

IBM Tivoli Risk Manager

Highlights

- ***Provides a single centralized view of security data across your enterprise***
- ***Helps integrate security management from applications, operating systems and network devices***
- ***Can reduce and classify security incidents to quickly identify and address real threats or vulnerabilities***
- ***Helps provide business intelligence that enables organizations to proactively address their business risks using analytical historical reporting guides***
- ***Provides predefined tasks to help quickly resolve denial-of-service attacks, viruses or unauthorized access***
- ***Assists organizations with audit compliance (event data persistence)***

The fast pace of e-business deployments means that more enterprise systems, applications and data are accessible to the Internet community. As a result, businesses face increasing risks from a multitude of fronts—virus threats, unauthorized access, denial-of-service attacks and other forms of intrusions that target e-business applications, networks, hosting infrastructure, servers and desktops.

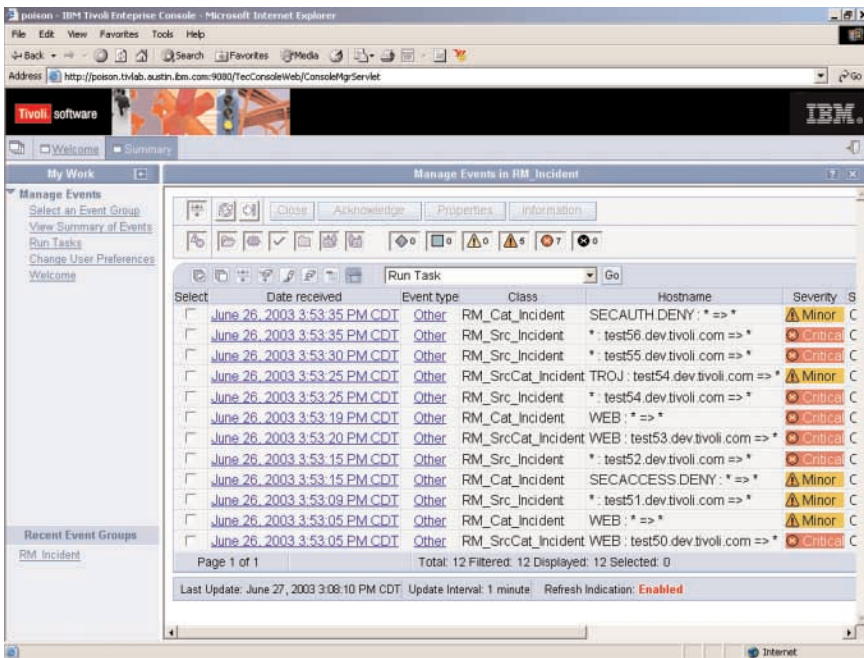
In this highly competitive environment, customers are demanding the highest quality of service, trust and security from corporations. Implementations of e-business should be secure, enforce the privacy of business transactions, protect the integrity of business operations, protect customer data and provide around-the-clock access. Businesses that have carefully built their brands understand that brand equity in the Internet world can be quickly eroded or destroyed by an attack. IBM Tivoli® Risk Manager can help you centrally manage security incidents and vulnerabilities across your enterprise.

Enterprise risk management

Enterprise risk management lets you manage external and internal vulnerabilities. You can proactively address vulnerabilities and exposures in an enterprise context by harnessing intelligence across different security checkpoints to gain knowledge and insight into the root causes of these problems, and you can use decision support to quickly upgrade your security policies.

Centralized management of incidents

Tivoli Risk Manager manages security incidents from a single security console. The communications and control center centrally manages enterprise vulnerabilities and can help you centrally detect and assess attacks, threats and exposures by correlating security information and risk alerts from firewalls, routers, networks, host- and application-based intrusion detection systems, desktops, and vulnerability-scanning tools. The centralized console provides real-time visualization and management of security incidents.



Tivoli Risk Manager provides a centralized view of your enterprise-wide security.

Tivoli Risk Manager provides the following functions to centralize risk management:

- Centralized correlation of security alerts and vulnerabilities
- Centralized archive of security alerts in the relational database
- Scalable event management infrastructure to manage events from thousands of security devices
- Single enterprise console to help your security analysts understand overall exposure and quickly implement policy modifications to mitigate risk
- Decision support, including predefined reports for firewall management, intrusion detection, risk assessment and virus management
- Wireless security auditor capability to audit a wireless network for proper security configuration

Integration with IBM Tivoli Enterprise Console and IBM Tivoli NetView

Tivoli Risk Manager now also includes IBM Tivoli Enterprise Console® and IBM Tivoli NetView®. Integration between Tivoli Enterprise Console and the Tivoli NetView consoles gives you the capability to drill down to the network topology to see where affected resources are located. This drill-down support includes the node-specific ability to run diagnostics or view object properties. The capability to drill up from the network console to determine other resources that might be affected as a result of a network outage is also available. Tivoli Risk Manager provides out-of-the-box rules that correlate security events with network and availability events. Examples include:

- **IBM Tivoli Monitoring/Tivoli Risk Manager event linkage:**
 - Tivoli Monitoring alert indicates server has unusually high CPU utilization or availability problem.
 - Tivoli Risk Manager alert indicates **same** server is target of denial-of-service attack.
 - Result: Rule will link events as related and severity will be adjusted as appropriate.

- **Tivoli NetView/Tivoli Risk Manager event linkage:**
 - *Tivoli NetView alert indicates that resource is down or unavailable.*
 - *Tivoli Risk Manager alert indicates that **same** resource is under attack or target of suspicious activity.*
 - *Results: Rule will link events as related and severity will be adjusted as appropriate.*

Heartbeat capability

The Tivoli Risk Manager components produce periodic “heartbeats,” and the upstream servers use special rules to detect missing heartbeats. An “agent inactive” alert is generated when the heartbeat for a specific system is not received in a timely fashion. This capability also can be used to track “keep alive” alerts from third-party sensors and adapters.

Integration with Tivoli identity management solution

Tivoli Risk Manager integrates with IBM Tivoli Privacy Manager, and accepts events from IBM Tivoli Access Manager for e-business, IBM Tivoli Access Manager for Business Integration and IBM Tivoli Access Manager for Operating Systems. Tivoli Risk Manager can correlate

and evaluate these events along with other enterprise events.

Integration with Tivoli Data Warehouse

Tivoli Risk Manager now also includes Tivoli Data Warehouse. Tivoli Risk Manager can store security events in the data warehouse for long-term persistence. Tivoli Data Warehouse also can store events from other sources, such as configuration and monitoring. New data warehouse reporting capabilities can be used to leverage the information.

Autonomic computing capabilities

Tivoli Risk Manager delivers on the autonomic computing tenets of self-configuration and self-protection by assessing potential security threats and automating responses such as server reconfiguration, security patch deployment and account revocation. Based on incidents, Tivoli Risk Manager can automatically launch tasks such as:

- *Deny connections from/to an IP address on the firewall.*
- *Upgrade software to prevent or stop threats.*
- *Close existing connections from/to an IP address on the firewall.*
- *Kill user process on a server.*
- *Cancel enabled rules on the firewall.*

Tivoli Risk Manager Integration Toolkit

With the Integration Toolkit, security events can easily be integrated with Tivoli Risk Manager. Based on the Intrusion Detection Message Exchange Format (IDMEF), a draft Internal Engineering Task Force (IETF) standard, the intrusion event data format provides a common alert format for security devices to send security events to the management console. By converting alerts into IDMEF format, new security technology products can quickly leverage the enterprise management and correlation capabilities of Tivoli Risk Manager.

Support of Ready for IBM Tivoli products

Tivoli Risk Manager provides out-of-the-box integration with security technology products from several leading-edge providers such as ISS, Cisco, Symantec, Network Associates and Check Point. Several independent software vendor and security providers—such as Tripwire, Sanctum, NFR, Secure Computing and Zone Labs—have solutions that interoperate with Tivoli Risk Manager. Together these solutions can help you implement a comprehensive security framework for your enterprise and e-business.



Tivoli Risk Manager

Platforms

Microsoft® Windows NT® 4.0, Windows® 2000, Windows XP
Sun Solaris 2.8, 2.9
IBM AIX® 5.1, 5.2
HP-UX 11
Linux on xSeries®, zSeries®, iSeries™ and pSeries®

Language support

English, Japanese, French, Brazilian Portuguese, Korean, Simplified Chinese, German, Italian and Spanish

For more information

To learn more about Tivoli Risk Manager and integrated solutions from IBM, contact your IBM sales representative or visit ibm.com/tivoli/solutions/security

Tivoli software from IBM

An integral part of the comprehensive IBM e-business infrastructure solution, Tivoli technology management software

helps traditional enterprises, emerging e-businesses and Internet businesses worldwide maximize their existing and future technology investments. Backed by world-class IBM services, support and research, Tivoli software provides a seamlessly integrated and flexible e-business infrastructure management solution that uses robust security to connect employees, business partners and customers.

© Copyright IBM Corporation 2003

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

09-03
All Rights Reserved

AIX, DB2, the e-business logo, e-business on demand, the e(logo)business on demand lockup, IBM, the IBM logo, iSeries, Lotus, NetView, OS/390, pSeries, Tivoli, Tivoli Enterprise Console, WebSphere, xSeries, z/OS and zSeries are trademarks of International Business Machines Corporation in the United States, other countries or both.

Rational is a trademark of International Business Machines Corporation and Rational Software Corporation in the United States, other countries or both.

Microsoft, Windows and Windows NT are trademarks of Microsoft Corporation in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.