EVM White Paper

Executive Summary

As networks continue to be mission-critical business systems for enterprises of all sizes, one of the top priorities for many IT departments has become securing the mobile devices being used by their mobile and remote workers. These endpoint devices, which historically were used mostly by road warriors and heavy business travelers, are more and more common across the entire workforce. Because these devices are open doorways into the enterprise information architecture for unauthorized intrusions, viruses, and worms, this reality weighs on the minds of many IT managers. Therefore, enterprises are looking for a solution, which incorporates effective processes and technologies to help them proactively identify, manage, and eliminate endpoint vulnerabilities.

Building a strong, agent-based endpoint vulnerability management solution based on mitigating known vulnerabilities has transformed from a reactive, security-centric process to an active, policy-centric process and has become an operational necessity for business success. A policy-centric, agent-based approach allows corporate IT departments to manage and provision their mobile and remote workforce according to the needs of the user, rather than to the contract terms of specific carriers or the connectivity limitations of specific technologies. This approach also enables IT departments to dynamically enforce corporate policies outside the traditional enterprise perimeter.

The extended enterprise can be defined as an intricate web of people, devices, access options, and applications. And, because of the ever-increasing number of vulnerabilities, the need for an effective vulnerability management strategy in the extended enterprise is greater than ever before. Gartner defines vulnerability management as a set of processes and technologies that establishes and maintains a security configuration baseline; discovers, prioritizes, and mitigates exposures, establishes security controls; and eliminates root causes. Gartner predicts that enterprises that implement a vulnerability management solution will experience 90 percent fewer successful attacks than those that make an equal investment only in intrusion detection systems.[1]

With security threats proliferating globally in just minutes, enterprises can no longer address these vulnerabilities by simply implementing 'fire fighting' security policies. Instead, they must implement proactive security policies through an endpoint vulnerability management solution that protects the enterprise from the network core all the way out to the most remote endpoints.

Endpoint devices that have been disconnected from the network are a growing threat to enterprise security and traditional IT security products have proved ineffective in mitigating the security risks associated with protecting an organization's mission-critical information.

There are on average 40 Microsoft Windows patches per year – a third of them critical and a great many more related to applications and other operating systems. According to The Yankee Group, any network greater than 500 seats that is patched in response to a vulnerability release consumes 100 to 120 hours of man-hours in testing, installation, and problem resolution. These man-hours cost the enterprise $3,000 to $4,000 in salaries and divert resources from vital business development. IDC estimates that over 60 percent of all serious security threats (e.g., damages revenue generation, decreases profitability, lowers worker productivity, violates intellectual property, breaches regulatory compliance, or endangers customer trust) come from internal sources, including employees, contractors, consultants, systems integrators, partners, distributors, and even customers that have privileged access to an enterprise's resources.[2]

[1] Gartner. "Predictions for IT Security Directors in 2004." September 11, 2003.
[2] IDC. "Endpoint Security Management: Maximizing Best of Breed." March 1, 2004.

To further the many challenges facing IT departments, more than 90 percent of all security breaches involved a software vulnerability that IT departments knew about but didn't patch. In addition, as organizations become increasingly more mobile and dependent on remote workers to fulfill critical sales, service, and executive roles the task of managing vulnerabilities on remote and mobile computers is fast becoming mission-critical.

The challenge? How can enterprises manage, integrate, and scale IT security technologies for mobile and remote workers? The answer: A comprehensive endpoint vulnerability management solution that *does not* require mobile and remote workers to connect to the enterprise network before enforcing patch and configuration policies. It also requires an endpoint vulnerability management solution, which is specifically designed to ensure that mobile and remote workers are armed with the latest software and operating system patches, updates, and configuration settings before connecting to the corporate network.

The problem

The traditional network perimeter continues to dissolve as endpoints move freely between un-trusted and trusted networks. In an enterprise, endpoints can be defined as a combination of devices, people, applications, systems, and access methods. As the network perimeter dissolves, vulnerabilities become increasingly more difficult to manage because employees, business partners, and customers can now access the corporate network from numerous locations and systems. Maintaining the security posture of computers that spend time outside the corporate firewall has become a significant problem for enterprise security.

More than 90 percent of all security breaches involved a software vulnerability that IT departments knew about but didn't patch. According to Gartner, 2/3 of all vulnerabilities are due to configuration issues. In 2002, the Computer Security Institute (CSI) stated that over 40 percent of respondents to its '*Computer Crime and Security Survey*' reported that detected system penetration came from outside the corporate network. And, the window to preventing these vulnerabilities is getting shorter. *For example*: the Sapphire/Slammer SQL worm required roughly 10 minutes to spread worldwide -- making it by far the fastest worm to date. In the early stages of the outbreak the number of compromised hosts was doubling in size every 8.5 seconds. At its peak, achieved approximately 3 minutes after it was released, Sapphire scanned the Internet at over 55 million IP addresses per second and infected at least 75,000 systems.

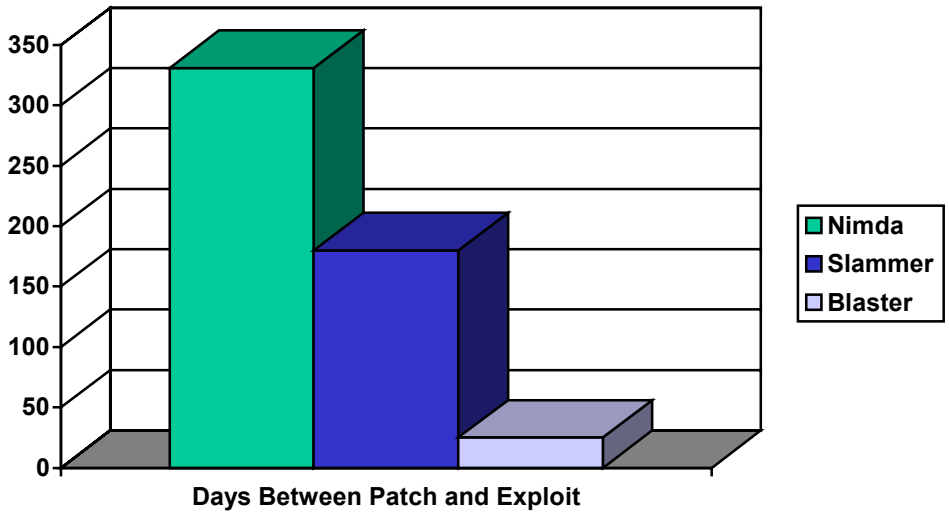


Figure 1: Days Between Patch and Exploit

Therefore, protecting an enterprise's endpoints is vital especially since the number of remote and mobile workers is expected to grow from 39 million in 2000 to more than 55 million in 2004[3]. As the traditional network perimeter continues to dissolve and endpoints move freely between untrusted and trusted networks, vulnerabilities become increasingly more difficult to manage.

Another issue associated with vulnerability management is Instant Messaging (IM). IDC predicts that the volume of corporate IM will increase by more than 130 percent per year through 2004. And, the number of hotspots (approximately 20,000 today) is likely to go up six fold by 2005.

All of these issues further the critical importance of deploying a secure and effective endpoint vulnerability management solution.

The myths behind vulnerability management
There are many common myths associated with the issue of vulnerability management. However, if enterprises understand these myths and take a proactive approach to mitigating them by deploying an effective endpoint vulnerability management solution, most, if not all of them, will dissolve in much the same way the traditional network perimeter is dissolving. These myths include:

The 'I'm Covered' Scenario

- Our VPN protects us with data encryption
- Our anti-virus is automatically updated within our LAN
- We don't allow Wi-Fi or hotel broadband access
- We shipped firewalls to all of our end users
- My mobile/remote users are outside the office -- therefore, I don't need to protect them
- Network intrusion detection systems are sufficient to secure my network

The 'You Don't Know What You Don't Know' Scenario

- New vulnerabilities exist today (e.g., shared drives in airplanes and hotspots) that many organizations don't know about
- The overall cost of remote access is unknown because alternative access technologies are not reported to IT or Finance
- SSL usage is growing and, therefore, so is the exposure of the browser (timely patches are more critical than ever for OS, applications, and anti-virus (AV).

The challenge
Because traditional IT security products have proved ineffective in completely mitigating the security risks associated with protecting mission-critical information, endpoint devices that have been disconnected from the network are a growing threat to enterprise security. According to ICSA Labs, laptops, wireless devices, and file sharing have contributed to an ever-expanding set of infection points, leaving companies scrambling to secure their networks. Therefore, organizations must take a more proactive stance in securing their networks and educating their employees. The challenge is figuring out how enterprises can manage, integrate, and scale endpoint security technologies for mobile and remote workers.

One of the ways to do this is by deploying a comprehensive endpoint vulnerability management solution that does not require mobile and remote workers to connect to the network before enforcing patch and configuration policies. To mitigate these vulnerabilities, enterprises must deploy a solution specifically designed to ensure that mobile and remote workers are armed with the latest software and operating system patches, updates, and configuration settings before connecting to the corporate network.

[3] Washington Technology

Although it is impossible to make networks immune from attack, there are ways to improve the overall security of these systems to make them less vulnerable. A first line of defense is to patch security holes, thereby closing the door on the most common entry point for security threats.

Unfortunately, this is no easy task. Security incidents rose from 2,412 in 1995 to over 82,000 in 2002. With the number of reported vulnerabilities rising sharply, from 171 in 1995 to over 4,000 in 2002, and a parallel increase in the number of security alerts and notes, from an average of 2 per month in 1995 to over 35 per month in 2002, enterprises across the globe are scrambling to keep up.

Because most enterprises patch monthly or quarterly, vulnerabilities are 'acceptable risks' -- in light of the cost and risks associated with patching and this practice creates even more challenges for the enterprise, including:

- Microsoft OS changes (repeated patches with selective implementation by enterprises)
- Browser exposures will be more relevant with the SSL explosion occurring
- Identity theft is increasing because threats are not always addressed by anti-virus solutions and 'phishware' (redirecting to a 'fake' Web site to collect proprietary information (e.g., credit card, credentials) is on the upswing
- Vulnerable device settings (if disk drives are either preset or left sharable, Wi-Fi hotspot access can be a real exposure)

The solution

Enterprise remote access has evolved from a simple access-centric model to one that is policy-centric and multidimensional – driven by a need to support proliferating access methods and devices. More and more enterprises are looking for more than a solution that "just connects." Instead, they want a solution that allows them to deliver "responsible connectivity" for their businesses by providing an endpoint security solution capable of automatically checking for compliance with established security policies and remediating vulnerabilities before allowing connections to the network. In other words, a comprehensive, yet flexible system architecture that helps them manage the seemingly limitless variables that impact their mobile and remote workers on a daily basis – whether attached directly to the corporate network or remotely via a VPN tunnel. And, implementing a remote access system architecture requires that IT managers balance three, sometimes, opposing forces:

Minimizing security risks

- Policy-based access aligns with business needs
- Unified authentication platform
- Integrate with leading encryption, FW, and AV technologies

Ensuring end-to-end productivity

- True anytime, anywhere access
- Support for trusted and un-trusted devices
- Easy access to enterprise resources

Controlling costs and user experience

- Full-service management and support
- Easy to deploy
- Dynamic policy management
- Lower TCO
- Match specific access types to user needs

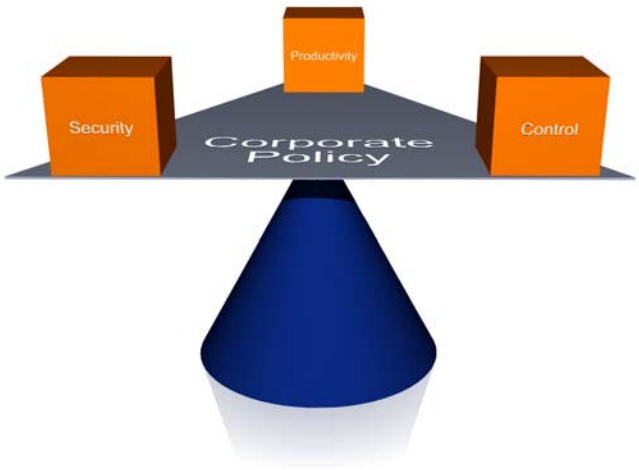


Figure 2: Balancing Opposing Forces

Fiberlink's integrated Endpoint Vulnerability Management (EVM) solution enables enterprises to identify security vulnerabilities at remote endpoints. The solution notifies and alerts IT managers of patch-and configuration-related problems, enforces upgrades, and delivers business intelligence on each event, thereby helping enterprises reduce exposure to security risks and maintain business productivity.

The components of Fiberlink's EVM solution include the following:

- **EVM Agent:** The EVM Agent is a small application that quietly runs on the remote laptop as a service and evaluates the endpoint for critical vulnerabilities. When the user connects to the network, the EVM server will deliver the appropriate corrective actions for any issues that were detected while the machine was off line. It is persistent in nature and runs from startup to shutdown, constantly monitoring the device for vulnerabilities.

- **EVM Server:** The EVM server is the primary repository, which houses all updates and patches for operating systems and anti-virus support. This hardware appliance resides in Fiberlink's secure network operations center and when proactively contacted by the EVM Agent, pushes the appropriate updates and patches to the endpoint device, thereby ensuring secure connectivity and compliance back the corporate network.

- **EVM Relay Server:** The primary function of the EVM Relay Server is to help with the efficient distribution of updates and patches. These relays are designed to alleviate the download burden of the EVM Server and to reduce congestion on low-bandwidth connections. Fiberlink has geographically distributed multiple EVM Relay Servers to optimized efficiency for enterprise users.

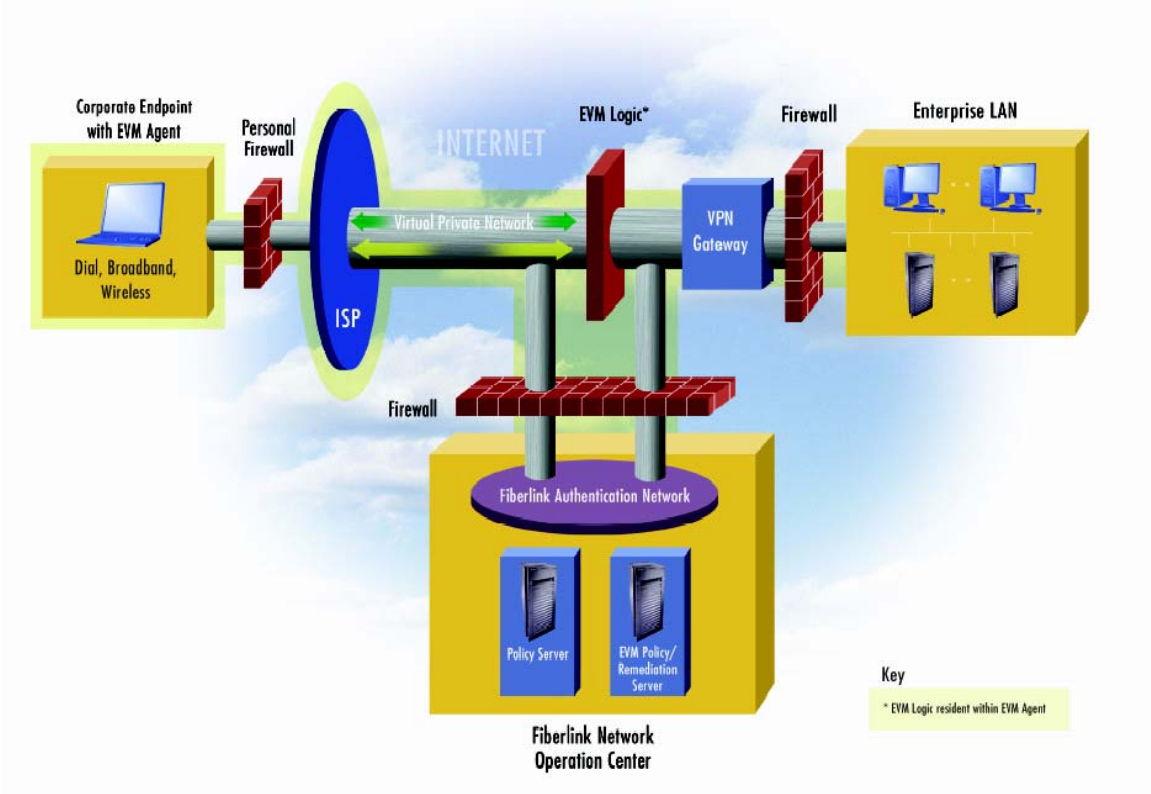


Figure 3: Fiberlink Network Operation Center

The EVM components watch for vulnerabilities even when a machine is not connected to the network – as is the case with mobile and remote workers. In addition, agent-based architectures install agent software on each client machine including sometimes-connected devices such as laptops. In agent-based systems, either the client or the server may initiate communications. This means that each machine can individually query the patch server for new updates or allow the server to scan machines to determine their status relating to new updates and fixes. This configuration eliminates the problems that result from roaming users and disconnected or inactive machines. Even in the case where a user logs onto the network only every few days, the agent automatically queries the server at that time and downloads any new instructions and patches.

Agent-based architectures result in less network traffic, because properties of the machine do not need to be connected to the server to patch relevance. A high degree of parallelism is achieved when the agents -- rather than the server -- compute patch relevance. These architecture attributes combine to create better scalability, and make it possible for agent-based systems to use a larger number of device attributes to determine patch-relevance, increasing accuracy and speed.

Real-time visibility, real-time control, and scalability are three other major benefits of Fiberlink's EVM solution.

- Real-time visibility allows vulnerability discovery across all of the computers in an enterprise in seconds to minutes (vs. hours to days) on or off the network.
- Real-time control allows continuous policy-based enforcement and automated-assisted control on every managed computer whether on or off the network.
- The scalability of the solution helps reduce TCO by reducing hardware investment, setup, and maintenance. In addition, the architecture is designed to adapt easily and efficiently to geographically distributed enterprise network topology and infrastructure.

The EVM solution also offers a high level of manageability by easily adapting to an enterprise's existing administration model. It also provides ease and speed of identification and prioritization of issues and vulnerabilities and has a low learning and training curve. And, its endpoint security features provide continuous identification of vulnerabilities and autonomous remediation of vulnerabilities even when mobile and remote computers are off-network

Fiberlink's EVM solution helps protect the enterprise by ensuring that all of its computers, (including laptops) that may be connected to the network only sporadically, are supplied with the latest software updates and patches. EVM agents on each system continually monitor all of the computers on the network, giving network administrators a detailed visibility into their configuration and patch levels. EVM also allows systems administrators to maintain full control of the patching process, deciding which updates to distribute and when EVM can automatically update the entire enterprise system, or just one system.

Fiberlink's EVM solution is a comprehensive answer to the challenges of patch management, vulnerability identification, and remediation. It ensures that enterprise-wide desktops and servers have the latest security fixes, and that mobile and remote users are protected while they're away from the office – and updated before they're allowed to connect back to the corporate network. Some of the benefits include:

- Integrating advanced security and management of worldwide enterprise access
- Implementing a solution that is both easy to use and deploy
- Closing the window of vulnerability – from weeks to minutes
- Protecting users (even when they are away from the corporate network)
- Regaining control of mobile and remote workers
- Freeing up the IT staff's time
- Increasing the speed of remediation

Describing the business benefits of the technology
There are on average 40 Microsoft Windows patches per year – a third of them critical and a great many more related to applications and other operating systems. According to The Yankee Group, any network greater than 500 seats that is patched in response to a vulnerability release consumes 100 to 120 hours of man-hours in testing, installation, and problem resolution. These man-hours cost the enterprise $3,000 to $4,000 in salaries and divert resources from vital business development.

It has been estimated that over 60 percent of all serious security threats (e.g., damages revenue generation, decreases profitability, lowers worker productivity, violates intellectual property, breaches regulatory compliance, or endangers customer trust) come from internal sources, including employees, contractors, consultants, systems integrators, partners, distributors, and even customers that have privileged access to an enterprise's resources.[5] Costs associated with other vulnerability issues include:

- PC viruses cost businesses approximately $55 billion in damages in 2003.
- The same calculations were done in 2002 and 2001, at $20-30 billion and $13 billion, respectively.

[5] IDC

- It was estimated that in 2001 alone, the worldwide impact of malicious code was $13.2 billion, with the largest contributors being SirCam at $1.15 billion, Code Red (all variants) at $2.62 billion, and NIMDA at $635 million.[6]

Among enterprises, security is the top concern for Wi-Fi deployment and security spending is skyrocketing. IDC estimated that enterprises spent approximately $7 billion building VPNs in 2002, and that figure is expected to grow to $10.3 billion by 2007. And, Gartner stated that worldwide spending on dedicated firewall and IP VPN equipment grew by 18 percent in 2002 in the wake of the September 11th terrorist attacks. Over 75 percent of this spending was on firewalls alone.

A managed endpoint vulnerability solution helps eliminate expenses by minimizing infrastructure and internal resources and addresses the ongoing problem of the vulnerability of users outside the corporate network.

- There was a 40 percent increase in the number of security incidents reported in the first 9 months of 2003.[7]
- The average time between the announcement of a computer system security flaw and the malicious code that takes advantage of it has declined to 10 days from 281 days in 1999.[8]
- Over 42 percent of IT professionals say that they spend (on average) 2 hours per day researching security management issues, from patch management to security management – and beyond.[9]
- The average cost per company for failure to patch vulnerabilities has risen to $2 million.

Best practices for vulnerability management
One of the most important considerations when choosing an endpoint vulnerability management solution is probably the most obvious: a solution that is easy to install, deploy and maintain so that you can be up and running quickly, reporting on known vulnerabilities before they are able to harm your corporate network.

[6] Computer Economics
[7] CERT® Coordination Center
[8] Foundstone, Inc.
[9] 2002 CSI/FBI study

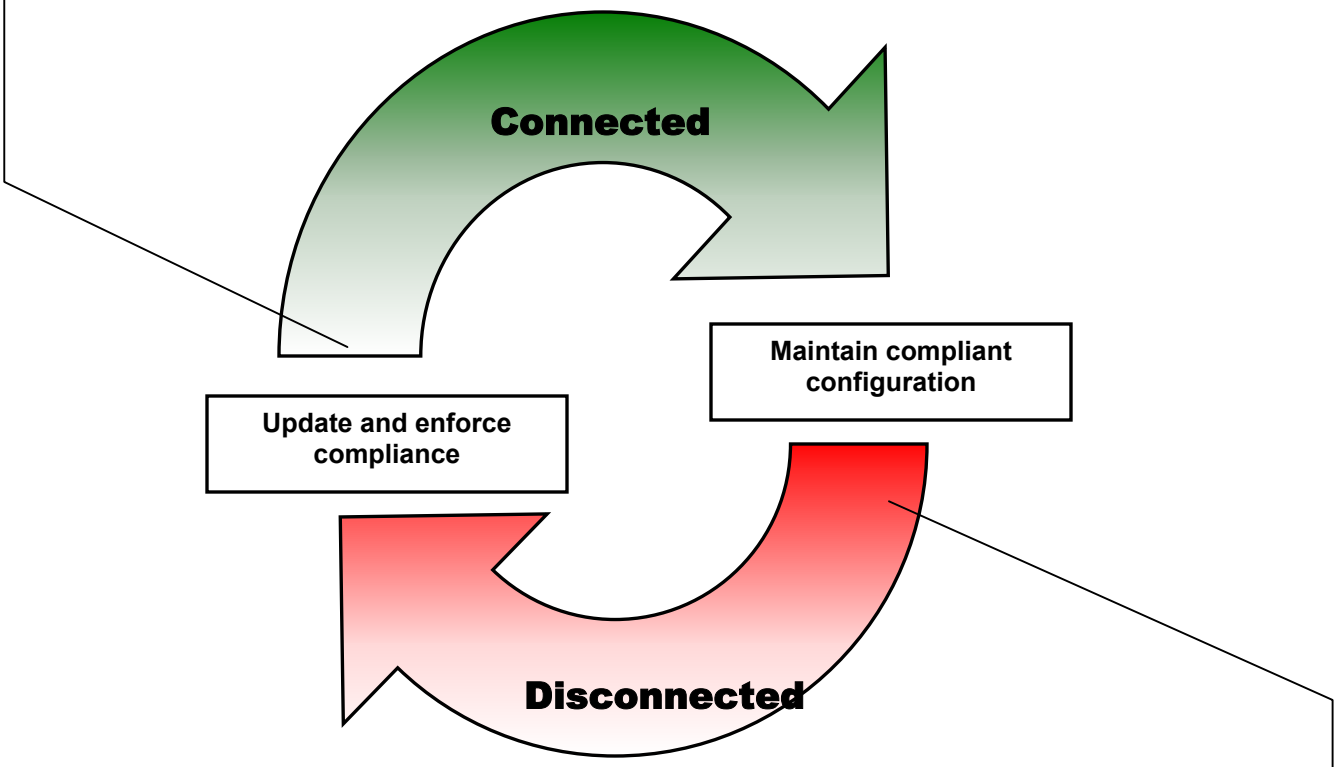
In practice, a successful endpoint vulnerability management strategy generally cycles through two key phases:

- Bringing systems into a state of compliance when connected to the corporate network
- Maintaining that last compliant configuration when disconnected from the network

Throughout the cycle of connecting and disconnecting from the network, IT departments must manage vulnerabilities across hardware, software, services and personnel resources.

At time of connection:

1. Run all pre-determined critical software: antivirus, firewall, etc.
2. Push latest policy updates and enforce on-network policy
3. Patch OS, third-party software
4. Disable or uninstall all non-compliant software
5. Secure browser and e-mail configuration:
    a. No password caching, no persistent cookies, proper security levels, proper ActiveX controls, etc.
6. Adjust other configuration settings:
    a. Power savings, file system encryption, auto-lock after idle, clear system page file on shutdown, bandwidth limitation per transport, etc.



At time of disconnect:

1. Run all pre-determined critical software: antivirus, firewall, etc.
2. Enforce off-network policy
3. Restrict installation of unauthorized software
4. Notify the user if there are open shares and the machine has an active wireless card
5. Enforce security and other configuration settings
6. Turn off USB drives, disable unused Ethernet adapters

Summary

In an age of accelerating vulnerabilities, hacker attacks, software updates and security patches, IT managers seek more specialized types of configuration management. And, the ability to access and manage vulnerabilities is essential in maintaining a network that supports a mobile and remote workforce.

With the number of remote and mobile workers expected to grow from 39 million in 2000 to over 55 million in 2004[10], network exposure from remote endpoint devices is spiraling out of control. In addition, security spending is increasing at a staggering rate as enterprises are expected to spend $10.3 billion on security by 2007.[11]

In 2001, Fiberlink became the first company to offer a managed endpoint firewall and full remediation for OS and AV patches, not just quarantining. Both of these offerings were designed to meet the vulnerability management needs of large enterprises by eliminating expenses through the minimization of additional infrastructure and internal sources.

In November 2001, The Yankee Group recognized Fiberlink for pioneering the Remote Endpoint Security (REPS) market when it began integrating managed security solutions for its Fortune 500 customers. At that time The Yankee Group stated that such managed solutions are going to be a "must-have" within 18 months given the explosive growth in blended security threats at that time. At the present time, Fiberlink has over 100,000 personal firewalls under management, making it the single largest provider of managed endpoint security services in the remote access marketplace.

Fiberlink's EVM solution enables policy-based access in today's extended enterprise and protects both remote and mobile users from known vulnerabilities even when they're not connected to the network. In addition, it protects corporate networks when mobile and remote workers return by making sure that laptops are updated during the authentication phase -- before they're allowed to log on.

The Fiberlink solution makes it possible to enforce patch, security, and business policies before endpoints connect to the network due to its uniquely designed Dynamic Network Architecture (DNA).™

The power behind the platform

DNA is the industry's first platform to integrate all aspects of secure remote access for the extended enterprise. DNA unifies control, availability, security, and management of worldwide access and integrates advanced security, emerging access standards, and tier-one networks into a single, unified system architecture. The architecture separates secure remote access into discreet components so that policy enforcement does not require a corporate network connection. This capability is augmented by an agent-based platform that provides speed and control to identify, investigate, and remediate vulnerabilities.

DNA powers Fiberlink's Extend360™ -- the industry's first intelligent access client that integrates policy-based remote access and security into a single intuitive interface. In addition to integrating all of the necessary connection and security elements into a single user interface, the client provides seamless connectivity and compliance with corporate security policies.

In order to maintain a remote and mobile workforce, it is essential for enterprises to assess and manage vulnerabilities that support those workers. Of course, it is vital that enterprises across the board are able to effectively manage patches, but more importantly is the ability for enterprises to be able to address and mitigate the much broader set of endpoint vulnerabilities.

[10] Washington Technology
[11] IDC

About Fiberlink
Fiberlink is a leading provider of secure remote access solutions, unifying worldwide remote access, management and enforcement within existing IT policy. Fiberlink addresses the growing infrastructure complexities of enterprise access brought on by the demands of an expanding business ecosystem. From employees to partners, remote offices to extranets, dial-up to wireless to broadband, Fiberlink allows enterprises to capitalize on extended business opportunities. Multi-network redundancy, best-of-breed application services and support, low total cost-of-ownership and minimal impact on IT help make Fiberlink an important business partner.

Analyst firms including Gartner, Burton Group and Yankee Group recognize Fiberlink as a leader and innovator in the remote access industry. Fiberlink has more than 300,000 corporate users. Fiberlink customers include General Electric, BMC Software, Computer Sciences Corporation, Royal Caribbean, The Gillette Company and Sun Healthcare. Headquartered in Blue Bell, Pa., USA, Fiberlink has offices throughout North America, Europe and Asia Pacific.
For more information on Fiberlink, visit its website at http://www.fiberlink.com.

About BigFix
Fiberlink has partnered with industry leader, BigFix, a leading provider of vulnerability management solutions to deliver the first fully managed solution to offer full identification and remediation of vulnerabilities and other configuration management capabilities for mobile and remote computers. BigFix software solutions help large organizations maintain the health, performance and security of their systems. The foundation for all BigFix solutions is a fully extensible agent-based platform, which gives IT managers' complete visibility into every computer running on a corporate network. The company's flagship product, Patch Manager, automates the complex process of assessing and remediating vulnerabilities across enterprise networks. BigFix also provides modules that harness the power of its platform to solve specific systems management issues. BigFix customers include large organizations in a range of markets including financial services, government and technology. For more information, visit www.bigfix.com.

###