IBM Tivoli and Consul: Facilitating security audit and compliance for heterogeneous environments.
Overview

Security and compliance challenges are greater than ever because of increased regulatory requirements and costs of compliance failures, increased complexity in technologies and IT environments, and a lack of predictability and visibility across infrastructures.

To help address these challenges, IBM continues to expand its security management portfolio through development and acquisitions. One such acquisition is Consul risk management international, B.V., a recognized leader in policy-based security audit and compliance. Designed for both distributed and mainframe environments, Consul products provide capabilities that combine with the IBM Tivoli® security management portfolio to help organizations:

- **Assess** the overall security and compliance status of business infrastructures:
  - Capture comprehensive log data.
  - Analyze data through sophisticated log interpretation and normalization.
  - Communicate results to management and auditors through a drillable dashboard and full set of audit and compliance reports.

- **Defend** against potential security threats and business risks across the enterprise:
  - Deliver comprehensive, end-to-end security management.
  - Improve security information and event management, addressing both internal and external threats.
  - Enhance preemptive security solutions.

- **Access** control for business systems and information to help maximize integrity and facilitate compliance:
  - Enable a mainframe-based hub for enterprise security management.
  - Combine security with compliance management.
  - Develop and support policy-based access and identity management.

- **Monitor** internal and external behaviors, address violations and manage data:
  - Monitor privileged users and their activities, including system administrators and database administrators (DBAs).
  - Automate analysis of user behavior against security policies to identify noncompliant activity.
  - Take action based on compliance violations.

Contents

2 Overview
3 Identify today’s challenges in security audit and compliance
3 Discover how Consul products enhance the IBM security management portfolio
5 Leverage extended Consul functionality through integration with other IBM products
6 Combine the benefits of Consul and IBM Tivoli solutions
8 Conclusion
8 For more information
Identify today’s challenges in security audit and compliance

In a recent IBM study, 64 percent of CIOs stated that the most significant challenges facing IT organizations include security, compliance and data protection. These challenges are being fueled by:

- **Increased requirements** — Numerous compliance initiatives already exist and requirements are only increasing in many industries. To manage risks and avoid penalties or lost business, businesses need improved monitoring and controls.

- **Increased complexity** — Disparate technologies and infrastructures constantly fragment and hamper compliance efforts. Organizations also struggle to link compliance at the infrastructure and business levels.

- **Increased costs** — Little-to-no predictability and visibility across complex infrastructures drive rapid cost inflation. Additionally, the failure to achieve compliance or prevent security breaches can impose enormous costs.

As a result, IT organizations must now find a way to support three imperatives that sometimes overlap and sometimes compete: managing security risks, addressing burgeoning compliance requirements and supporting the core business. The need to serve these three imperatives simultaneously with limited resources has created arguably the most complex and challenging IT environment that CIOs have ever faced.

Discover how Consul products enhance the IBM security management portfolio

To address today’s challenges in security audit and compliance, IBM provides a portfolio of flexible security management solutions that span assessment and discovery, defense, access management, monitoring and reporting analytics. The IBM security management portfolio is enhanced by ongoing IBM development and the acquisition of world-class technology solution providers.
One such acquisition is Consul risk management, B.V., a recognized leader in policy-based security audit and compliance. Designed for both distributed and mainframe environments, Consul products include:

- **Consul InSight™ Suite** that captures comprehensive log data and then interprets the data through sophisticated, patent-pending W7 analysis, privileged user monitoring and out-of-the-box compliance support modules. Consul InSight Suite helps greatly accelerate policy and compliance initiatives.

- **Consul zSecure™ Suite** of integrated mainframe tools that enable mainframe administration managers, security officers and auditors to facilitate compliance with regulations, prepare for and pass security audits, improve operational efficiency and reduce chances of downtime.

Organizations that already understand the strengths of the IBM security management portfolio can leverage the addition of Consul products to deploy solutions for both distributed and mainframe environments, including the following:

- **An enhanced security and compliance dashboard** that enables information protection efforts, accelerates audit and compliance activities, establishes access accountability and helps reduce the cost of security operations.

- **Comprehensive, end-to-end security management** with identity and access management, security incident and threat management, powerful visibility into insider threats, in-depth user activity monitoring and comprehensive auditing capabilities.

- **A mainframe-based hub for enterprise security management** with capabilities to administer, audit, alert and monitor IBM z/OS® RACF® for security and compliance; administer and manage mainframe users and security; and connect the mainframe to centralized compliance and administration efforts.
By leveraging Consul capabilities to enhance support for mainframe investments, IBM helps customers extend the value of their existing investments and minimize disruptions when they adopt new security management technologies. They can take a phased approach to enhancements and continually verify that the solutions they deploy will align with their strategic initiatives.

Additionally, Consul best practices combine with those that IBM has developed for both distributed and mainframe environments to help customers address standards, laws and compliance initiatives, including the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Basel II and ISO17799.

Leverage extended Consul functionality through integration with other IBM products

Organizations that already use Consul products can also enjoy substantial benefits from future integration of Consul products with other IBM security management offerings. The following examples show the extended benefits planned through the future integration of Consul InSight, Consul zSecure and the IBM Tivoli security management portfolio.

• **Security information and event management (SIEM):** An SIEM solution integrates security information management (SIM) with security event management (SEM). To support this objective, all events and alerts from Consul InSight can be forwarded in real time to the IBM Tivoli Security Operations Manager console. At the same time, events and alerts generated by IBM security management tools can be populated within Consul InSight for normalization and compliance reporting. This integration harmonizes the collection infrastructure among the product lines, thereby supporting an effective, comprehensive SIEM solution.
- **Change and configuration management**: One of the biggest contributors to IT outages is unregulated or unauthorized change. IBM offers a number of change management products including IBM Tivoli Change Process Manager. Leveraging deeper integration with Consul InSight, IBM customers will be better able to meet requirements regarding verification and enforcement. Deeper integration supports the ability to definitively answer policy and enforcement questions.

- **Storage management**: Businesses today must often maintain huge stores of sensitive, private and financially critical documents for many years. As part of this process, they must prove — by means of audit trails and other means — that documents have not been misused, altered or otherwise compromised. The integration of Consul InSight with IBM storage solutions provides:
  - Monitoring and enforcement of data management and retention processes.
  - Secure, manageable, long-term storage of audit trails.

- **Identity management**: IBM Tivoli Identity Manager, IBM Tivoli Access Manager software and Consul InSight can be fully integrated to deliver improved identity management. For example, Consul InSight compliance and forensic reports can draw on Tivoli Identity Manager user profile information. Additionally, Consul InSight can use Tivoli Access Manager policies as the basis for policy monitoring. Organizations can also integrate IBM Tivoli Provisioning Manager with Consul InSight to update workstation and server configurations or correct them when noncompliance occurs.

**Combine the benefits of Consul and IBM Tivoli solutions**

The integration of Consul and IBM Tivoli security management solutions blends strengths to create a broad portfolio of security and compliance management solutions for distributed and mainframe environments. The tables on page 7 provide more detail about the benefits of the IBM Tivoli security management portfolio now that Consul products have been added.
### Security compliance dashboard and reporting
- **Requirements**: Quickly gain an overview of the security compliance posture. Compare user activities and security events to regulatory requirements and acceptable use frameworks.
- **Benefits with IBM and Consul**: A security compliance dashboard along with specific modules that customers can use to address their compliance activities related to SOX, HIPAA, GLBA, Basel II and ISO17799.

### Log management
- **Requirements**: Automate rapid, reliable log file collection and management across a variety of applications, operating systems, databases and security devices for compliance.
- **Benefits with IBM and Consul**: Ubiquitous, secure and native log collection across heterogeneous platforms, with query capability and reporting to address log collection and storage.

### Security information and event management (SIEM)
- **Requirements**: Efficiently correlate, analyze and respond to security events for intruders from perimeter and network devices in a real-time security operations dashboard.
- **Benefits with IBM and Consul**: A real-time SIEM dashboard and reporting engine, with support for leading network and security devices as well as support for hundreds of predefined correlation rules, enabling effective incident management.

### Privileged user monitoring and audit (PUMA)
- **Requirements**: Monitor privileged users and their activities in regards to key corporate systems and data. This monitoring should help ensure that confidentiality, integrity and systems compliance are properly maintained.
- **Benefits with IBM and Consul**: Privileged-user monitoring that uses Consul InSight W7 methodology and PUMA reports to enable security personnel to help protect corporate systems from rogue or accidental breaches and outages.

### Database auditing
- **Requirements**: Help protect core data sets and databases (such as IBM DB2 Universal Database™, Oracle, Sybase or Microsoft® SQL) from abuse by users and DBAs. This helps organizations address compliance requirements, close audit findings and minimize the risks of improper data access.
- **Benefits with IBM and Consul**: Database auditing across leading enterprise database platforms, using Consul InSight W7 methodology to ensure DBAs and users do not access data outside of application controls and the change management process.

### Mainframe audit
- **Requirements**: Monitor mainframe events and incidents, help reduce security vulnerabilities, enforce policy compliance and generate audit reports.
- **Benefits with IBM and Consul**: A mainframe compliance and auditing solution, including the analysis and reporting of mainframe events and automatic detection of exposures through extensive status auditing.

### Mainframe administration
- **Requirements**: Help reduce the cost and complexity of RACF administration while enabling decentralization and compliance reporting.
- **Benefits with IBM and Consul**: A mainframe administration suite that enables efficient and effective RACF administration by using less resources, providing richer functionality and facilitating compliance.

---

### Future integration is planned to address:

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Enhanced benefits with IBM and Consul</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change management audit</strong></td>
<td>Monitoring of all changes in comparison with change management policy, for compliance purposes. Audit leverages reporting for compliance and operational management.</td>
</tr>
<tr>
<td><strong>Storage auditing</strong></td>
<td>Monitoring of access to and use of stored data for confidentiality and privacy, while verifying secure storage of security audit trail information for regulations and investigations.</td>
</tr>
</tbody>
</table>
| **Identity and access management** | Closed-loop identity management to answer who can, who should and who does touch data. A broad range identity and access management requirements ranges from provisioning and sign-on through to audit and compliance. | A solution with:  
  - Tivoli Identity Manager and Tivoli Access Manager software event sources.  
  - Integration of Tivoli Identity Manager identity store and Tivoli Access Manager software policy definition.  
  - Remediation from Consul InSight to Tivoli.  
  - Integration with status audit. |

---

**Disclaimer:** All statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.
Conclusion
The integration of Consul with IBM Tivoli blends strengths to create a powerful, comprehensive portfolio of security and compliance management solutions.

Based on this integration, both Consul and IBM customers can enhance the effectiveness of their security and compliance management practices, helping to:

- Address growing requirements.
- Manage increased complexity — The combined solution integrates mainframe and distributed environments into one view of security and compliance across the total infrastructure.
- Contain rising costs — The combined solution provides visibility to threats across heterogeneous infrastructures to help reduce costs and enable better risk management.

For more information
To learn more about the IBM Tivoli security management portfolio, including Consul products, contact your IBM representative or IBM Business Partner, or visit ibm.com/tivoli