*Stop hackers before they get through*

# Tivoli Cross-Site for Security

## Highlights

***Fosters e-business growth by scaling to fit evolving needs—without exposing your existing networks to security threats***

***Detects hacker attempts in realtime, and sends prioritized alerts***

***Updates security clients automatically with new detection signatures***

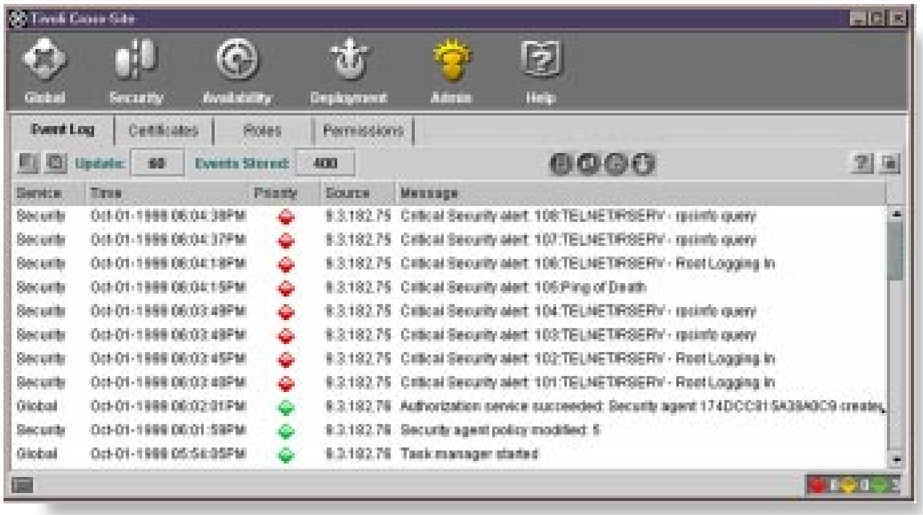
***Prevents hacking through a secure architecture that uses 128-bit encryption[1] for all management server to security agent communications***

***Helps improve your return on investment through fine-grained tuning of security agents, reducing the number of false alarms***

***Offers extensive, easy-to-use reporting features which deliver quick views of detailed intrusion data***

***Allows flexible deployment so that you can avoid disrupting your production environment***

In a ten-year period, the number of certified security incidents reported yearly to CERT Coordination Center® (CERT®/CC) increased from virtually none to over 4,000.[2] The reason for the increase? More businesses are exposing more of their critical business systems as the practice of conducting e-business becomes a requirement for success. Clearly, the increased exposure is unavoidable if you're trying to remain competitive. But security holes may appear at many levels in your enterprise, including applications, databases, operating systems and networks.



Update: 60 Events Stored: 400

| Service | Time | Priority | Source | Message |
|---|---|---|---|---|
| Security | Oct-01-1999 06:04:38PM | 🟥 | 9.3.182.75 | Critical Security alert: 108:TELNETIRSERV - rpcinfo query |
| Security | Oct-01-1999 06:04:37PM | 🟥 | 9.3.182.75 | Critical Security alert: 107:TELNETIRSERV - rpcinfo query |
| Security | Oct-01-1999 06:04:18PM | 🟥 | 9.3.182.75 | Critical Security alert: 106:TELNETIRSERV - Root Logging In |
| Security | Oct-01-1999 06:04:15PM | 🟥 | 9.3.182.75 | Critical Security alert: 105:Ping of Death |
| Security | Oct-01-1999 06:03:49PM | 🟥 | 9.3.182.75 | Critical Security alert: 104:TELNETIRSERV - rpcinfo query |
| Security | Oct-01-1999 06:03:48PM | 🟥 | 9.3.182.75 | Critical Security alert: 103:TELNETIRSERV - rpcinfo query |
| Security | Oct-01-1999 06:03:45PM | 🟥 | 9.3.182.75 | Critical Security alert: 102:TELNETIRSERV - Root Logging In |
| Security | Oct-01-1999 06:03:40PM | 🟥 | 9.3.182.75 | Critical Security alert: 101:TELNETIRSERV - Root Logging In |
| Global | Oct-01-1999 06:02:01PM | 🟩 | 9.3.182.76 | Authorization service succeeded: Security agent 174DCC91 5A39A0C9 create |
| Security | Oct-01-1999 06:01:59PM | 🟩 | 9.3.182.76 | Security agent policy modified: 5 |
| Global | Oct-01-1999 05:54:35PM | 🟩 | 9.3.182.76 | Task manager started |

*This consolidated realtime view shows all alerts from deployed agents.*

e-business

# *Detect, log and respond to intrusions–in realtime*

At the same time that security exposure is increasing, hackers are becoming more sophisticated—and more malicious. Unfortunately, a significant number of all malicious attacks come from people inside your own enterprise. Whether your business systems are hacked by those seeking thrills, by competitors trying to obtain confidential information for their own gain, or by a dissatisfied employee who intends to damage your business systems or security structure, you must find a reliable, trustworthy solution for protecting your business assets against security threats to help ensure your success.

## Detect, log and respond to threats—before they get through

Establishing a way to quickly and reliably detect, log and respond to security threats—without hindering business growth or tying up all your security resources with manual processes—is what Tivoli® Cross-Site™ for Security is all about. A component of IBM SecureWay® FirstSecure, Tivoli Cross-Site for Security is a network-based intrusion detection product that detects, logs and responds to intrusion attempts in realtime. Tivoli Cross-Site for Security can protect against the latest varieties of hacker attempts, including denial of service, port scanning and attacks specific to application services, such as telnet, FTP and DNS.

## Realtime intrusion detection from leading security experts

Tivoli Cross-Site for Security provides two components to perform realtime intrusion detection. One is the Tivoli Cross-Site for Security agent; the other is a management server with a Java™ console. The two components work together to watch for and respond to attack signatures in packets or data streams on the network. IBM teams, including  IBM's Global Security Analysis Laboratory (GSAL), work in partnership to identify and deploy new intrusion signatures. After being validated, new attack signatures are made available on the Tivoli Cross-Site Web site for authorized users to access. The security management server can automatically distribute the signatures to security agents, or you can choose to evaluate the signatures before sending them to agents.

## Security agent

The security agent is placed on key systems in your enterprise, such as Web servers and databases. When the security agent detects a match between an incoming signature and one of the current, validated GSAL attack signatures, it sends an alert to the management server component. The prioritized alerts are displayed in the GUI from the management console, allowing administrators to take immediate action.

Each agent's policy is configurable, allowing you to specify the parameters that trigger alerts, including activity type, source, destination and time of day. You can also associate policy violations with differing levels of severity, such as critical, serious or non-critical—allowing your staff to respond appropriately to different types of alerts. Agents can be deployed on a dedicated system that monitors traffic for a designated area of the network, or on an individual network server. This provides efficient monitoring of non-critical network areas, allowing redundant monitoring in highly sensitive areas like human resources or finance.

## Management server and console

The Tivoli Cross-Site for Security management server and console work together to monitor and display realtime alerts sent from agents throughout the network—inside and outside of the firewall or boundary server. This Tivoli Cross-Site for Security application is installed on a central management server, and allows you to manage events originating from agents, administer policy for agents and produce reports.

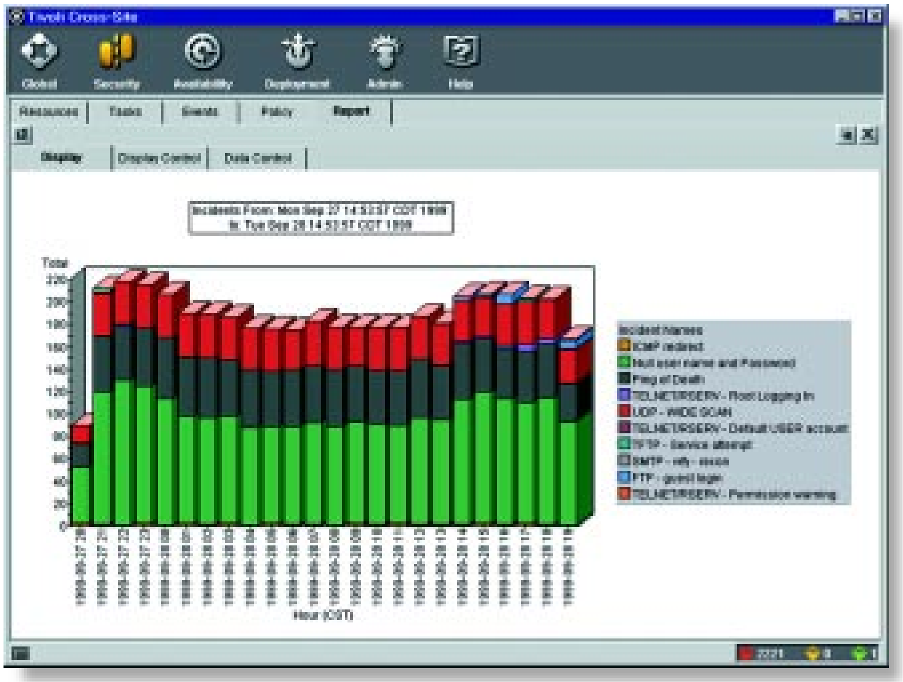
With this architecture, all communications between security agents and the management server can be encrypted using 128-bit[1] Secure Sockets Layer (SSL). And because communications between agents and the server are initiated by the agents, hackers can be prevented from obtaining and spoofing the unique identity of an agent. These agents can be updated on the fly through the use of Marimba's Castanet technology. Designed to be highly scalable, each management server can manage up to 60 clients. For highly distributed environments that demand server-to-server communication, the Tivoli Enterprise Console™ can be used as the top tier of a structure that consolidates control through a master server.

### Track hacker attempts with extensive reporting features

No matter what steps you take to prevent security breaches, someone may still try to hack your system. To effectively combat hacker attempts, you need to know what happened, where it happened and when it happened. Having this knowledge is the only way you can track hacker attacks and prevent them from happening again. With Tivoli Cross-Site for Security, you get extensive reporting features that can be used to generate predefined reports, or you can create your own custom reports using the report generator.

You can generate reports designed to show security events for individual agents, for all agents or for a specified group of agents. Many types of reports can be generated, including incident versus time, severity versus time, incident versus source host and source host versus incident type.

You can use detailed reports to examine and compare various aspects of incidents. For example, you can use reports to show the severity of alerts generated by incidents; the port number used by the system for which the attack was intended; the IP address of the destination host; and in some cases the group ID or user ID of the person who initiated the incident. Reports can be stored in a relational database—such as IBM DB2® or Oracle—where they can be accessed by third-party tools and used for investigations or management reports.



*This built-in report shows a summary of attacks by category.*

### Supported platforms

Tivoli Cross-Site for Security runs in the following operating environments: Sun Solaris™ 2.6 or 2.7; Microsoft® Windows NT® 4.0 with SP4 or higher; and IBM AIX® 4.3.2. This product supports Oracle 7.3.4 or higher databases and Netscape Enterprise Server 3.5.1 or higher.

### Open for trusted e-business with IBM SecureWay FirstSecure

IBM SecureWay FirstSecure enables companies to build and operate secure and trusted environments to conduct e-business. FirstSecure offers an integrated, policy-driven solution for your IT security needs, including digital identities, network boundary protection, detection for viruses and intrusions, and tools for developing secure applications.

FirstSecure relies on the strengths of industry-standard technologies, along with the security expertise of IBM and other leading security vendors. With FirstSecure, your enterprise can achieve intrusion and virus immunity using Tivoli Cross-Site for Security in conjunction with Norton AntiVirus™/IBM Solution Suite.

Tivoli Cross-Site for Security is available as part of IBM SecureWay FirstSecure.

### For more information

To learn more about Tivoli Cross-Site for Security and IBM SecureWay FirstSecure, visit:
*www.ibm.com/software/security/firstsecure*

IBM Corporation
Department VK4A
3039 Cornwallis Road
Research Triangle Park, NC 27709

Produced in the United States of America
10-99
All Rights Reserved

[1] 128-bit encryption available in the North American version only; other versions use 56-bit encryption.

[2] Study by Carnegie Mellon Software Engineering Institute CERT Coordination Center, 1998 - 1999. For more information, see *www.cert.org/stats/cert_stats.html.*

♻

Printed in the United States on recycled paper containing 10% recovered post-consumer fiber.