TotalCOMMAND™

70% of security problems patch-related

Gartner Group reported that 70% of security incidents can be traced to patching issues. Another study by Carnegie Mellon University revealed that 99 percent of all intrusions arise from exploitation of known vulnerabilities and security holes. This demonstrates the importance of regularly patching corporate systems and keeping current with network and system security.

However, time constraints are a major issue for administrators wanting to keep their networks in optimal order. Administrators have to actively search and locate the appropriate patches, test and verify them for compatibility, and then apply them to each desktop or server system.

A study by UK-based managed security services provider, Activis, indicates that a company with an infrastructure of 9 NT servers and 8 firewalls, for example, would have needed 1,315 updates during the first 9 months of last year. That works out to 5 updates per working day, not to mention having to manage 500,000 log entries every day, the study adds.

And while many shops now automatically update virus definitions, patches for security vulnerabilities still need to be installed manually. "Although we take great pains to make certain all of our mission critical servers are patched promptly, we are lacking sometimes at rolling out these patches to our workstations," said Timothy Bruess, network manager with Learning Resources, Inc. of Vernon Hills, Ill.

auto-patching critical to future business success

Auto-patching solutions such as Command Software's TotalCOMMAND can reduce a typical manual patch deployment for 1,000 workstations - a task that could take more than 350 man-hours if done manually - to a fully-automated process, overnight. In addition, TotalCOMMAND can save administrators countless hours - hours that currently go into researching and identifying the necessary patches, or dealing with the business consequences of system vulnerability.

In addition to avoiding downtime and the man-hours needed to restore and fix systems and networks damaged by hacker attacks, a regularly patched network results in numerous benefits and savings, such as optimized system performance, improved uptime, and higher data integrity. In today's business environment, these benefits are critical to future success.

COMMAND an Authentium company

we build trust

TotalCOMMAND™

TotalCOMMAND™

Command Software's TotalCOMMAND provides secure, enterprise-wide vulnerability patching and software management. TotalCOMMAND incorporates patent-pending fingerprinting technology that fully automates the patch process. With TotalCOMMAND IT administrators can easily, efficiently and securely distribute security patches to workstations and servers across their entire network.

TotalCOMMAND includes:

- Secure web-based management interface
- Remote deployment of critical security patches
- Support for Internet and ISOnet delivery
- Powerful hardware and software inventory analysis
- Extensive patch archive; fast and easy installation
- Administrator-definable trusted signature verification
- Fully encrypted SSL-based Data Transmission

TotalCOMMAND operates continuously and is capable of automatically scanning entire networks for patch-related security holes and other potential security problems. When a problem is found, TotalCOMMAND allows IT administrators to immediately correct the vulnerability across all computer platforms and enterprise boundaries, before the vulnerability can be exploited by hackers.

"... a slick Web-based interface that anyone familiar with any Web-based administration tool will find easy to use" - Mandy Andress, Network World, 02/04/02

sales

United States
PH (561) 575-3200 • FAX (561) 575-3026
www.commandsoftware.com

Asia Pacific
PH +61(03)9762 2203 • FAX +61(03)9762 0847
www.commandcom.com.au

Europe
PH +44(0)207 931-9301 • FAX +44(0)207 931-9302
www.command.co.uk

Canada
PH (877)243-9669 • FAX (905)987-4823
www.commandsoftware.com

COMMAND SOFTWARE SYSTEMS