

---

## IBM Tivoli Risk Manager

---

### Plattformen

---

Microsoft® Windows NT® 4.0  
Sun™ Solaris™ 2.7  
AIX® 4.3.3

---

### Sprachunterstützung

---

Englisch, Japanisch, Französisch, brasilianisches Portugiesisch, Koreanisch, vereinfachtes Chinesisch, Deutsch, Italiensich und Spanisch

---

### Produktvoraussetzungen

---

#### Software

Zu den notwendigen Produkten für den Einsatz mit Tivoli Risk Manager gehören:

Tivoli Management Enterprise Framework, Version 3.6.3 oder 3.6.4  
Tivoli Enterprise Console, Version 3.7

Zu den notwendigen Produkten für den Einsatz mit Decision Support for

Enterprise Risk Management gehören:

Tivoli Decision Support, Version 2.1

---



© Copyright IBM Corporation 2002

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

Printed in the United States of America  
04-02  
Alle Rechte vorbehalten

IBM, das e-business-Logo, das IBM Logo, AIX, pSeries, Tivoli, Tivoli Ready und Tivoli Enterprise Console sind Marken oder eingetragene Marken der International Business Machines Corporation in den Vereinigten Staaten, anderen Ländern oder beidem.

Microsoft, Windows und Windows NT sind eingetragene Marken der Microsoft Corporation in den Vereinigten Staaten, anderen Ländern oder beidem.

Sun und Solaris sind Marken von Sun Microsystems, Inc. in den Vereinigten Staaten, anderen Ländern oder beidem.

Bei sonstigen im Text verwendeten Bezeichnungen von Unternehmen, Produkten und Dienstleistungen kann es sich um eingetragene Marken anderer Unternehmen handeln.

Die Homepage von Tivoli im Internet finden Sie unter **tivoli.com**

Die IBM Homepage im Internet finden Sie unter **ibm.com**

Gedruckt in den USA auf Recycling-Papier mit 10 % Altpapier.

## IBM Tivoli Risk Manager

---

### Highlights

---

- **Überwachung, Ansicht und Verwaltung sicherheitsrelevanter Meldungen in Ihrem gesamten Unternehmen über eine bedienerfreundliche Konsole**
- **gemeinsames Datenformat und gemeinsame Namenskonvention für Meldungen**
- **Reduzierung und Klassifizierung sicherheitsrelevanter Meldungen zur schnellen Erkennung von echten Gefahren**
- **mit einem analytischen und Web-basierten Historienprotokoll als Decision Support; Anzeige der Muster von Einbruchversuchen; Darstellung der Nutzung von Systemen und Netzen sowie der Einhaltung der Sicherheit**
- **vordefinierte Tasks zur schnellen Reaktion auf Denial-of-Service-Attacken, Viren oder unbefugte Zugriffe**

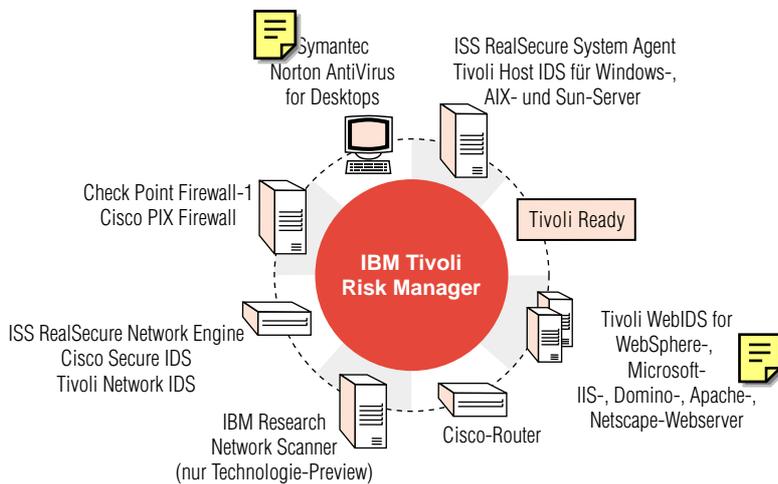
Weltweit bereiten sich Unternehmen darauf vor, im Wettbewerb auf den neuen Internet- und e-business-Märkten gegeneinander anzutreten. Das schnelle Entstehen von e-business-Angeboten bedeutet, dass immer mehr Unternehmenssysteme, Applikationen und Daten für die Internet-Gemeinde zugänglich sind. Dies bedeutet aber auch, dass Unternehmen an zahlreichen Fronten verstärkt Gefahren ausgesetzt sind - Viren, unbefugtem Zugriff, Denial-of-Service-Attacken und anderen Formen von Einbruchversuchen, die gegen e-business-Applikationen, Netze, Host-Infrastrukturen, Server und PCs gerichtet sind.

In diesem heißumkämpften Bereich fordert und erwartet der Kunde von einem Unternehmen die höchste Qualität von Diensten, Vertrauenswürdigkeit und Sicherheit. Eine e-business-Implementation sollte sicher sein, die Vertraulichkeit von Geschäftstransaktionen gewährleisten, die Integrität von Geschäftsvorgängen sowie Kundendaten schützen.

Der IBM® Tivoli® Risk Manager gestattet Ihnen die zentrale Verwaltung von und die Reaktion auf verschiedene Sicherheitsrisiken und Attacken, die sich gegen Ihr Unternehmen richten.

### Enterprise Risk Management

Enterprise Risk Management gestattet Ihnen den Umgang mit internen und externen Bedrohungen. Sie können sich aktiv auf Verwundbarkeiten und Schwachstellen im Zusammenhang mit Ihrem Unternehmen konzentrieren, indem Sie verschiedene Sicherheits-Checkpoints mit Intelligenz ausstatten, um Informationen über die tieferen Ursachen dieser Probleme zu erlangen, und Sie können Entscheidungshilfen verwenden, um Ihre Sicherheitsrichtlinien schnell anzupassen.



Mit dem Tivoli Risk Manager verwalten Sie ein breites Spektrum von Applikationen, Geräten und Produkten in Ihrem Unternehmen.

### Zentrale Verwaltung von Gefahren

Der Tivoli Risk Manager verwaltet sicherheitsrelevante Meldungen von einer einzigen Konsole aus. Das Kommunikations- und Kontrollzentrum verwaltet zentral die Verwundbarkeiten im Unternehmen und unterstützt Sie bei der zentralen Erkennung und Bewertung von Angriffen, Bedrohungen und Schwachstellen durch die Korrelation von sicherheitsrelevanten Informationen und Gefahrenmeldungen von Firewalls, Routern, Netzen, Host- und applikationsbasierten Intrusion-Detection-Systemen und Vulnerability Scanning Tools. Der Tivoli Risk Manager enthält folgende Funktionen für das zentrale Gefahrenmanagement:

- zentrale Korrelierung von Meldungen über Eindringversuche

- zentrale Archivierung sicherheitsrelevanter Meldungen in der relationalen Datenbank
- skalierbare Verwaltungsinfrastruktur für die Verwaltung der Ereignisse von Tausenden von Sicherheitseinrichtungen
- Über eine einzige Unternehmenskonsole erfassen Ihre Security Analysts die gesamte Sicherheitslage und können schnell modifizierte Richtlinien zur Reduzierung von Gefahren umsetzen
- Unterstützung bei Entscheidungen mit vordefinierten Protokollen für die Organisation von Firewalls, Intrusion Detection, Gefahrenbewertung, Virusabwehr und universelle Tivoli Ready™-Protokolle

### Tivoli Network Intrusion Detection System

Das leistungsfähige Tivoli Network Intrusion Detection System unterstützt

mehr als 200 Netzangriff-Signaturen und benötigt dabei wenig Platz auf der Festplatte. Ein wesentlicher Vorteil des Tivoli Network Intrusion Detection System ist seine enge Integration in die Tivoli Enterprise Console® und die Management-Plattform Tivoli. Ihre Systemadministratoren können Intrusion-Detection-Systeme einrichten, neue Signaturen und Richtlinien einführen und Code zentral von einer einzigen Konsole aus verteilen.

### Tivoli Web Intrusion Detection System

Der Tivoli Risk Manager enthält das hochentwickelte Tivoli Web Intrusion Detection System (Tivoli WebIDS), das Sie bei der Überwachung von Einbruchversuchen und verschiedenen Formen von Angriffen auf Webserver unterstützt. Heutzutage werden Angriffe mit raffinierten Mitteln ausgeführt, die Websites mittels HTTP oder HTTPS ins Visier nehmen; diese Arten von Angriffen lassen sich typischerweise nicht durch eine Firewall abwehren und umgehen häufig die Überwachungsfunktionen von Werkzeugen zum Auffinden von Attacken im Netz. Tivoli WebIDS konzentriert sich auf folgende Aktivitäten: Eindringen in das System, Denial-of-Service-Angriffe, legale, aber unerwünschte Aktivitäten, Common-Gateway-Interface-(CGI)Verwundbarkeiten und Richtlinienverstöße. Tivoli WebIDS wird von einer Reihe weitverbreiteter Webserver unterstützt.

### **Tivoli Risk Manager Integration Toolkit**

Mit dem Integration Toolkit lassen sich Ereignisse einfach in den Tivoli Risk Manager integrieren. Auf der Basis von IDEF, einem IETF-Standard im Entwurfsstadium, ermöglicht das Intrusion Event Data Format ein gemeinsames Meldungsformat, in dem Sicherheitseinrichtungen sicherheitsrelevante Ereignisse an die Verwaltungskonsole senden. Durch die Umwandlung von Meldungen in IDEF können neue sicherheitstechnologische Produkte schnell die Unternehmensverwaltungs- und Korrelationsfunktionen des Tivoli Risk Manager nutzen.

### **Unterstützung von Tivoli Management Framework und anderen Tivoli Produkten**

Der IBM Tivoli Risk Manager unterstützt IBM Tivoli Management Framework, die IBM Tivoli Enterprise Console und die Produktfamilie IBM Tivoli.

### **Unterstützung von Tivoli Ready-Produkten**

Der IBM Tivoli Risk Manager unterstützt Sicherheitstechnologie-Produkte von verschiedenen führenden Anbietern von Sicherheitsdienstleistungen. Er bietet standardmäßig die Unterstützung von ISS RealSecure Network-Engine- und Systemagenten, Cisco PIX Firewall, Cisco Secure IDS, Cisco-Router, Check Point Firewall-1, McAfee Active Virus Defense Suite und Symantec Norton AntiVirus. Einige unabhängige Software-Hersteller und -Anbieter von Sicherheitsdienstleistungen - wie z. B. Argus Systems Group, ClickNet Security Technology, LockStep Systems, Deloitte & Touche, Zone Labs, Compaq, SRA International und IBM eServer pSeries™ bieten Lösungen, die mit dem IBM Tivoli Risk Manager zusammenarbeiten und das IBM Tivoli Ready-Logo erhalten haben. Zusammen unterstützen diese Lösungen Sie bei der Umsetzung eines umfassenden Sicherheits-Framework, mit dem Sie Internet-Angriffe auf Ihr Unternehmen und Ihr e-business erfolgreich abwehren können.

### **Hier erfahren Sie mehr**

Weitere Informationen über den IBM Tivoli Risk Manager und integrierte Lösungen von IBM erhalten Sie bei Ihrem IBM Vertriebsbeauftragten. Im Internet finden Sie uns unter **tivoli.com/security**

### **Tivoli Software von IBM**

Als integraler Teil der umfassenden IBM e-business-Infrastrukturlösung unterstützt Tivoli Technologie-managementsoftware etablierte Unternehmen, neue e-Commerce-Anbieter sowie Internet-Unternehmen weltweit bei der Maximierung des Nutzens aus ihren bereits getätigten und zukünftigen Technologie-Investitionen. Basierend auf den weltweit erstklassigen Leistungen, dem Support und der Forschung von IBM, bietet Tivoli Software eine nahtlos integrierte und flexible Managementlösung für die e-business-Infrastruktur, die mit robusten Sicherheitsmerkmalen Mitarbeiter, Geschäftspartner und Kunden miteinander verbindet.