

Enforcing Network Integrity Using CyberGatekeeper from InfoExpress



InfoExpress T. 650.623.0260 F. 650.623.0268 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: GE10-0501-04

Introduction

Battling viruses and worms that continue to impact business operations and threaten the integrity of networks continues to be a major challenge for network and security administrators. Failure to implement more comprehensive network security has resulted in an array of problems, including restricted bandwidth, computer downtime, loss of employee productivity, and a negative financial impact.

The Aberdeen Group estimates organizations suffer an average \$2M loss per Internet-related security incident that disrupts core business operations. Today's self-propagating viruses can quickly spread throughout a network in a matter of minutes from a single endpoint device that has been infected. As a result, Aberdeen has observed that over 82% of enterprise organizations have dramatically shifted their security strategies to better avoid and prevent the damaging affects of a malicious code attack. Finding proactive measures to the network virus problem is the new holy grail of security.

It is well known and documented that virus writers prey on vulnerable computers that are out of compliance with system or application software security policies. These non-compliant machines offer the open door in which a virus can be successfully implanted. Organizations are even more vulnerable when devices such as home computers or mobile laptops are not under the strict control and monitoring of network administrators. This lack of consistent control often leads to infections among policy or patch deficient devices. Furthermore, these infected devices then serve as the launch pads for spreading a virus deep into the network and to other network connected devices.

In order to combat today's highly virulent code attacks, network security strategies must divorce themselves from a sole reliance on static perimeter defenses such as firewalls, anti-virus protection and intrusion prevention, and be prepared to adopt the next-generation of network security where persistent and proactive policy enforcement technology is integrated into everyday network operations. Only by incorporating an advanced proactive approach can true network integrity, availability and performance be maintained.

CyberGatekeeper Solution Overview

CyberGatekeeper from InfoExpress is the leading technology for proactive network security enforcement. It uses the existing network infrastructure to form a broad, all-encompassing network security umbrella. By isolating non-policy compliant endpoints, CyberGatekeeper not only blocks potentially damaging infections and intrusions, but also helps strengthen all existing perimeter security solutions. For example, corporate security policy requires all endpoint devices to have the most recent anti-virus signatures installed. With CyberGatekeeper, administrators are assured that this policy will be enforced as all machines are quarantined until they have been thoroughly scanned and checked for compliance.

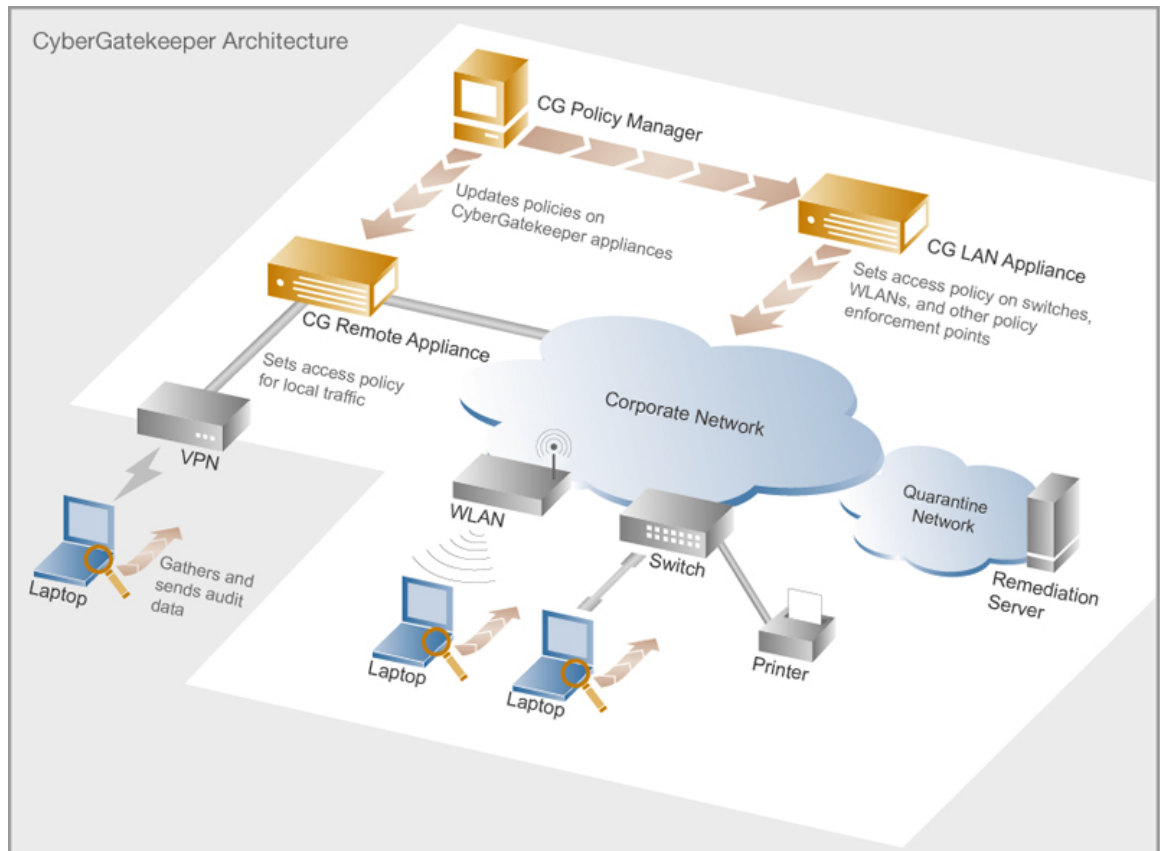
CyberGatekeeper is capable of surveying diverse endpoints, including laptops, desktops, servers, and wireless devices for vulnerabilities, wrong configurations, infections, and other non-compliance violations of security policy. By blocking vulnerable or infected systems, CyberGatekeeper proactively maintains a high level of network integrity for continued smooth operation, availability and peak performance.

CyberGatekeeper offers two solutions: The CyberGatekeeper LAN Appliance controls endpoint access to corporate LAN and WLAN environments, and the CyberGatekeeper Remote Appliance controls network access for remote endpoint devices, typically through VPN connections.

Key Components of CyberGatekeeper

Three main components serve as a foundation for both CyberGatekeeper LAN and CyberGatekeeper Remote network integrity enforcement solutions: the CyberGatekeeper Policy Manager (CGPM), CyberGatekeeper Server (CGS), and the CyberGatekeeper Agent (CGA). These components are used to create and distribute policies, gather information to audit endpoints for compliance, and to control access based on audit results.

The CyberGatekeeper architecture is designed to provide organizations with flexible and strong enforcement capabilities for all types of users, endpoints, and access points. The combination of components provides scalable policy for users accessing the network remotely over VPN or dialup, LAN, wireless access points, and within the network. Because the solution integrates with an organization's existing network environment, CyberGatekeeper becomes a scalable, proactive defense wherever and whenever endpoint devices seek network entry. The diagram below shows how these components are typically positioned within the network.



CyberGatekeeper Policy Manager (CGPM)

CyberGatekeeper offers an extensive and flexible policy management system that allows administrators to create policies that specify compliance criteria and remediation options, and distribute policies to CyberGatekeeper Servers. Dozens of policies may be defined with the CyberGatekeeper Policy Manager. Conditions within policies are built on top of previous ones to reduce the effort when creating custom policies. CGPM comes preloaded with many predefined tests, but the system also lets administrators define their own tests. This lets administrators create custom tests for applications that are not included, that can be incorporated into policies and that are enforced by CyberGatekeeper Servers.

CyberGatekeeper Server Appliance (CGS)

A key function of the CyberGatekeeper Server appliance is to allow or prohibit access to the corporate network. When used in in-line mode, the CyberGatekeeper appliance can enforce remote access (typically VPN or NAS) to the rest of the corporate network. For non-inline operation, the appliance is placed anywhere on the network so long as it can communicate with network enforcement points such as switches or wireless access points. Regardless of the method used, CyberGatekeeper Server audits the endpoint for compliance to determine whether to grant access to the network.

CyberGatekeeper Agent (CGA)

The CyberGatekeeper Agent software performs the deep inspection necessary to collect key information about the end user's system. CGA sends audit information to the CyberGatekeeper Server appliance, which determines if access should be granted to the corporate network. CGA is distributed to users as a stand-alone, self-extracting installer created by the CyberGatekeeper Policy Manager.

CGA is given a list of items to check by the CyberGatekeeper Server. These items are based on the policies distributed to the server appliances and are sent back to the Server. CGA collects the requested information (such as registry keys, etc) and sends the data back to CGS, which compares it to the appropriate policy and determines if the end system is in compliance. If an endpoint is not in compliance, it can be immediately remediated or asked to perform some other action.

Depending on customer requirements, CGA is offered in two versions-- a desktop agent and a Web agent. The desktop agent runs automatically and transparently in the background on the user's system to provide deep scanning on an endpoint device. No interaction by the user is required. The Web agent runs on systems when a browser is launched and the user accesses a specific Web site.

CyberGatekeeper LAN Appliance

The CyberGatekeeper LAN appliance controls access to the network for endpoints attached to switches, wireless LANs, and other network equipment. Compliant endpoints are allowed onto the production network, and non-compliant endpoints remain isolated from the network. To ensure the system is scalable, normal data traffic such as email or file sharing does not pass through CyberGatekeeper LAN.

CyberGatekeeper LAN can be positioned anywhere on the network that has connectivity to the network access points that it is managing. Access to the LAN is enforced by managing switches at the port level or wireless devices at the session level. Devices attaching to enforced access points are placed into an isolated network by default, and remain there until they have audited with CyberGatekeeper. Systems in compliance are granted access to the production network while all others remain quarantined on the restricted network.

When a system connects to the switch, an audit is automatically initiated. This audit scans the internal configuration of the system and allows the CyberGatekeeper appliance to determine if they are in compliance with the security policy administrators have deployed.

For systems that are not in compliance, nothing needs to change because they are already on an isolated network. While being quarantined, systems can be remediated and kept off the production network. CyberGatekeeper automatically reassesses the non-compliant systems to see if they have been remediated, and if so, grants access to the network.

CyberGatekeeper Remote Appliance

The CyberGatekeeper Remote appliance controls access to the network for endpoints that are connecting through a remote access VPN or dialup connection. It filters all traffic to and from remote systems and the rest of the network, only allowing traffic from endpoints that are compliant with security policies.

Traffic from endpoints that fail the audit is blocked or redirected, except for traffic to remediation servers and limited network services. Because the CyberGatekeeper Server appliance is located behind the VPN concentrator or dial-up pool, a failed audit does not interrupt the user's RAS session. Even if access to internal systems is restricted, users still have means to bring their systems into compliance and obtain regular network access.

Benefits of CyberGatekeeper

Protects Against Network Infections

Prevents the spread of viruses and worms by scanning all endpoint devices for vulnerabilities or infections prior to allowing network access. Endpoints default to a quarantine area, and only compliant machines are allowed access, thus keeping networks free from infection.

Pervasive Network Enforcement

Secures all remote, VPN, LAN and wireless access points across the enterprise network, and continues to monitor all endpoint devices for compliance 24x7.

Compatible with Networks

Integrates with the existing network infrastructure, so there is no need for costly hardware or software upgrades.

Works with All Third Party Applications

Checks for OS versions, system updates and versions, programs, and other configuration information. Administrators can create custom policies.

Easy to Deploy and Manage

Scales to support very large networks by providing a single policy management interface for all access points, low bandwidth and non-intrusive agents, and support for a variety of endpoint platforms.

Integrated Enforcement Solution

CyberGatekeeper offers a common administrative and end user experience regardless of the type of access or the type of enforcement point. Users enjoy a consistent experience when accessing the network through a VPN, LAN, or WLAN.

Administrators benefit from having a single set of policies that can apply to all enforcement points, or can define policies that only apply to certain enforcement points. The combination of a single interface for administrators and end users creates a scalable solution to enforce network integrity for enterprises.

Why InfoExpress?

InfoExpress has been in the endpoint security business for over a decade and pioneered the first endpoint policy enforcement solution with the delivery of CyberGatekeeper Remote in 2002.

Today, the CyberGatekeeper suite is the leader in endpoint policy enforcement for open and heterogeneous network environments. InfoExpress has received numerous product awards, and in 2004 was recognized by the Gartner Group as one of eleven 'Cool Vendors in Security and Privacy' for Innovation, market impact and Intrigue.

Further details can be obtained by calling InfoExpress at 613-727-2090, email to info@infoexpress.com, or by visiting our Website at www.infoexpress.com.