C·O·M·O·D·O
ENTERPRISE

Enterprise Security Solutions

Driving Company Security and Profitability Through Centralized Management for PC Endpoint Security

The Challenge

Businesses with 5-250 desktops face multiple PC endpoint security challenges, including:

- Limited IT staff resources
- Limited software budgets
- Non-standard PC endpoint software image/configuration
- Immature and/or loosely enforced security policies
- High staff turn-over
- Lots of virtual and other away from office work

Threats to Company Security and Profitability

These challenges pose threats to both company security and profitability. The security threats are more obvious; even a small proportion of un/under-protected PC endpoints can jeopardize an entire business. Just having some form of security software deployed on each PC endpoint within a business is better than not having it, but only marginally better. Leaving the administration of that software up to each individual user is a recipe for a security breach – again, a single computer with weak security is the proverbial weak link in your company's security chain.

The threats to business profitability arising from this situation are many. Just a modest incident can take computers off-line for hours, impacting company productivity, customer, and business partner relationships. With so many businesses of this size being “knowledge businesses” where the product is information being produced, stored, and distributed via company computers, data loss or data theft has potential ramifications well beyond lost productivity. In a very real sense, that information is the company itself. Even prior to an incident, utilizing understaffed and overworked IT staff in an attempt to keep each individual PC endpoint secure one-at-a-time is a costly exercise, and one that takes away from other pressing tasks that can improve employee productivity, customer satisfaction, and similar contributors to profitability. Finally, “doing the job right” has historically required costly software licensing from security software companies.

Key Strategy: Centralized Management of PC Endpoint Security Software

Centralized management of PC endpoint security software can enhance both company security and profitability. Centralized management gives qualified systems administrators within an organization the ability to manage global, or workgroup security policies from their own desktop console, delivering the necessary rigor and control today’s business environment demands. From a security perspective, this means that critical items ranging from installing updates, configuring security levels, and allowing/disallowing various programs to run or even be installed are done centrally by a trained professional, rather than a PC endpoint at a time by a harried, frequently disinterested in the consequences of their actions, the user. Even in organizations with minimally defined, formal security policies, taking this step can go a long way in lowering the security risk to a business.

Business profitability is enhanced through increased productivity of both IT staff and the employee base at large, as ad-hoc, manual processes are replaced by standardized, automated ones. PC endpoint or network outages are likely to be reduced as a result of more effective security policy enforcement. In short, the organization as a whole functions better.

Comodo Endpoint Security Manager – A Fresh Approach to Centralized Management

Once installed, Endpoint Security Manager can be configured to scan for all endpoints connected to the network using either Active Directory or Workgroup environments. Through the use of a single agent installed remotely, Endpoint Security Manager’s intuitive interface allows for centralized management of security policies and task scheduling. Additionally, Endpoint Security Manager can be configured to protect registry keys from being changed by malicious programs, port monitoring and more all from a single console.

Comodo Endpoint Security Manager and Comodo Firewall Pro – A Great Starting Point for Small and Midsize Companies

Leveraging Comodo's s award-winning Firewall as the first line of defense provides 360° protection against internal and external threats. Comodo Endpoint Security Manager combines an enterprise-class packet-filtering firewall with an advanced host intrusion prevention system (HIPS) that blocks viruses and malware before the program has the opportunity to install. Furthermore, the preventative and proactive A-VSMART™ (Anti-Virus, Spyware, Malware, Adware, Rootkit and Trojan) technology further protects against multiple threats.

Comodo Firewall Pro should be the first and primary line of defense for security and protection within any organization. Comodo's best-in-class low resource utilization ensures seamless and unobtrusive end-user operation not typically seen in software from other security vendors.

It provides the ability to control all execution paths. Simply put, if malware is unable to receive CPU time, it will be unable to execute. Therefore, preventing malware from executing inherently protects the endpoint from becoming infected and ultimately spreading malware throughout the network. The basic concept behind HIPS is to control all execution paths, such that no opportunity exists for malware to execute. In addition to monitoring CPU usage, through the use of Comodo Firewall Pro, critical components such as memory, port and registry settings are monitored and protected from malware.

Taking an advanced approach to malware prevention involves application white-listing, which utilizes Comodo's database of thousands of programs known to be safe. This approach replaces an old methodology of requiring daily signature updates. This presents a vulnerability to users who do not have the latest signatures installed. The programs may become infected between the time the security vendor develops a signature for the malware and releases an update. White-listing takes preventive measures to maintain a strong defense.

Comodo Endpoint Security Manager – A Solution You Can Grow With

Comodo is a security industry innovation leader, with a growing portfolio of PC Endpoint security products. Our Endpoint Security Manager customers will soon have access to a broad range of PC-Endpoint security solutions in addition to the industry's top firewall. Planned introductions include Anti-Virus, Disk Encryption, DiskShield and SecureEmail. Policies and controls for all of these and future solutions will be manageable from a single administrator console.

About Comodo

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet providing enterprises with a comprehensive array of PKI Digital Certificates, eCommerce Acceleration and Infrastructure Security solutions including Enterprise Endpoint Security software, UserAccessAuthentication (Two-Factor / Multi-Factor), Network Vulnerability Scanning and PCI compliance services.

Comodo secures and authenticates the online transactions, communications and endpoints for over 200,000 business customers and 3,000,000 users of our desktop software products.

Continual innovation, a core competence in PKI, and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development.

Comodo Security Solutions, Inc.

525 Washington Blvd.
Jersey City, NJ 07310
United States

Tel: +1.888.256.2608
Tel: +1.703.637.9361
Fax: +1.201.963.9003

Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay
Trafford Road, Salford, Manchester M5 3EQ
United Kingdom

Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 7025

For additional information on Comodo - visit **http://www.enterprise.comodo.com/**