



U.S. Intelligence Agency

A large intelligence agency in the U.S. Federal Government was struggling with managing the vast volume of security information that crossed its networks, as well as managing this data to ensure security at all times. Using Sentinel™ from Novell®, the agency now has centralized security knowledge management and can better comply with regulatory standards.

Overview

A large intelligence agency in the U.S. Federal Government is required to provide timely information to U.S. decision makers and military leaders. The agency intercepts and analyzes a vast array of foreign military and national security-related communications worldwide.

Challenge

For decades, the agency has held the technological edge, making significant intelligence contributions to the U.S. dominance over the Soviet Union during the Cold War. But the fast pace of today's technological changes and the slow pace of modernization at the agency resulted in disparate systems across multiple networks, duplicative efforts and a compromised position for the nation's outcomes—threatening the agency's ability to carry out its mission.

The agency realized an immediate need to invest in its IT infrastructure and sought secure and non-secure telephony and network services, distributed computing services, and enterprise and security

management of its non-mission IT infrastructure at headquarters and surrounding offices. This massive undertaking was a dramatic change in its longstanding IT operations, designed to reverse years of modernization neglect.

Solution

With the explosive growth of global network and new technologies, partnership with industry to improve IT operations was more vital to the agency's success than ever before. After a 15-month study comparing outsourcing with in-house efforts, its decision to deploy Sentinel would enable it to focus on core missions and cost-effectively upgrade its infrastructure. Key factors in the decision that ultimately led to Sentinel as the solution of choice were:

- *Proven record of success with more than a hundred successful deployments*
- *Scalability to securely monitor some of the country's largest networks*
- *Rich features for both security perimeter and audit compliance monitoring*

U.S Intelligence Agency at a glance:

A large intelligence agency in the U.S. Federal Government

■ Industry:

Government

■ Location:

United States

■ Solutions:

Sentinel from Novell

■ Results:

- *Improved compliance with regulatory standards*
- *Centralized security knowledge management*
- *Improved decision-making capabilities*
- *Increased protection of information assets*

Sentinel from Novell enhances awareness of real-time security events at the U.S. Intelligence Agency, and improves security and compliance management as part of the agency's modernization effort.



Sentinel provides an integrated, centralized view of all events, and manages correlation across all security-relevant data, ensuring fast resolution and prevention of attacks.

www.novell.com

Proven Record of Success

As a pioneering product in the emerging security information and event management (SIEM) market, the market-leading Sentinel solution from Novell is customizable, flexible and scalable. The deployment of Sentinel provides the agency with a new security infrastructure and the means for real-time enterprise security management—enabling the agency to improve efficiency and effectively monitor security-related information assets.

Scale for the Nation's Largest Networks

Sentinel has a successful track record of supporting many large and complex networks, including the nation's largest communications companies, financial institutions and government agencies. Based on a truly distributed, multi-tier architecture, Sentinel uses a high-volume enterprise message bus that allows for unlimited scalability while maintaining a holistic view of an enterprise security environment. It provides the agency with a proven, scalable solution to effectively manage its security operations and meet compliance requirements.

Perimeter and Audit Compliance Reporting

In addition to standard security operations and management of its perimeter infrastructure, Sentinel provides a solution to manage and monitor the agency's three air-gapped networks independently and collectively. By presenting the sheer volume of security data in a meaningful way, based on classification

levels (unclassified, secret and top secret), the agency would be in the position to effectively monitor and manage its security posture.

Sentinel provides an integrated, centralized view of all events, and manages correlation across all security-relevant data, ensuring fast resolution and prevention of attacks. Furthermore, the solution would enable the agency to pull in referential data, integrating asset and patch data into its back-end systems and providing the agency with full access to evaluate real-time security events with asset criticality, current patch levels and audit levels. This would help ensure compliance with internal and external regulatory requirements and protect the agency's mission-critical assets.

Results

After conducting the initial assessments and developing the business plan, project plan and IT architecture, the agency is positioned to reap the following benefits from Sentinel:

- *Improved compliance with regulatory standards*
- *Increased efficiency and performance*
- *Enhanced awareness and ability to evaluate real-time security events*
- *Centralized security knowledge management*
- *Real-time correlation across multiple networks*
- *Improved decision-making capabilities*
- *Increased protection of information assets*



Contact your local Novell Solutions Provider, or call Novell at:

1 888 321 4272 U.S./Canada
1 801 861 4272 Worldwide
1 801 861 8473 Facsimile

For More Information:

To read more customer success stories, visit: www.novell.com/success

Novell, Inc.

404 Wyman Street
Waltham, MA 02451 USA