NETWORK ASSOCIATES

YOUR NETWORK. OUR BUSINESS.

EXECUTIVE WHITE PAPER

The Enterprise Strikes Back: Defending Against Blended Threats

Proactive Strategies to Protect Networks from Today's Most Virulent Security Threat

McAfee SECURITY

networkassociates.com

I. Executive Summary

The computer viruses that grabbed news headlines just a few years ago—LoveLetter, Melissa, and Michelangelo, to name a few—would barely cause a ripple in today's media, having been superseded by a new type of security threat that is geometrically more destructive. This new threat, called a *blended threat,* combines the traditional malice of email borne viruses with new network-based capabilities that quickly seek and find security vulnerabilities across the enterprise network, spawning further destruction such as denial of service attacks, crashed servers, and vulnerability at the core, or "root," of computers.

Blended threats strike with blinding speed, and are poised to quickly dwarf the destruction inflicted by previous generations of computer viruses. Unfortunately, despite a high level of awareness of the risk of computer attacks, many enterprises are unprepared to handle blended threats. The tentacle-like hold that blended threats quickly exert demands a protection strategy designed to neutralize attacks before they take place. The strategy must be proactive, rather than reactive, and it must be integrated to provide protection on the desktop and at the enterprise network level. Easy manageability and powerful reporting are additional essential requirements.

McAfee® Security's integrated, proactive solution for combating blended threats affords the industry's first proactive platform for eradicating vulnerabilities, protecting the enterprise before blended threats strike. McAfee's approach to blended threats is an extension of its multi-tier anti-virus defense, a comprehensive approach to security that ensures virus protection both within the four walls of the enterprise and beyond. Broadening and deepening the multi-tier virus protection provided by the combination of products such as VirusScan®, NetShield®, GroupShield®, and WebShield®, McAfee's blended threat solution comprises three key products:

- *ThreatScan ™,* which provides proactive virus vulnerability detection for desktops and servers. It helps administrators find devices, applications and operating systems that are vulnerable to viruses, are infected or are unprotected.

- *Desktop Firewall ™,* the market-leading desktop firewall and intrusion detection software, protects the desktop against malicious code and hackers.

- *ePolicy Orchestrator ™ (ePO),* McAfee's management platform for enterprise-wide security monitoring and solution deployment, which translates masses of data into business-actionable information.

McAfee's blend of proactive protection technologies greatly simplifies proactive security management, resulting in fewer emergency downloads or distribution of .DAT files, less user down-time and significantly reduced virus clean-up costs.

For enterprises looking to rid their network of blended threat vulnerabilities, the McAfee solution uniquely affords proactive detection against discrete blended threats. McAfee allows IT organizations, finally, to strike back against today's most virulent security threat.

II. Bigger, Badder, and Faster than Ever: The Blended Security Threat

Starting with CodeRed, blended threats have taken the computer security world by storm, combining the traditional destruction of email borne viruses with new network-based capabilities that quickly seek and find security vulnerabilities across the enterprise network, spawning denial of service attacks, crashed servers, root vulnerability and other mayhem. In addition to Code Red, other high-profile blended threats in the past two years have included Goner, Klez, BugBear and perhaps the most notorious, Nimda, whose numerous modes of propagation illustrate its tenacity:

- Nimda infects Web pages; viewing infected pages results in automatic download and execution of README.EML on vulnerable desktops.

- It infects files by appending to .EXE files, converting C and D drives to open shares. It sets itself to automatically restart when booted.

- Nimda uses the backdoors left by CodeRed C/D, Sadmind, and others to infect, as well as a number of Unicode exploits.

More recently, BugBear quickly spread across global networks by replicating itself through a Windows machine's email address book, attaching itself to previously sent email messages. BugBear also spread through the network system, with keystroke-logging and backdoor capabilities that allowed hackers to intercept passwords and gain access to computers over the Internet.

Blended threats inflict swift, severe damage

Blended threats strike with blinding speed; at its peak, Goner infected more than 12,000 computers per hour[1], causing billions of dollars' damage worldwide. Based on their speed and malicious capabilities, blended threats are poised to quickly dwarf the destruction inflicted by previous generations of computer viruses. For example, fully 20 percent of respondents to ICSA Labs 7th Annual Computer Virus Prevalence Survey suffered attacks from blended threats, up from just two percent the year before—a figure even more meaningful considering that the final survey responses were still being tallied when Nimda struck in September 2001.

The bottom-line impact is sobering; in the 2002 CSI/FBI Computer Crime and Security Survey, the total financial losses reported by the 188 respondents willing and/or able to quantity them were $50 million, reflecting the impact of the blended threats CodeRed, Nimda and SirCam.[2] Computer Economics estimates that the worldwide economic impact of Code Red was $2.62 billion, SirCam $1.15 billion and Nimda $635 million.[3]

Disaster preparedness: Many enterprises are not ready

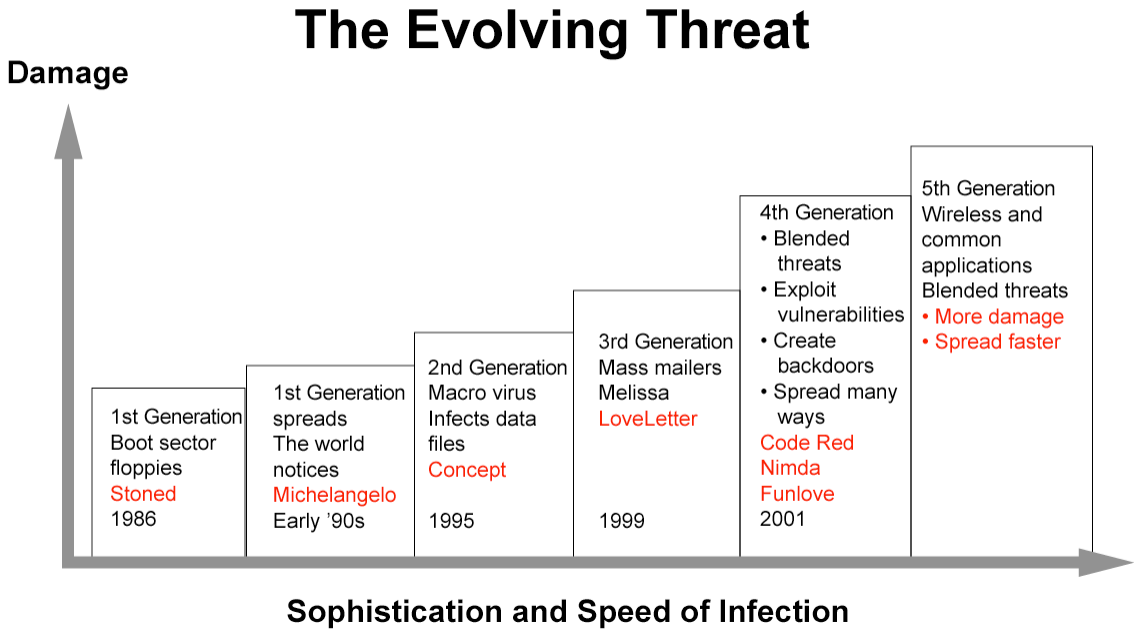
Unfortunately, despite a high level of awareness of the risk of computer attacks, many enterprises are unprepared to handle blended threats. The Global Security Survey, jointly conducted in 2002 by the Internet Security Alliance, the National Association of Manufacturers and Red Siren Technologies, Inc., found that although 91 percent of respondents recognize the importance of information security, an alarming 30 percent reported their business-critical information is still not adequately protected. Moreover, 45 percent of respondents reported they are not adequately prepared to deal with information security and cyber terrorism threats.[4] Most of the 227 participating organizations reported at least one attack in the past year, with 25 percent reporting one to five attacks, 10 percent reporting 6–20 attacks, and 17 percent reporting more than 20 attacks. However, 18 percent did not know how many times their organizations were attacked.[5]

As a result of these and other equally frightening statistics, Giga Information Group lists blended threats as one of the principal content security threats challenging today's enterprise, noting, "Use of new communication tools in the enterprise, such as instant messaging and collaboration portals, is outpacing IT's ability to protect the organization, their systems and the users against security threats."[6]

Digital Darwinism: An Integrated, Proactive Approach to Network Defense

Clearly, blended threats are a force to be contended with. And although they have quickly stormed onto global networks, today's blended threats have in fact been in the making for more than 15 years. (Figure 1.)

[1] Source: McAfee 2001-2002.
[2] 2002 CSI/FBI Survey, Computer Security Institute.
[3] As cited in 2002 CSI/FBI Survey, Computer Security Institute.
[4] As cited in SupportIndustry Newsletter, September 20, 2002.
[5] *Ibid.*
[6] "IT Trends 2002: Content Security," by Jonathan Penn, Giga Information Group, April 9, 2002.



Computer viruses have evolved to inflict greater damage, more quickly.

The first computer virus, called "Brain," appeared in 1986. It was a boot sector virus that infected 360Kb floppy disks, creating a volume label "(c) Brain" on infected floppy disks. Since it was spread through the sharing of floppy disks, Brain's transmission was slow and stealthy.

The first virus to prove itself to be more than a pesky nuisance was Michelangelo, which became the subject of media hype on March 6, 1992. Although millions of PCs were predicted to be stricken by Michelangelo, only thousands were affected—still, the world now viewed computer viruses as a serious threat.

The other type of first-generation virus infected programs—first .COM files, then later.EXE files. The development of local area networks enabled viruses like Jerusalem and Cascade to spread quickly across corporate networks.

The second generation of viruses was the platform-independent macro virus, embedded in word processing or spreadsheet documents. Macro viruses spread quickly through shared documents, and thousands of them cropped up in the years following the appearance of the Concept virus in July 1995.

But macro viruses provided just a hint of the destruction to come from more sophisticated viruses like Melissa, which in 1999 caused $1.1 billion in damage worldwide.[7] Melissa, like LoveLetter and many others, used email systems to proactively spread their destruction by distributing .VBS and .EXE files, spawning the rise of virus protection via scanning at the gateway.

While all viruses prior to Melissa had been written by computer hobbyists and other intelligent individuals, it was Melissa and the blended threat Nimda that revealed the work of a new breed of hacker—cyber vandals who understood not just how individual computers operate, but entire corporate networks. Spread through mass-emails of a README.EXE file, Nimda was a 32-bit virus mass-mailer that gathered email addresses from mailboxes and cached .HTM[L] files, and then sent out the .EXE file which executed automatically on vulnerable systems.

Nimda went one step beyond traditional .EXE viruses, infecting Web pages. Viewers of infected pages unwittingly

[7] As cited in 2002 CSI/FBI Survey, Computer Security Institute.

automatically downloaded and executed a README.EML file on vulnerable desktops, setting off another wave of infections. Others of Nimda's caliber include CodeRed, SirCam, Klez, and BugBear.

McAfee's Laws and the predictive nature of computer viruses

Unfortunately, computer viruses promise only to become more virulent, more quickly. John McAfee, founder of McAfee Security, a division of Network Associates, authored a series of three postulates about the nature of computer viruses to help guide enterprise preparedness efforts. McAfee's Laws, as the are called, have been proven time and again to be accurate guidelines for companies looking to proactively protect themselves from viruses and blended threats.

McAfee's First Law states, "The time required for malicious code to spread to a point where it can do serious infrastructure damage halves every 18 months." So, while several years ago it took four or five months for a macro virus to spread, today's blended threats can infect computers worldwide in a matter or hours. CodeRed infected computers at a rate of 2,000 per hour, while Nimda raised the stakes to 6,000 infections per hour. Goner, as previously noted, infected 12,000 computers per hour at its peak outbreak.[8] Additionally, while the average 1,000 corporate computers withstood 20 infections per month in 1996, that number has risen to 113 per month in 2002[9].

McAfee's Second Law predicts, "When a platform or application gains wide spread popularity, it will be attacked." Many industry experts believe that instant messaging platforms and personal digital assistants (PDAs) such as Palm Pilot and Handspring devices will be the target of the next wave of viruses. These devices, while providing easy ways to share information, also make it easy to spread viruses. As the "floppy disks" of the new millennium, PDAs can pose a portable threat to corporate networks. Early threats targeted at the PalmOS include the Trojan horses, Liberty and Vapor, and the Phage virus.

McAfee's Third Law states that "The cleverness, technical sophistication and malicious intent of virus writers increases consistently over time." The fact that new viruses and blended threats manage to inflict staggering amounts of damage is a sufficient proof point to McAfee's Third Law—and provides the motivation for enterprises of all kinds to proactively protect their networks from blended threats. Security spending is on the rise, as documented by many surveys and studies. For example, the Global Security Survey of in 2002 found that 47 percent of respondents said their companies had increased spending on information security over 2001, and 38 percent said that trend would continue in 2003.[10]

Thwarting blended threats with a proactive, integrated defense

In considering new security investments, the tentacle-like hold that blended threats quickly exert demands a protection strategy designed to neutralize attacks before they take place. The strategy must therefore incorporate two tenets:

First, it must be *proactive,* rather than reactive. Blended threats demand proactive protection for several reasons, principally the speed and severity with which they strike; the extraordinary cost of downtime, and the amount of IT resources required to clean up after an attack constitute significant motivation to thwart blended threats before they strike. The proactive network protection should provide heuristic analysis to inspect the code in a file to see if it contains virus-like instructions. It should also provide generic detection, based on a virus definition that will detect all subsequent variants of a particular virus family.

Second, the strategy must be *integrated* to provide protection on the desktop and at the enterprise network level. Easy manageability and powerful reporting are corollary requirements. For example, desktop capabilities—typically a firewall—must be easily administered in order to keep down overhead costs, and the reporting function should afford easy visual analysis at both macro and granular levels.

[8] Source: McAfee 2001-2002.
[9] Source: ICSA 2002.
[10] As cited in SupportIndustry Newsletter, September 20, 2002.

Manageability: A many-faceted requirement

Ease in manageability is, in itself, a multi-faceted requirement. The broad reach of blended threats, and the distributed solutions used to protect against them, demands full visibility into all aspects of the network, as well as split-second response capabilities. The chosen protection solution must provide full visibility into network activities at both a global and granular level, with "drill down" reporting to examine specific servers, network links, and desktop machines, correlating network events with these components' status. In turn, these precise diagnostics must be complemented by fast, succinct remediation that involves no emergency downloads of .DAT files, no .DAT distributions, no user downtime, and no virus clean-up costs.

Ideally, the management platform for the blended threat solution should accommodate multiple vendors' products, giving the enterprise the flexibility to choose best-of-breed products, not just management platform vendor's own. This capability is critical in building a defense that is impermeable by even the most sophisticated threats.

III. McAfee's United Front Against Blended Threats

Built atop a multi-tier anti-virus defense, McAfee's integrated, proactive solution for combating blended threats across the enterprise combines three key products:

- *ThreatScan,* which provides proactive virus vulnerability detection for desktops and servers. It helps administrators find devices, applications and operations systems that are vulnerable to viruses, infected or unprotected.

- *Desktop Firewall,* the market-leading desktop firewall and intrusion detection software, protects the desktop against malicious code and hackers.

- *ePolicy Orchestrator (ePO),* McAfee's management platform for enterprise-wide security monitoring and solution deployment, which translates masses of data into business-actionable information.

ThreatScan: Virus vulnerability assessment

Unique in the network security arena, McAfee ThreatScan proactively protect the network against blended threats with scheduled virus vulnerability scans and updated signatures. It does not require operation by a security expert, instead proactively scanning and reporting on unprotected, unmanaged, infected, and virus-vulnerable machines. In doing so, it helps companies achieve higher levels of anti-virus protection and policy compliance by identifying virus-vulnerable devices, operating systems, and applications, and discovering unprotected and rogue devices that open the door to network infections.

With ThreatScan, enterprises can transition from reacting to infections to actively preventing blended threats, and deflecting their associated costs. ThreatScan allows a wide range of security vulnerabilities to be proactively identified, including:

- Susceptible machines
- Susceptible applications
- Infected machines
- Security threats by specific, named viruses
- Security threats by general class of exploitable hole

Prior to ThreatScan, each machine on the network had to have been physically audited to check for vulnerabilities. Some methods or tools require extensive security expertise or definitions just to find the trouble spots in the network. Administrators are caught in a double bind—they are pressed for time, yet need to prevent the costs of virus outbreaks. ThreatScan allows a scan to be scheduled, probing machines attached to the network, utilizing installed agents managed through ePolicy Orchestrator. Through ePO, ThreatScan allows IT users to easily deploy an ePO

agent with standard deployment methodology (SMS, ePO, email, Tivoli, login scripts, etc.) so new machines can be easily audited, remotely.

Desktop firewall: Comprehensive defense at the PC level

McAfee Desktop Firewall blends market-leading desktop firewall and intrusion detection software. It acts as a desktop "traffic cop," allowing known applications to connect to desktops while stopping damaging traffic from hackers, malicious code, distributed denial of service attacks, and vulnerable or unauthorized applications. A distributed intrusion detection system (IDS) provides the first line of defense to block common hacker attacks, stop Trojan horses, denial of service attacks, and other threats, while a distributed firewall provides the second line of defense with robust packet filtering and application-level policy enforcement.

Desktop Firewall can be set up to operate transparent to the users, inspecting inbound and outbound traffic on the computer, and then allowing or blocking connections based on policies for addresses, ports, protocols, and applications. These policies can be set by a user or by an administrator.

McAfee Desktop Firewall protects desktops from attacks inside or outside the corporate network, and can even foil malicious code attacks once they have been set off within the enterprise perimeter. Malicious code can silently invade desktops from a single Web site visit, and then attack other machines on the network; McAfee Desktop Firewall detects unauthorized intrusions and application connections, blocks them, records the event, and reports to the administrator through ePolicy Orchestrator. ePO also affords centralized management, including installation, ongoing management, reporting and policy lock-down.

ePolicy Orchestrator: Fulfilling the manageability mandate

ePolicy Orchestrator makes it easy to protect the enterprise against blended threats, providing full visibility into the enterprise network, and allowing updates to be deployed across the network almost instantaneously. Using ePO's comprehensive policy management, graphical reporting and software deployment, administrators can manage policies and deploy ThreatScan and Desktop Firewall protection while generating detailed graphical reports on McAfee anti-virus products, as well as Symantec desktop and server anti-virus products.

The ePolicy Orchestrator single-server model can be scaled up to 250,000 users. Administrators can enjoy a range of powerful options, setting policies by machine or by group. Policies can be changed as often as necessary to adapt to changing threats and network environments, all from a single console. This extends to outbreak management. ePolicy Orchestrator responds instantly to virus outbreaks by configuring an enterprise-wide AutoUpdate, scanning manually, and generating detailed reports to pinpoint entry points and identify a pattern of propagation. This coordinated response speeds the update process and helps stop a spreading virus.

Across the board, ePO's superlative reporting capabilities help to correlate network events with business-actionable remedies. Many management tools simply produce reams of data that the administrator must sort through in order to determine a specific network problem. ePolicy Orchestrator answers the two questions that are constantly asked regarding virus infection: "Am I protected?" and "Am I infected?" With ePO, administrators can be certain that computers are up to date with the latest virus definitions and scan engine. A wide range of customizable charts are available, including 3D bar charts, pie charts, line graphs, and tables.

Finally, ePolicy Orchestrator allows IT users to manage blended threat security over the Internet, including remote users or offices even that are not connected to the corporate network. Any Internet connection will allow the ePolicy Orchestrator agent and server to communicate, making management of mobile users of Desktop Firewall seamless. Even the administrator's console can be connected remotely.

IV. Summary: The McAfee® Advantage

Blended threats are today's most ominous security challenge, quickly distinguished by their speed and virulence. McAfee Security uniquely offers proactive detection of new threats with a multi-tier approach to anti-virus protection, and a three-pronged solution comprising ThreatScan, Desktop Firewall, and ePolicy Orchestrator. McAfee's blend of

proactive protection technologies ultimately leads to greatly simplified proactive security management—fewer emergency downloads or distribution of .DAT files, less user down-time, and significantly reduced virus clean-up costs.

For enterprises looking to rid their network of blended threat vulnerabilities, McAfee's multi-tier approach to enterprise security offers a superior approach. Coupled with the mission-critical protection afforded by award-winning anti-virus products, McAfee enables specific blended threats to be detected and eliminated by ThreatScan, the easily implemented and managed high-performance Desktop Firewall product, and easy-to-use, interpretive reports from ePolicy Orchestrator. ePO is a leading platform for integrating best-of-breed security components from a variety of vendors, allowing IT organizations, finally, to strike back against blended security threats.

For more information about McAfee Security's blended threat solutions, please visit http://www.networkassociates.com.

6-AVD-MBT-001 11/02