Case Study: University of Dayton and Novell® Identity & Security Solutions

Rick Wagner
Senior Product Manager, Security Management
rwagner@novell.com
University of Dayton

- Recognized by US News and World Report as one of the 10 best Catholic Universities in the nation
- 12,0000 Students and 3,000 Faculty
- The Challenge:
  - "We had a huge pile of data and no way of getting to the few bits of data that were really important to us"
  - "We needed a way to not only analyze this data but also simplify ongoing report creation for PCI compliance. Previously we had to do a lot of manual work to produce reports."
University of Dayton

• The Solution

  • Deployed Sentinel™ and Sentinel Log Manager Log Manager to detect and collect an average of three million security events a day simplifying the process of collecting, archiving and analyzing its log data.

  • “Novell Sentinel Log Manager allows us to take all the log information and look at it by any parameter. It brings meaning to the hundreds of security logs we receive.”

  • The University uses Sentinel™ to collect security-related events from its firewalls, intrusion detection systems, Novell eDirectory™, Novell Identity Manager and Novell Access Manager™.

  • "The real strength of Novell Sentinel, coupled with Novell Identity Manager, is the ability to clearly connect security events with individual identities, which is critical for achieving PCI compliance.”

  • "Novell Sentinel Log Manager does an amazing job at handling the huge volume of data we're throwing at it.”

  • "Within this year, the Novell solution will have easily paid for itself in reduced administrative time, not to mention our improved security posture."
Integrated Approach to Security

- Access Control
- User Provisioning
- Security Monitoring
- Challenges
Identity and Security Business View

Business Processes
- Business Managers
- IT Security Team
- Internal Audit, Risk and Compliance

People
- Accountability
- Visibility
- Certification
- Agility

Process
- Automate
- Validate

Information Resources
- Databases
- Homegrown Applications
- Authorization Systems
- RACF Top Secret Z Series
- Windows Networks
- ERP / CRM Applications
- Directories
Novell® Sentinel™

Replace manual processes with automated IT controls, monitoring and reporting

- Network Infrastructure
- Logs
- Security Devices
- Logs
- Workstations and Servers
- Logs
- Mainframes
  - RACF
  - ACF 2
  - Top Secret
- Databases
- Logs
- Applications
- Logs

Monitor

Remediate

Report
Sentinel™ Automates the Monitoring and Reporting of IT Controls

**Collect** and consolidate feeds from multi-vendor sensors
**Normalize** logs from across the enterprise seamlessly
**Monitor** and analyze for control violations in real time
**Respond** to violations … incident management tied to existing workflows
**Report** on the effectiveness of the control environment

- Anti-virus
- VPN
- Server
- Firewall
- Database
- IDS
- Router

Collect → Normalize → Analyze → Report → Respond

Real-time View

Aggregate • Normalize • Correlate
Real-time Identity Enriched Security Information

Who caused this security event?

What else have they been doing recently?

What other accounts do they have throughout the enterprise?
For Additional Information

- Novell Open Audio

- Success Story

- Sentinel Log Manager
Unpublished Work of Novell, Inc. All Rights Reserved.

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Novell, Inc. Access to this work is restricted to Novell employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. Novell, Inc. makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for Novell products remains at the sole discretion of Novell. Further, Novell, Inc. reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.