

Consul InSight™ Security Manager

Revolutionizing security event management

It's the first solution that offers you complete security throughout your business.



Security used to be about simple perimeter protections and alarm systems. Those days are gone. Today, technology and globalization have combined to make organizations more open than ever before, and this makes them more vulnerable to a whole range of security threats from both inside and outside the enterprise.

Modern security systems are helping to combat these threats, but most of them cover only parts of the business, leaving dangerous loopholes for potential network criminals.

They are also insufficient for complying with the rigorous new security regulations being set by governments, as well as the security demands of your customers and business partners.

Consul InSight™ empowers security staff.

Consul InSight™ is a complete solution that offers you enterprise-wide security event audit and compliance, taking a people-centric view (whether 'trusted' or intruders), monitoring all technologies (security devices, applications, servers, operating systems, mainframe) and incorporating security policies (generation and enforcement).

Consul InSight™ empowers security staff to work more effectively and efficiently by:

- Seamlessly integrating with the broadest range of perimeter security devices such as firewalls, anti-virus and IDS systems
- Monitoring the full spectrum of internal network assets such as servers, databases, applications, and mainframes.
- Consolidating, correlating and analyzing security data (logs, alerts, etc.) from over 50 platforms
- Providing best-practice and regulatory policy templates customizable to any organization
- Providing prioritized alerts of meaningful security events and policy violations
- Delivering powerful reporting and analysis tools to track suspicious activity and demonstrate effective security

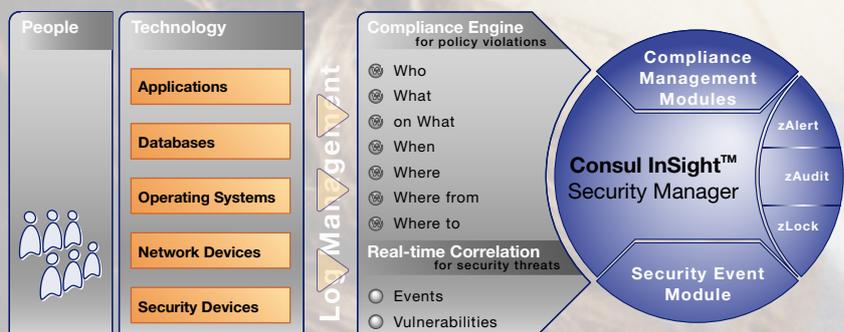
Different than any other solutions on the market.

- Most complete, people-centric view of security
- Most complete regulatory compliance
- Most complete platform coverage - internal systems and security devices
- Most complete event correlation engine - covering insider and perimeter events
- Most complete archiving capability
- Most complete mainframe expertise
- Most complete policy generation and filtering

How it works.

Consul InSight™ Security Manager offers you the most comprehensive Security Event Management solution enabling security auditing, regulatory compliance, security device management, and insider and intruder monitoring. Security data from the entire enterprise is consolidated and normalized through Consul's patent-pending W7 methodology whereby Who, did What, When, Where, Where from, Where to and on What is determined based on the information in security alerts and log files. Through best-practice and customizable policy templates, only the essential events are filtered to provide urgent, relevant and actionable information.

Consul InSight™ Suite



Features

Consolidation & Correlation

Exhaustive log and alert consolidation.

By collecting and storing all relevant log files and security alerts, Consul InSight™ eliminates the time-consuming and costly burden of manually reviewing thousands of log files. Logs and alerts are encrypted and compressed, facilitating secure transmission with low bandwidth demands. Beyond real-time alerting, this information is stored to enable historical auditing and reporting.

Complete Network Coverage.

Consul InSight™ covers the most comprehensive range of information assets—from perimeter security devices to internal servers, applications and mainframes. This unparalleled coverage provides the industry's most integrated, comprehensive view of network security, enabling staff to efficiently monitor security across the enterprise without the need for system specific technical expertise.

Consul InSight™ Correlation Engine.

At the heart of the Consul InSight™ system, the output from over 50 platforms and devices is correlated using the patent-pending W7 methodology, facilitating investigation. For example: add a time range around a suspicious event to see what other relevant events occurred simultaneously; correlate a user or event across platforms to get a full picture of behavior. Meaningful correlation to speed your work.

Configuration & Management

Central Management Console.

A management console provides an integrated view of the entire network, enabling security staff to review security status, add platforms and devices for monitoring, and investigate incidents. This provides security managers with a consistent, manageable, actionable view of suspicious activity across the enterprise – whether it's a filtered IDS alert, an unauthorized mainframe configuration change, a firewall attack, or unauthorized access on an internal server or application.

Consul InSight™ Policy Generator.

Consul InSight™ provides policy templates that are based on years of experience implementing security best practices at leading organizations around the world. These templates can be easily customized to any organization's environment or regulatory need. Consul InSight™'s policy filtering engine makes it easy to enforce compliance to these policies on a continuous basis.

Integrated Mainframe Monitoring.

For those enterprises that need it, the Consul InSight™ solution uniquely includes mainframe security monitoring technologies that have led the market for over 10 years. Mainframe security can now be integrated into a total enterprise view of security, with one central console and alert framework assuring the continuous security of all critical assets. Deep mainframe monitoring tools enable further investigation.

Action & Investigation

Real-Time Actions and Alerts.

Consul InSight™ provides real-time notification of security events and policy violations. Customizable alerts can be delivered by phone, email and pager. Consul InSight™ allows custom, instant actions to be taken when an event reaches a critical threshold.

Consul InSight™ Reporting Wizard.

Consul InSight™ offers robust reporting capabilities that enable easy demonstration of policy compliance and efficient documentation of security events. It delivers custom reporting as well as standardized report templates for different platforms, such as perimeter security devices, operating systems, mainframes, etc. Consul InSight™ also enables easy compliance to leading security regulations and standards, such as GLB, Sarbanes-Oxley, Basel II, HIPAA, BS/ISO17799 and more.

Archive and Forensics.

By storing all log and alert data, Consul InSight™ enables exhaustive forensics analysis following suspected malicious activity. With powerful reporting and analytical tools, security staff can reconstruct historical events and explore activity not previously suspected as malicious. The archival and forensics abilities help speed recovery from breaches and support prosecution as appropriate.

About Consul

Consul risk management, a renowned expert in security audit and compliance solutions, with more than 350 customers across two-dozen countries, delivers to the market The InSight Required™ for sound compliance, security event management, and identity and access management initiatives. Consul's enterprise solutions monitor, report and investigate both malicious and accidental violations of information use against external regulations and internal policies



At a glance overview of enterprise compliance status and trends.



Consul risk management, BV

Olof Palmestraat 10
2616 LR Delft
The Netherlands

Tel: +31 15 251 3333
Fax: +31 15 262 8070
contactsales@consul.com

Consul risk management, Inc.

Suite 250
2121 Cooperative Way
Herndon, VA 20171
USA

Tel: +1 703 547 3577
Fax: +1 703 547 3587
contactsales@consul.com