

# Toward Infection and Intrusion Free Networks: Using Network Self Defense in Practice



**infoexpress**

T. 650.623.0260 F. 650.623.0268 [www.infoexpress.com](http://www.infoexpress.com)

© 2004 InfoExpress, Inc.

The information contained herein is the property of InfoExpress, Inc. and may not be copied, used or disclosed on whole or in part, stored in a retrieval system or transmitted in any form or by any means (electronic, mechanical, reprographic, recording or otherwise) without the prior written permission of InfoExpress, Inc.

CyberArmor, CyberGatekeeper Remote and CyberGatekeeper LAN are registered trademarks of InfoExpress Inc. All other product names are registered trademarks of their respective owners.

Document ID: GE10-0324-04

## Executive Summary

In the face of sophisticated cyber attacks, keeping networks available and at high performance has become a major, time-consuming challenge for IT organizations. Security point products have provided some relief in specific areas such as perimeter defense, vulnerability and patch management, SPAM control, among others. IDC predicts that organizations worldwide will spend a projected \$48 billion on security technology in 2004. However, despite increased spending, enterprise LAN/WANs are still plagued by destructive intrusions and infections. Embattled network and security professionals are only marginally confident that their networks can fend off the next malicious code attack.

For networks to stay available and at peak performance, then it is clear that a new approach to network security is required. This approach must recognize the expanding role of networks that has moved its outer edges far beyond traditional, self-contained borders. With ubiquitous Internet availability, mobile computing and wireless access, the network edge is now harder to define and control. A fresh approach to network security must also factor in the increased virulence of recent threats. Self-propagating worms are capable of causing much more damage and in a much shorter time frame. It must be realized that applying layer upon layer of security is now akin to patching holes in a dam that threatens to burst at any moment. For networks and businesses to continue without disruption, network security practice must shift from the current reactive patchwork mentality to a proactive and enforced network self defense. Any device attempting to access the network must be isolated and screened for infections or vulnerabilities. Only then, can they connect to the network.

This paper discusses the enforcement security approach to network security, what it is, how it works, and its value to virtually any organization that houses a packet-switched network. CyberGatekeeper from InfoExpress is offered as an example of this type of network self defense that screens endpoint devices for infections and vulnerabilities prior to network connection.

## The Nature of Today's Threats

In early 2003, the SQL Slammer worm spread around the globe in less than 30 minutes. In its wake, networks were severely clogged; some stopped functioning, and ultimately causing more than estimated \$1 billion damage. In that summer, a denial of service attack labeled MS Blaster infected over 300,000 machines. Unlike viruses triggered through user action such as opening a questionable email, self-propagating network worms spread completely on their own. In late April of 2004 the Sasser worm was first detected. It exploited a known and previously addressed flaw in Windows Local Security Authority Service Server (LSASS) to crash infected devices and cause them to reboot continuously. Any organization that had patched their systems in advance of Sasser was spared any disruption. Unfortunately, that was not the case with the Taiwanese post office, Sydney Australia train system, and several Scandinavian banks, among others that were hit the hardest. This vulnerability allowed the remote attacker to execute arbitrary code with system privileges on Microsoft Windows XP and Windows 2000 systems. The worm installed a copy of itself into the infected computer's memory, which then infected other hosts.

What is similar to all virus writers is their ability to exploit vulnerabilities in popular software such as Windows and Linux operating systems. In just a five year period from 1998 to 2003, the CERT Coordination Center at Carnegie-Mellon University reported a rise in identified vulnerabilities from 262 to 3,784. The total number of mail messages they handled went from 41,871 to 542,754 in that same period. As quickly as a hole is plugged or patched, a new one is constructed and launched. The time window between the discovery of vulnerability and the appearance of a worm that targets the hole has shrunk to a matter of days, leaving organizations little time to 'patch' potentially vulnerable systems. In many cases, these worms penetrate hardened network perimeter defenses.

The experience by the Security community over the last year and half indicated a new level of malicious payload that can result in data loss or damage, or for a hacker to take over a system. Each one of these episodes and other ones required significant IT resources to clean up the worms' mess, as well as find new ways to prevent the next one. But, despite technology advances and additional investment, *preventing* the spread of network worms has been unsuccessful if devices across the entire enterprise are not effectively and consistently maintained with most current security updates. Further, if the policies that govern safe computing are not enforced, then all the precautionary measures taken such as user education and training, security audits, risk analysis, alert systems, will be wasted.

## A Big Trade Off - Open Networks, High Risks

Security and productivity have always shared an uncomfortable union. Too lax a security infrastructure and intrusions can happen, too strict, and user communities voice their complaints. Currently, a real life example exists as businesses have opened up network usage to heretofore high risk practices – Internet connectivity, remote access, mobile computing, and wireless access. Everyday, 24x7, employees, business partners, contractors are allowed to bypass perimeter security as part of business practice. Mobile devices are at a higher risk to contract a worm outside of the corporate network and then let it loose upon their next reconnection. A worm's payload executes quickly and according to its pre-determined game plan such as shutting down a service, wiping out a hard drive, launching a distributed denial of service attack, or in Sasser's case to continuously re-boot a machine. But all it takes is a single vulnerability, a single exploit, a single oversight, and a single failure to heed a warning and a domino-like contamination can bring network operations to an abrupt halt.

IT professionals are no strangers to fighting fires that they can see, but managing threats that can emanate from both outside the organization as well as from within, and at any time, is another story. Tools such as intrusion detection or prevention have improved the ability to warn of anomalous network behaviors, but these systems are not perfect as they occasionally report false positive (or false negative) warnings. Even organizations prepared with elaborate security solutions are being exploited due to frailties in the business and/or technical infrastructure. A patch project is delayed, and a worm such as Sasser finds its hole in TCP Port 445, which is normally used for Windows networking. A user overlooks security policy and disables a piece of security software and it's his or her machine that gets infected and spreads a virus to other hosts on the network. Tightened financial resources put a freeze on IT hiring and basic perimeter defense maintenance slips. Although networks are critical to business continuance and growth strategies, their availability and performance are jeopardized by any number of events that diminish the ability to protect the infrastructure. As long as an organization's approach to network

security is reactive and with an element of incalculable risk, the likelihood of a devastating intrusion remains high.

Combating cyber attacks requires an effective network-based enforcement technology solution. This solution can tell IT through an initial audit process the soundness of their network edge – the health of endpoint devices, and a clear pattern of how employees access the network. Administrators gain a clear idea as to the level of compliancy of corporate- assigned machines. But one of the most important benefits of a comprehensive enforcement process is for organizations to be able to enjoy the productivity gains of an open network because of a more stringent security process.

## CyberGatekeeper – Assess/Quarantine/Remediate

Fundamental to CyberGatekeeper is the premise that good network security begins by allowing access to only those endpoints that comply with security requirements. It achieves this through a complete, full cycle scan and block enforcement process that consists of Assessment, Quarantine and Remediation of all endpoint devices. At initial connection, all devices are placed momentarily in a pre-connection staging area or Quarantine network, while a rapid discovery process checks the health of the machine. Policy compliant systems are issued a clean bill of health and they are allowed network access. Unsafe, unauthorized, unknown, and unrecognized endpoints are blocked and barred from network entry. CyberGatekeeper then helps to bring non-compliant or infected systems back to a healthy status through the remediation process.

Below is the CyberGatekeeper model that indicates a wide array of endpoint applications and configurations that can be enforced on any endpoint device such as desktop computers, laptops, PDAs, etc. The enforcement process is transparent to users and does not require their intervention.



CyberGatekeeper can strictly enforce the following endpoint elements:

- Security software. This includes VPN client versions, antivirus software, endpoint firewalls, application behavior enforcement, and other security related applications and data files such as signature files and engine versions.
- Network attached devices. Devices such as handhels are becoming network aware, and may be able to attach directly to the network. USB mass storage devices have also become an insider threat to safe computing practices, and can be quickly detected.

- Custom applications. Administrators must be able to define applications and configurations that they wish to require or prohibit. The ability to enhance existing audits or create new ones lets organizations react quickly and precisely to new threats.
- System configuration. Some vulnerabilities can be blocked by simply ensuring that the system is properly configured by disabling certain features in the operating system or applications.
- Application patches. The appropriate patches can mitigate most of the common threats. The ability to ensure patches are in place on all systems reduces the likelihood of being exploited.

## The CyberGatekeeper Solution Family

### **CyberGatekeeper LAN Appliance (CGLAN)**

CGLAN controls endpoint access to corporate LAN/WAN environments. It can be placed anywhere on the network that can communicate to the network infrastructure devices. It uses the VLAN capability on the switches to move individual ports back and forth from the Restricted VLAN to the Production VLAN. The endpoint's CyberGatekeeper Agent sends audit information to CGLAN which decides whether or not the endpoint should have access the corporate network. The rules that specify whether access should be allowed are created by the CyberGatekeeper Policy Manager.

### **CyberGatekeeper Remote Appliance (CGREM)**

CGREM controls access to the corporate network by remote endpoints. CGREM is placed between the company's remote access entry point (typically the VPN or NAS) and the rest of the corporate network. The remote endpoint's CyberGatekeeper Agent sends audit information to CGREM which decides whether or not the endpoint should have access the corporate network. The rules that specify whether access should be allowed are created by CyberGatekeeper Policy Manager.

## Key CyberGatekeeper Components

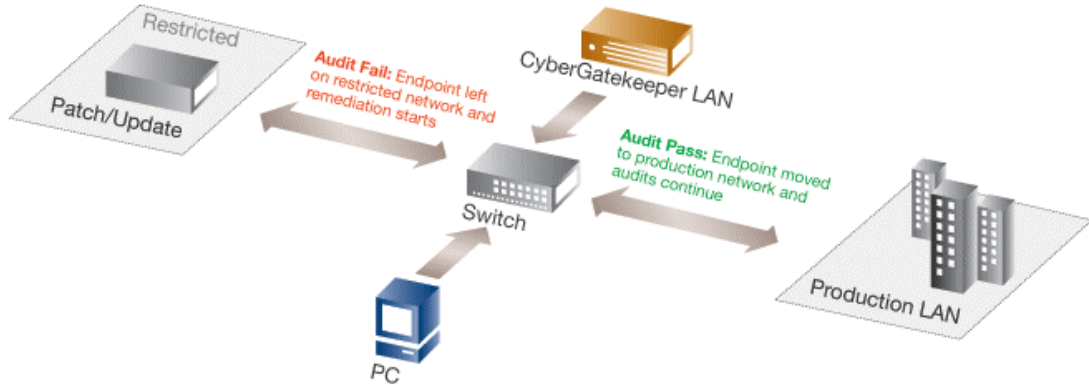
- **CyberGatekeeper Policy Manager (CGPM)**

CGPM lets administrators create policies, build agents, and distribute policies to CyberGatekeeper appliances. Policies contain validation criteria that determine whether endpoints are in compliance with policies or not.

- **CyberGatekeeper Agent (CGAgent)**

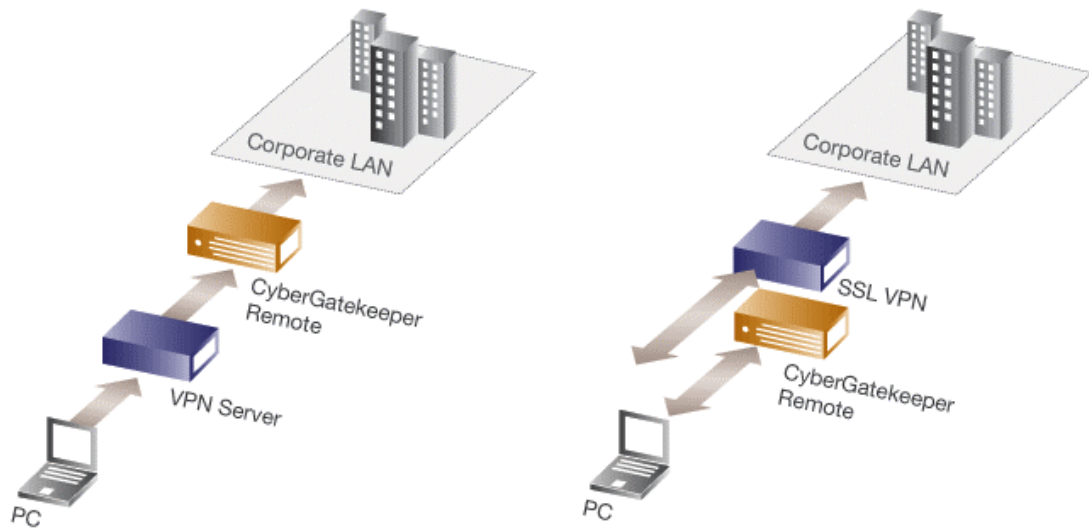
CGAgent runs on endpoints and collects information about them when requested by the CyberGatekeeper server appliance. The appliance determines what information to request and whether the endpoint is in compliance based on the information received. Two types of agents are available: a desktop agent and a web based agent.

Here is a typical scenario of how CyberGatekeeper LAN enforces security inside the network:



A typical session may start with a notebook user connecting to the network. The notebook sits in a quarantine network or restricted LAN until its compliance is verified. The CyberGatekeeper Agent sends the endpoint's system configuration to the CyberGatekeeper LAN Appliance for auditing. If acceptable, the CyberGatekeeper LAN moves the user from the Quarantine network onto the production network and with continuing audit screenings to make sure the computer stays compliant and infection-free. If the computer fails the audit, it is left on the restricted LAN and based on administrator option can be remediated in a number of ways including the downloading of software updates or patches.

CyberGatekeeper Remote performs the same type of endpoint policy enforcement except devices are not maintained in quarantine. An immediate pass or fail of the audit determines the ability to access the network or not. CyberGatekeeper offers Inline Mode via VPN Server or SSL Mode via SSL VPN.



CyberGatekeeper LAN and Remote come with a Policy Manager to create and distribute policies to the appliances. CyberGatekeeper enforces policy compliance through a three-step

process. First, the administrators define and deploy policies from the CyberGatekeeper Policy Manager. Next, CyberGatekeeper audits endpoints for policy compliance before allowing network access. Lastly, CyberGatekeeper grants access to the network if the endpoint is in compliance.

### **CyberGatekeeper Benefits**

CyberGatekeeper's scan and block enforcement overcomes the weaknesses inherent in current endpoint security that lack any type of enforcement capability. In addition to providing an iron-clad, intrusion-free network environment, CyberGatekeeper offers the following benefits:

- **Compulsory Network Edge Enforcement**  
Prevents the spread of worms, Trojans and viruses by scanning all endpoint devices for vulnerabilities or infections. Only compliant machines are allowed access thus making sure networks are available and at peak performance.
- **Pervasive and Vigilant Network Security**  
Secures all remote, VPN, LAN and wireless access points across the enterprise network, and continue to monitor all endpoint devices 24x7.
- **Integrated All-In-One System**  
Because CyberGatekeeper includes extensive Assess, Quarantine, and Remediate capabilities in a single system it can maximize investment by eliminating the need for other point products or act as an umbrella technology to make the most of current non-integrated point products.
- **Compatibility with Existing Heterogeneous Network Infrastructure**  
As CyberGatekeeper integrates with the existing mixed network infrastructure there is no need for costly hardware or software upgrades. CyberGatekeeper delivers value instantly to all organizations from large global enterprises to small and medium sized businesses.
- **Comprehensive Policy Management**  
Centralized policy management system checks OS, endpoint security, among others, for latest updates and version levels. Helps administrators to fine tune policies so they are more robust and more effective than general ones. Improves overall network availability and performance and security.
- **Standards-Based Appliance**  
Standard, network-based appliance provides scalability, performance, and easy deployment on networks of all sizes.
- **User Friendly Non-Intrusive Approach**  
CyberGatekeeper can be deployed on endpoint device or as a Web-based agent based on preference. System is transparent to user requiring little or no intervention.
- **Secure Approach**  
All communication and traffic between components is signed and encrypted to provide privacy and integrity.

## Conclusion

Due to the acceleration of potentially devastating malicious code attacks targeting weaknesses in endpoint devices, a network self defense approach is required. Security must be proactively enforced throughout the network edge. It needs to become more comprehensive, and compulsory as part of an engrained best practice process. Without constant device assessments and enforcement, there is no assurance that networks will ever be intrusion free. A rigorous enforcement process guarantees that endpoint security products such as personal and network firewalls, anti-virus, and security patches are updated and in compliance with corporate security policy. CyberGatekeeper from InfoExpress is the leader in supplying a complete Assess-Quarantine-Remediate enforcement technology to ensure safe, continuous operation of the corporate network.

## For More Information

InfoExpress is a leader in network edge security solutions. The company's CyberGatekeeper product family uses the network edge to enforce configurations, quarantine Trojans and worms, and block unauthorized endpoints. InfoExpress solutions suit companies of all sizes, ranging from small to medium businesses to more than 100,000 seats in Global 2000 organizations. Further information on InfoExpress solutions can be found at [www.infoexpress.com](http://www.infoexpress.com), or by calling 613-727-2090. Email inquiries can be sent to [sales@infoexpress.com](mailto:sales@infoexpress.com).