Monitor for external and internal mainframe threats to help ease security and compliance challenges

Tivoli software

IBM Tivoli zSecure Alert

Highlights

- Monitor sensitive data for misuse to help enhance access controls
- Leverage configurable alerts to help analyze and improve security
- Help detect configuration mistakes before others exploit them
- Help reduce operational costs associated with incident response activities
- Easily send critical alerts to enterprise audit, compliance and monitoring solutions
- Available for z/OS systems with RACF or CA ACF2

As the core repository for crucial company data, the mainframe is increasingly at the center of the networked enterprise. Employees, consultants and customers depend on the mainframe for vital information, which makes it essential to protect this important resource against the threats of external or internal intruders, and unwanted configuration changes. At the same time, you want to stay ahead of potential compliance violations.

Ideally, mainframe monitoring should be part of your overall enterprise threat monitoring solution. As a near-real-time mainframe monitoring solution that allows you to efficiently monitor for intruders and improper configurations, IBM Tivoli® zSecure Alert makes this easier to accomplish. Through faster incident management and more streamlined audit efforts, Tivoli zSecure Alert can help minimize security housekeeping on the mainframe, enhance system availability and supplement access controls.

Monitor critical data to help maintain data integrity

When certain crucial data is touched — even by authorized users — you should know about it. The ability to successfully monitor data is even more critical when your compliance posture is at stake. Tivoli zSecure Alert resides on the mainframe, monitoring IBM z/OS®, IBM Resource Access Control Facility (RACF®), CA ACF2™ and UNIX® subsystems. By combining a threat knowledge base with parameters from your active configuration, it can help identify resources that need protection and isolate relevant attack patterns.

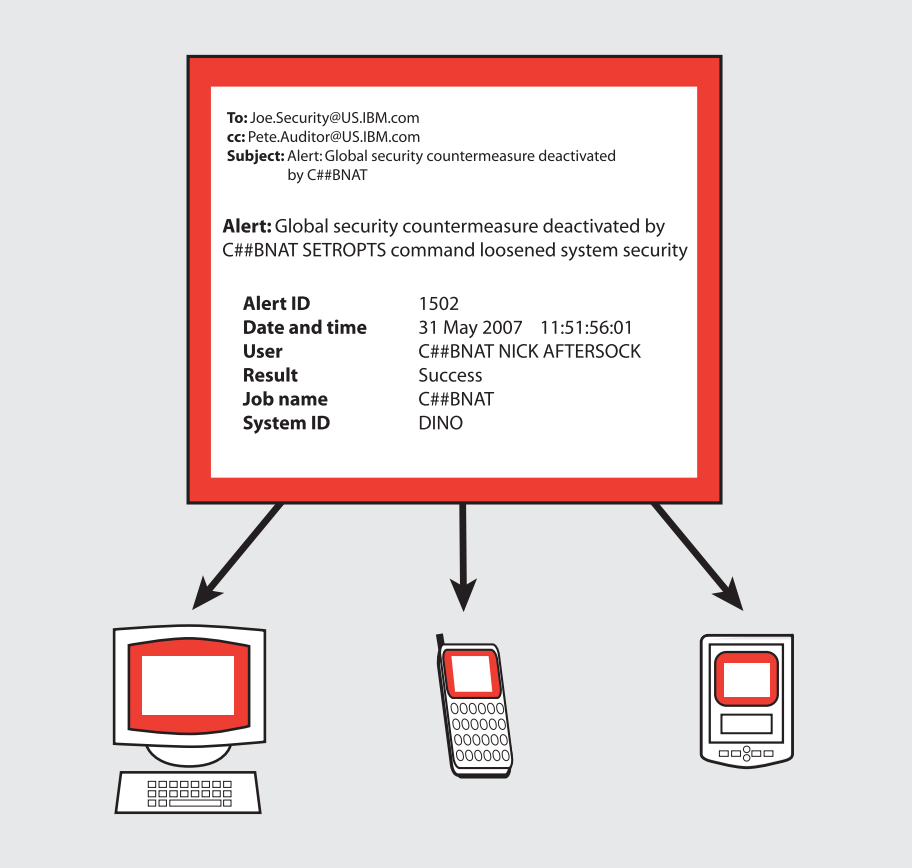
Unlike other products that only detect breaches from IBM System Management Facility (SMF) information, Tivoli zSecure Alert can also detect malicious activity even if it is not

registered in the event log (SMF record). And through the ability to compare real-time activity with recent patterns, Tivoli zSecure Alert can help discover additional threats.

With a broad range of monitoring capabilities, Tivoli zSecure Alert can help you detect multiple types of attacks and configuration threats, including:

- Unwanted logons and attempts:
  - Logon by unknown users.
  - Logon with emergency user ID.
  - UNIX privileged user logon.
- Changes that violate security policy:
  - Addition or removal of system authority.
  - Revocation of production user IDs.
  - Granting of excessive universal access.
  - Disabling of system security options (SETROPTS, GSO).
  - Disabling of audit trail.
- Suspicious activity on the UNIX subsystem:
  - File access violations.
  - Authorized program facility (APF) or controlled program assignment.
  - Global write or read specification.

In addition, Tivoli zSecure Alert can help determine when your core system resources are at risk through the occurrence of one or more of several events:



Tivoli zSecure Alert offers timely alerts to help you provide more efficient incident response. Configurable alerts can be sent via e-mail, cell phone, pager, and to central security and network management consoles.

- Updates on a system data set
- Dynamic addition of an APF data set
- SMF buffers becoming full, risking data loss
- Tasks started with unspecified authority

Get fast, flexible alerts to help prevent costly damage

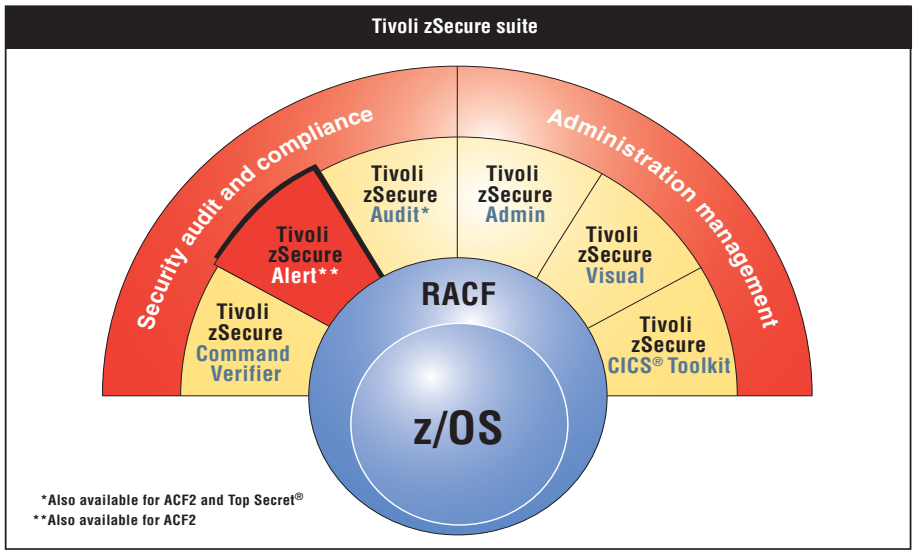
Timely alerts are a critical part of monitoring because they help you respond quickly to prevent further damage. For example, you want to be able to fix detected configuration mistakes before others can exploit them. Tivoli zSecure Alert delivers robust alerting capabilities to quickly notify relevant personnel of changes, improper access and security holes. The alerts are written in the easy-to-use Consul Auditing and

Reporting Language (CARLa) and can be customized for e-mail, cell phones, pagers and text messaging. The selection and layout can also be dynamically reconfigured from an ISPF application.

Tivoli zSecure Alert integrates with other tools, enabling you to send relevant alerts to your central security or network management console. For example, you can send Simple Network Management Protocol (SNMP) alerts to the IBM Tivoli Compliance Insight Manager dashboard for security policy violations, to IBM Tivoli Security Operations Manager for real-time correlation and threat monitoring, to IBM Tivoli Enterprise Console® and more.

Take effective countermeasures

Tivoli zSecure Alert goes beyond conventional intrusion detection solutions to help you determine what countermeasures to take when a threat is detected. For example, you can predefine and customize a measure, such as instantly revoking a user or shutting down an application if a certain security event occurs. In addition, you can send Write to Operator messages to trigger automated operations or issue RACF commands autonomously.



For more information

Tivoli zSecure Alert is the result of decades of experience — gained through conducting tests on mainframe systems — collected into a threat knowledge base that can quickly alert you to suspicious activities. Tivoli zSecure Alert integrates seamlessly with the complete Tivoli zSecure suite of enterprise-wide security administration and auditing solutions, providing a comprehensive, end-to-end workbench for RACF security management.

To learn more about how Tivoli zSecure Alert can help your organization detect potential violations to more effectively meet audit and security challenges, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli

Tivoli zSecure Alert at a glance

System requirements:

- z/OS or z/OS.e

Supported administrative platforms:

- RACF
- CA ACF2

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

Produced in the United States of America
6-07

TID10370-USEN-00