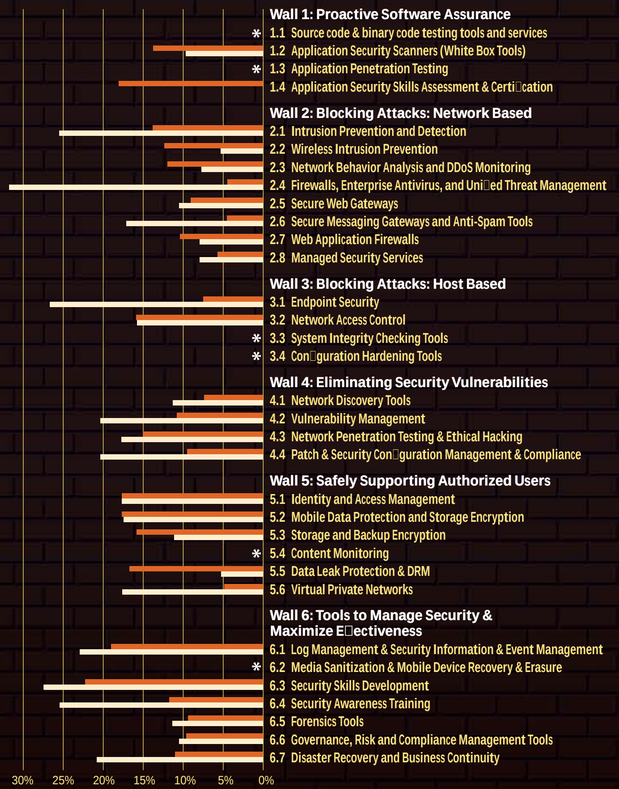
What Tools Are Growing?



Fall 2008 – 17th Edition

SANS WhatWorks™ In Internet Security

Six Defensive Walls for a Layered Approach to Security

&

Cyber Attack Threat Map

Here's what you have to defend against

(On reverse side)

SANS

SANS is the most trusted and by far the largest source for information security training certification and research in the world.

Gartner

The Leader in Research and Analysis on the Global IT Industry

Note: Gartner's John Pescatore helped shape the categories and the thinking behind the WhatWorks poster. Selection of WhatWorks products and recorded interviews with users are entirely the work of the SANS Institute.

www.sans.org/whatworks

SANS WhatWorks™ In Internet Security

SIX DEFENSIVE WALLS for a Layered Approach to Security

For hands-on courses covering how to make many of these technologies effective, see www.sans.org

Security pros recognize the need for a layered approach to security, but not everyone knows which technologies result in a comprehensive defensive posture. The SANS WhatWorks user-to-user program lets you learn from actual users of security products before talking to vendors. Don't risk buying a security product that doesn't work. Start your search at the WhatWorks website to find a list of proven tools that will help your organization build and maintain the six defensive walls. www.sans.org/whatworks

WW You can hear users talk about how this product actually works by visiting www.sans.org/whatworks

- Users of this vendor's products have described their successes at SANS WhatWorks Summits.
- No users have come forward to explain why these products work so well and should be on their short list.

Visit the *SANS Buyers Guide for INFOSEC Professionals* for more information about these WhatWorks ™ vendors and other solutions.

DEFENSIVE WALL 1: Proactive Software Assurance

For full information on best practices in application security, see www.sans-ssi.org

Summary: The application layer is now the number one vector for attackers. However, in most organizations application security is in its infancy and development groups are not yet integrating security into application design and programming. If we want to turn the tide against the attackers, our highest priority must be to help programmers design applications and develop code with fewer security flaws.

1.1 Source Code and Binary Code Testing Tools and Services *(White Box Scanners)*

These tools search through code with the goal of finding potential vulnerabilities.

- Ounce 5
- Fortify 360
- Coverity Prevent
- Klocwork Insight
- Veracode Enterprise Security Review

1.2 Application Security Scanners *(White Box Tools)*

These tools detect common programming errors in Web-based applications and source code. While tools should be part of the solution, skilled humans are the key to doing this job well.

- HP (SPI Dynamics)
- IBM (Watchfire)
- Cenzic Hailstorm

1.3 Application Penetration Testing

In addition to automated tools, traditional penetration testers usually need new skills to do application layer penetration testing.

- Internet Security Systems (now IBM)
- IntelGuardians
- Cigital
- Stach & Liu
- Ernst & Young
- Security Compass
- WhiteHat Sentinel Services

1.4 Application Security Skills Assessment & Certification

Application security managers can ensure that programmers are able to identify and eliminate common security flaws from code by using assessment tools and having outsourced programmers prove their knowledge through certification.

Assessment of Secure Coding Skills through online measurement in Java, C, and .NET (SANS GSSP Assessments)

Certification of Secure Coding Skills in Java, C, and .NET (SANS GSSP Certifications)

DEFENSIVE WALL 2: Blocking Attacks: Network Based

Summary: Although many of the most damaging attacks will come from insiders, malicious traffic from the outside makes up the vast majority of all recorded attacks – and those attacks can be launched from anyone, anywhere in the world. Effective cyber defense starts with technology that makes it very hard for those external attacks to get in.

2.1 Intrusion Prevention (IPS) & Detection (IDS)

IPS and IDS work together – you have to detect something before you can block it. IDS monitors network traffic looking for the characteristics of known attacks. IPS provides high-confidence recognition of the unique characteristics of attack traffic, and blocks it. Its strength over typical stateful firewalls is that IPS can recognize the "content" of network traffic at a high enough rate to block malicious connections and allow legitimate traffic to get through.

WW SourceFire SNORT
WW Lancope StealthWatch
WW NitroSecurity NitroGuard
WW IBM/ISS Proventia & RealSecure
WW StillSecure Strata Guard

- Bradford Software Campus Manager

2.2 Wireless Intrusion Prevention (WIPS)

These tools monitor traffic to and from wireless networks and provide reporting and analysis for compliance.

- Airtight SpectraGuard
- AirDefense Enterprise
- Aruba RFprotect

2.3 Network Behavior Analysis and DDoS Monitoring

These tools monitor traffic looking for patterns that are abnormal and suspicious – especially those that might be associated with denial of service attacks.

WW Lancope StealthWatch
WW Cisco Guard DDos

- Mazu Profiler
- Arbor Peakflow

2.4 Firewalls, Enterprise Antivirus and Unified Threat Management

Firewalls are the first line of defense. Traditional firewalls do not look inside the packets but rely on information in the packet headers: ports, source and destination addresses, and protocol state. Next generation firewalls incorporate traditional firewall functionality with IPS and Web security gateways (anti-malware such as viruses, worms, spyware, etc.)

- CheckPoint VPN-1
- Juniper Netscreen
- Cisco IronPort
- Bluelane's Virtual Shield
- Symantec Endpoint Protection
- TrendMicro Interscan Security Solutions
- Palo Alto PA-4000 Series Firewall

2.5 Secure Web Gateways

Enterprise applications and collaboration systems increasingly use HTTP as the underlying protocol. Secure Web Gateways provide inbound filtering of malware and spyware, as well as outbound URL blocking and other forms of policy enforcement.

WW Secure Computing Webwasher
WW McAfee Secure Web Gateway

- BlueCoat Proxy SG
- Finjan Vital Security Web Appliances
- Iron Port S-Series Web Security Appliances

2.6 Secure Messaging Gateways and Anti-Spam Tools

Spam continues to waste productive time for millions of increasingly angry Internet users. Secure email gateways block inbound spam as well as viruses, worms and other malicious executables and can enforce outbound policy control as well for email and instant messages.

WW Secure Computing Webwasher/SmartFilter

- Webroot E-mail Security SaaS
- Google Postini E-mail Security & Anti-Spam
- Symantec Endpoint Protection
- Sophos ES E-mail Appliances
- TrendMicro Interscan Security Solutions

2.7 Web Application Firewalls

These appliances and software packages block typical attacks against Web applications, while allowing normal user interaction to continue. These products should be used in addition to strong application development security processes, particularly Web application penetration testing and intense training of Web application developers.

2.8 Managed Security Services

MSS ensure that trained eyes are watching the firewalls, IPS and IDS systems, Web security gateways and even the logs from inside systems. They provide rapid analysis and quick notification. More advanced services provide automated vulnerability scanning services, give early warning, and help determine when and where to act to protect against new vulnerabilities and exploits.

WW SecureWorks Professional Services
WW IBM/ISS Professional MSS

- Symantec Managed Security Services
- BT Counterpane Enterprise Protection Suite

DEFENSIVE WALL 3: Blocking Attacks: Host Based

Summary: If an attack gets through the network defenses, the PCs, workstations, and servers should be prepared to stop it or at least minimize the damage. On PCs individual protection products are being replaced by broader endpoint protection platforms that use common engines and management interfaces to provide equivalent or stronger protection with reduced acquisition and operations costs.

3.1 Endpoint Security

Endpoint security includes anti-virus, anti-spyware, personal firewalls, host-based IPS, and related technologies.

- McAfee Endpoint Encryption (formerly Safeboot Encryption)
- Cisco Security Agent
- Symantec Endpoint Protection
- Microsoft Forefront/ Microsoft NAP

3.2 Network Access Control (NAC)

NAC verifies secure configurations and patch levels and should also determine if malicious software is present on an endpoint. Personal computers that do not meet the enterprise standards can be denied access until their configurations have been corrected but more commonly NAC is used to accelerate getting those vulnerabilities remediated.

WW Symantec Sygate NAC
WW StillSecure Safe Access
WW CheckPoint NAC

- Cisco NAC
- Microsoft Network Access Protection

3.3 System Integrity Checking Tools

Checks for unwanted changes to files.

- Tripwire
- AIDE (free)
- Easy Integrity Check System (EICS) (free)

3.4 Configuration Hardening Tools

Tests security configurations for variance from standards.

- Center for Internet Security templates (free)
- Bastille Linux (free)
- Microsoft Baseline Security Analyzer (free)

DEFENSIVE WALL 4: Eliminating Security Vulnerabilities

Summary: Vendors sell software and hardware with vulnerabilities baked in. Your own programmers and system administrators also make mistakes. That means every user organization has the never-ending task of finding, removing and replacing the bad code or reconfiguring the misconfigured systems.

4.1 Network Discovery Tools

Actively scan networks and/or analyze network traffic to determine what hosts are active on a network. A second class of tool passively watches the network, constantly finding and characterizing all hosts that are active. Both can find evidence that new devices have appeared or that existing hosts now have vulnerable or infected software active.

- Nmap (free)
- DHS/NSA Trickler (free for government agencies)

4.2 Vulnerability Management

Vulnerability assessment tools discover vulnerabilities and monitor the organization's progress in eliminating the vulnerabilities that are found.

WW QualysGuard

- nCircle IP360
- Nessus (free)
- eEye Retina Network Security Scanner

4.3 Network Penetration Testing and Ethical Hacking

Penetration testing tools go beyond vulnerability discovery; they exploit the vulnerabilities to prove to system administrators that their systems are vulnerable and to determine what the impact of a vulnerability could be.

WW CORE Impact

- Metasploit (free)
- IO Active
- SAINTexploit
- Neohapsis
- Intelguardians

4.4 Patch and Security Configuration Management and Compliance

To reduce exposure to attacks, known vulnerabilities, (both patches and misconfigurations) should be fixed as quickly and as efficiently as possible. Patch management systems automatically deliver and install the correct patches; security configuration management systems automatically eliminate configuration weaknesses from weak passwords to unnecessary services.

WW BigFix Discovery
WW Lumension PatchLink

- Shavlik NetChk

DEFENSIVE WALL 5: Safely Supporting Authorized Users

Summary: Solutions in this group help ensure that authorized users are not unduly impacted by security requirements while unauthorized individuals are blocked.

5.1 Identity and Access Management

These products verify that the right people are allowed to use a system, that they are allowed to perform only those tasks for which they have authorization, and that their access is blocked when their employment is terminated or when their status changes. Advanced IAM systems include workflow and provisioning capabilities to make sure access controls are consistent across applications.

- Oracle
- IBM-Tivoli
- A10 Networks
- Quest Software

5.2 Mobile Data Protection and Storage Encryption

Credit card information and other sensitive, private information would be a lot safer if it were encrypted. In addition, most breach disclosure laws do not require losses to be reported if the data was fully encrypted.

- CheckPoint (formerly Pointsec Mobile)
- PGP Whole Disk Encryption
- Utimaco SafeGuard
- Guardian Edge Encryption Plus
- Seagate Momentus, MobileMax
- Credant Mobile Guardian (CMG)
- GuardianEdge Data Protection Platform

5.3 Storage and Backup Encryption

Sensitive information has been lost on unencrypted back-up tapes and through unauthorized network penetration. Encryption appliances, or backup drives with built-in cryptography, encrypt data stored on those tapes or file systems.

- NetApp's DeCru DataFort
- NCipher NeoScale CryptoStor

5.4 Content Monitoring

Content monitoring and filtering tools are used to enforce acceptable use policies, as well as detect information leakage. They inspect local storage and internal network traffic looking for sensitive information stored inappropriately or exiting the enterprise.

- Symantec (formerly Vontu)
- Websense (formerly PortAuthority)
- Tiversa Enterprise Monitoring Services
- SafeMedia Clouseau Network Security

5.5 Data Leak Protection and Digital Rights Management

- Vontu (now Symantec) Enforce Platform
- Vericept Monitor, Protect, Discover, Edge
- Reconnex Data-in-Motion, Data-at-Rest, Data-in-Use
- Oakley (now Raytheon) SureView, CoreView, SureFind

5.6 Virtual Private Networks (VPNs)

VPNs save communication cost by enabling users to access their corporate networks through low-cost Internet connections, but they encrypt the data when it travels over the network. VPNs should be used in conjunction with network access control to ensure the endpoints are secure. Most new installations are SSL VPNs.

- F5 FirePass
- Microsoft Forefront
- Citrix Access Gateway

DEFENSIVE WALL 6: Tools to Manage Security and Maximize Effectiveness

Summary: This area focuses on the tools that manage and improve security processes, as well as on tools needed to reduce the damage done in a successful attack.

6.1 Log Management and Security Information and Event Management

These solutions bring together data from server logs, IDS, firewall, vulnerability management, and other tools to enable an enterprise to find out what actually happened after an attack takes place.

WW LogLogic 4 LX
WW ArcSight Log Management Suite
WW SenSage Enterprise Security Analytics
WW Prism Microsystems EventTracker
WW TriGeo Security Information Manager

- RSA (EMC) enVision Platform
- NetIQ Security Manager

6.2 Media Sanitization and Mobile Device Recovery and Erasure

Tools to empty all information off storage media before discarding them, and to recover or disable mobile devices.

- Darik's Boot and Nuke
- Absolute Software CompuTrace

6.3 Security Skills Development

Effective security skills development is training that can prove it enables individuals to develop and demonstrate mastery of the skills and knowledge that are essential for their jobs.

SANS Institute

- BlackHat Briefings

6.4 Security Awareness Training

End users cannot be "trained" into protecting their systems and networks, but once security staff have ensured that all systems are configured securely and networks safely protected, then this training can help users know about mistakes they must avoid. Here are some of the most highly valued, free tools that security professionals use in awareness programs.

- Videos: US Department of Veterans Affairs and US Department of Defense
- Security Tip of the Day: US AID (Users cannot sign on unless they answer a security question correctly)

Monthly Security Awareness Newsletter: *SANS OUCH!*

6.5 Forensics Tools

Some attackers get through and when they do, enterprises need to find out what they accessed, what they damaged, and how they got in. Finding those answers is a task made easier through forensics tools that intelligently and rapidly study the disk images and other evidence available after an attack.

- Mu Security Mu-4000 Security Analyzer
- Guidance Software (Encase)
- Access Data Ultimate Tookit
- Netwitness Investigator
- Technology Pathways

6.6 Governance, Risk and Compliance Management Tools

GLB, FISMA, SOX, PCI, Basel, DITSCAP, DIACAP, and HIPAA each generate enormous documentation burdens for companies, universities, and/or government agencies. GRCM tools help automate creation of necessary reports, support the update and dissemination of security policy, and provide consolidated means for tracking disparate compliance efforts.

6.7 Disaster Recovery and Business Continuity

Bad things happen – flooding, cyber attacks, bombs. Being ready to respond means having alternative sites with data and systems ready; it also means testing those recovery capabilities.

- EMC
- Sunguard