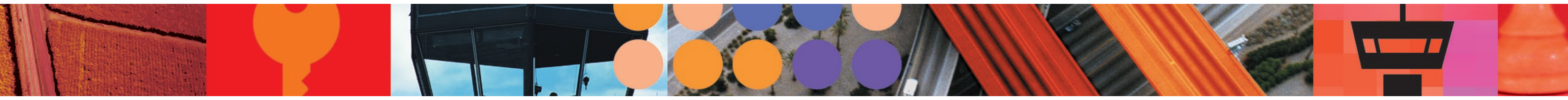
Security solutions
To support your business objectives

Tivoli software

# Regain control over a critical threat to business information integrity and data privacy: privileged users.



## Highlights

- Help prevent unauthorized access by establishing clearly defined user rights and segregation of duties, backed by automated policies
- Spot potential problems and proactively address the risk of insider threats through real-time behavior monitoring
- Resolve threats quickly using near-real-time alerts and correlated analysis

Most businesses harden the perimeters of their IT networks and systems to counter external threats that confront their computing infrastructure, such as those caused by hackers, denial of service attacks or malware. But while protecting your IT systems from external harm is crucial, there's a subtle, yet powerful threat lurking right inside your enterprise: privileged users.

Privileged users are the individuals inside your enterprise who routinely use your IT systems, applications or data to perform their jobs. These trusted insiders have access to critical information and assets and are often highly capable technology users. Whether they perform actions with intentional maliciousness or simply by accident, insiders entrusted with access to your IT systems are the biggest threat to your company's information integrity and data privacy. Studies suggest that approximately 80 percent of security breaches originate from internal sources.*

Clearly, network and database administrators, IT operations staff, employees and managers across lines of business must have access to your IT infrastructure. But many businesses lack appropriate levels of internal visibility into these users' actions. Others rely on manual, time-consuming processes to defend against possible "insider" infringements.

With only insufficient or manual solutions in place, many business leaders today are left to wonder: Have we set up appropriate permissions for each role in our organization? Can we enforce compliance with industry regulations and business policies that protect data privacy and integrity? Do we have a reliable way to quickly identify, track and stop suspicious activities and inappropriate behaviors before they spiral out of control?

To confidently defend your business against insider threats — and demonstrate the efficacy of your approach — you can use solutions from the IBM Tivoli® security portfolio. Comprehensive Tivoli security solutions protect you at one of your most vulnerable points, from the people inside your organization who have legitimate access and are closest to your computing systems. So you can maintain the integrity of financial information and other data, enforce privacy policies and comply with numerous regulations. Use these solutions to:

- Manage access to systems and applications using automated policies to enforce user rights.
- Leverage insight gathered from real-time behavior tracking to spot potential problems and reduce the impact of insider threats.
- Use near-real-time alerts and correlated analysis to resolve threats quickly, and escalate as needed.

**Establish user rights and clearly segregate duties to avert inappropriate access**

In large, heterogeneous computing environments, maintaining appropriate user access to IT systems, applications and data for multiple layers of organizational roles can be a tedious chore. With the IBM Tivoli Access Manager family, you can effectively manage access to business-critical applications and data throughout the enterprise while giving users fast, convenient access to the information they need.

IBM Tivoli Access Manager for e-business lets you manage user entitlements in alignment with your corporate security policy. To enforce compliance, you can design an access policy that manages user entitlements to the service or application. This helps ensure that people access what they're supposed to — no more and no less. For example, you can allow a payroll clerk limited access to employee records at specific times of the day, week or month — while giving the HR manager full access to the same records at any time during business hours.

Employing a rules-based authorization engine in conjunction with the policies and user roles your firm has established, Tivoli Access Manager for e-business automatically authenticates and authorizes individuals to access appropriate corporate Web, client/server and enterprise applications. Then, it collects audit data from multiple enforcement points — and generates records to show who accessed what application, which data and when. Consequently, you can:

- Make sure systems, applications and data are accessed appropriately.
- Manage authentication, access and audit data centrally and automatically.
- Demonstrate compliance with specified security policies.

IBM Tivoli Access Manager for Operating Systems protects individual application and operating system resources by addressing system vulnerabilities surrounding UNIX® and Linux® super-user or root accounts. Fine-grained authorization management of these root accounts lets you maintain control over privileged user access. To help you audit compliance with both internal security policies and external mandates, you can use the extensible, configurable auditing capabilities of Tivoli Access Manager for Operating Systems.

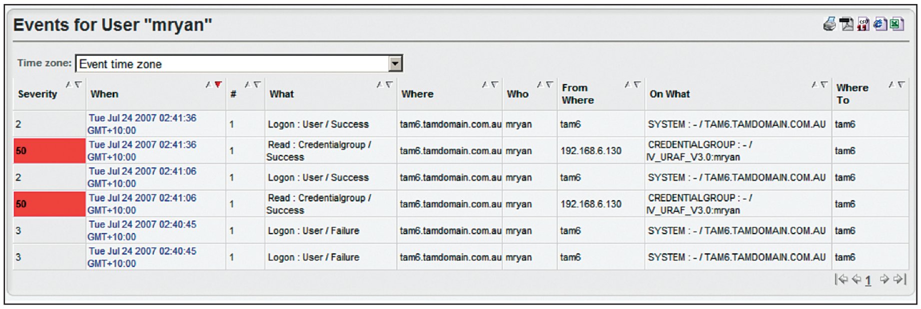
### Use fact-based insight to reduce the likelihood and impact of insider threats

Once you’ve established an effective, automated system to manage privileged user access, you must turn to address the “human element.” Experience proves that insider threats posed by privileged users cannot be adequately controlled by attempting to predict how people will behave. For example, a network administrator may unintentionally grant privileges to view classified intellectual property to someone who is not entitled to see that type of information. Or, a seemingly friendly IT worker who has passed background checks may stage outages that only he can resolve in an attempt to “stump” his peers — because he’s worried about losing his job.

As you consider the many factors behind insider threats, you must understand that:

- Your privileged users typically have deep, legitimate access rights and the capabilities necessary to exploit them.
- Human behavior is unpredictable — so insider threats are particularly challenging to identify.

The question remains: In cases where you cannot restrict access without impeding privileged users from doing their jobs, how can you secure your IT systems and data and make sure that you adhere to regulations?



**Events for User "mryan"**

Time zone: Event time zone

| Severity | When | # | What | Where | Who | From Where | On What | Where To |
|---|---|---|---|---|---|---|---|---|
| 2 | Tue Jul 24 2007 02:41:36 GMT+10:00 | 1 | Logon : User / Success | tam6.tamdomain.com.au | mryan | tam6 | SYSTEM : - / TAM6.TAMDOMAIN.COM.AU | tam6 |
| 50 | Tue Jul 24 2007 02:41:36 GMT+10:00 | 1 | Read : Credentialgroup / Success | tam6.tamdomain.com.au | mryan | 192.168.6.130 | CREDENTIALGROUP : - / IV_URAF_V3.0:mryan | tam6 |
| 2 | Tue Jul 24 2007 02:41:06 GMT+10:00 | 1 | Logon : User / Success | tam6.tamdomain.com.au | mryan | tam6 | SYSTEM : - / TAM6.TAMDOMAIN.COM.AU | tam6 |
| 50 | Tue Jul 24 2007 02:41:06 GMT+10:00 | 1 | Read : Credentialgroup / Success | tam6.tamdomain.com.au | mryan | 192.168.6.130 | CREDENTIALGROUP : - / IV_URAF_V3.0:mryan | tam6 |
| 3 | Tue Jul 24 2007 02:40:45 GMT+10:00 | 1 | Logon : User / Failure | tam6.tamdomain.com.au | mryan | tam6 | SYSTEM : - / TAM6.TAMDOMAIN.COM.AU | tam6 |
| 3 | Tue Jul 24 2007 02:40:45 GMT+10:00 | 1 | Logon : User / Failure | tam6.tamdomain.com.au | mryan | tam6 | SYSTEM : - / TAM6.TAMDOMAIN.COM.AU | tam6 |

*Tivoli Compliance Insight Manager is designed to detect all events generated by Tivoli Access Manager for e-business. Because these events become part of an audit system, you can more easily investigate all events over a period of time and be alerted automatically if specific thresholds are exceeded.*

### *Discover policy breaches by monitoring privileged user activities*

To protect your enterprise data assets, intellectual property and IT resources, you can leverage IBM Tivoli Compliance Insight Manager. With this software solution, you can create policies to automatically monitor user behavior and shed insight into potential problems. As you monitor, report on and investigate user behavior, you can address accidental and malicious actions that violate policies or regulations — without putting unnecessary restraints on users.

Tivoli Compliance Insight Manager offers sophisticated, privileged user monitoring and analysis (PUMA) capabilities that encompass databases, operating systems, mainframes, applications, security devices and network devices. With this cross-enterprise, platform-independent dashboard and reporting engine, you can non-intrusively collect detailed access information to show *who* did *what*, on *what, when, where* they did it, *where* they came *from* and to *where* they were going. Then, the product can compare this user behavior log to a variety of policy settings to reveal activities that are outside the scope of the user’s job or don’t match normal user behavior. As a result, you can rapidly identify noncompliant behavior. Tivoli Compliance Insight Manager also integrates closely with Tivoli Access Manager to capture and report on audit trails related to administrative actions.

### *Monitor and track routine, but sensitive, activities*

For some roles in an organization, high-level activities require almost daily contact with sensitive information or powerful applications. For example, the database administrator needs to be able to perform all types of actions to databases, such as table modifications. Even though you want the administrator to be able to change the definition of a table called "salaries," it would be wise to monitor and track this activity any time it occurs — simply because it deals with such sensitive information. By monitoring and logging the administrator's behavior, you'll know quickly if she oversteps her legitimate business bounds and actually reads the content of the table rather than just changing its definition.

### *Use reporting tools to analyze user behavior and prove compliance*

To make collected user activity monitoring information actionable, Tivoli Compliance Insight Manager includes an at-a-glance dashboard designed for compliance purposes. The dashboard provides a concise view of all activities on the system, prioritizing areas of concern by size and color. The software highlights any unusual activity as an exception so you can quickly spot potential trouble, then drill down to get more details. As a result, you can measure security posture internally and respond rapidly to auditors' requests. Tivoli Compliance Insight Manager also provides best-practice reporting tools, including hundreds of customizable reports. For example:

- A user-by-event-type report lets you see details of who performed specific administrative activities on multiple platforms throughout the enterprise.
- Various "overview" reports let you do things like identify access to sensitive data, monitor operational changes or detail incident investigation information.

### Use near-real-time alerts and analysis to respond to threats quickly and effectively

For near-real-time alerting capabilities that let you respond quickly to out-of-line activities, you can link Tivoli Compliance Insight Manager with IBM Tivoli Security Operations Manager software. If Tivoli Compliance Insight Manager identifies a policy breach or other suspicious activity, it can automatically route this information to the Tivoli Security Operations Manager centralized event database. Here, the information is logged, analyzed and correlated with other activity in the environment related to that asset or user. If this analysis indicates anomalous activity, the events can be escalated through your incident management process to be investigated appropriately.

For example, you might want to set an alert for your main business system that lets you know if an administrator logs on as "root." While this activity may be legitimate, it is sensitive enough to require real-time monitoring — and escalation to an appropriate manager, if needed.

### Help privileged users do their jobs without impeding productivity

Together, IBM security solutions for privileged user monitoring and audit provide an integrated, end-to-end approach to managing privileged users: the people who pose the biggest challenge to your business' information integrity, data privacy and compliance. IBM solutions offer reliable ways to set up and automatically enforce appropriate levels of access; use real-time monitoring to identify, track and report on suspicious or inappropriate behavior; and quickly respond to problems through detailed investigations. As a result, you can have confidence — and prove to auditors — that you're doing everything possible to help trusted insiders do their jobs, without overstepping their bounds.

### For more information

To learn more about how your organization can use Tivoli insider threat solutions to identify, track and prevent privileged users' accidental or malicious behavior, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli

### About Tivoli software from IBM

Tivoli software provides a set of offerings and capabilities in support of IBM Service Management, a scalable, modular approach used to deliver more efficient and effective services to your business. Helping meet the needs of any size business, Tivoli software enables you to deliver service excellence in support of your business objectives through integration and automation of processes, workflows and tasks. The security-rich, open standards–based Tivoli service management platform is complemented by proactive operational management solutions that provide end-to-end visibility and control. It is also backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli customers and business partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world — visit www.tivoli-ug.org

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

Produced in the United States of America
9-07

**Disclaimer:** The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

*CIO Magazine Survey 2007.

TAKE BACK CONTROL WITH Tivoli.