CASE STUDY

tenable network security

McKesson

Enterprise-wide Visibility for Vulnerabilities and Compliance

Overview

With sales of $112 billion in 2011, McKesson Corporation (NYSE: MCK) is the largest pharmaceutical company in the world — providing medicines, pharmaceutical supplies, information, and care management products and services across the healthcare industry. McKesson has more than 50 global offices and employs more than 32,500 people.

- **Key Business Needs**: McKesson needed a robust, scalable, and cost-effective vulnerability management system to ensure the company would continue to meet core regulatory compliance initiatives.
- **Tenable Products Selected**: McKesson selected Tenable SecurityCenter™ integrated with the Nessus® vulnerability scanner to gain a rapid, centralized view of vulnerability status across its immense and complex global network.
- **Top Benefits**: The company's enhanced security process streamlined compliance reporting and ensured auditors have visibility into the vulnerability status of newly-acquired and existing systems. As McKesson continues to grow by acquisition, Tenable's technology scales quickly and easily and helps the company pinpoint and prioritize vulnerabilities and threats.

Business Needs

McKesson needed a robust, scalable, and cost-effective vulnerability management system that could quickly and easily expand with the healthcare giant as it acquired new businesses. The new security system needed to ensure the company would continue to meet its core regulatory compliance initiatives, such as HIPAA, PCI, SOX, HITRUST, and FISMA.

"We're a growth-by-acquisition kind of company, acquiring roughly five to ten new businesses every year," said Eric Dixon, Information Security Manager, McKesson. "A core part of my responsibility in the security division of McKesson is to understand how many new IT systems we're inheriting – do they expose us to any new risks or vulnerabilities – and what kind of impact the acquisition will have on our compliance status."

Business Challenge

Internal and third-party audits are frequent, if not constant, for the security team at McKesson. The Fortune Global 500 company has a vast network that spans tens-of-thousands of customers, employees, and partners around the world. As a result, McKesson must comply with a wide variety of regulations.

McKesson recognized that its process for security and vulnerability assessment would quickly become unmanageable if the business continued to grow at its current pace. The company began to investigate best practices and technology solutions, including vulnerability management, to automate core facets of its security process and meet the demand of its aggressive growth strategy.

Project Goals

McKesson had three key business requirements during its search for appropriate technology solutions.

1. **Scalability**: McKesson's success showed no signs of slowing down, and the company needed solutions that could scale just as fast. With each acquisition, McKesson wanted to have an immediate and comprehensive snapshot of the vulnerability, risk, and compliance status of the acquired systems.
2. **Robust Capabilities**: The technology solutions needed a dynamic feature set that could manage large-scale deployments and provide fast and accurate results to save time for McKesson's security team and extend their compliance and security capabilities.

McKESSON

Business Needs

- Find and remediate vulnerabilities quickly to protect information systems
- Reduce the time spent running and analyzing scans
- Maintain up-to-date information about vulnerabilities and fixes

> "Part of the way we sold SecurityCenter to our management was by bringing in a third-party penetration testing team and comparing their results to the results we got through SecurityCenter. The findings were impressive. SecurityCenter found everything that the penetration team found and more — and did it in a fraction of the time."
>
> *Eric Dixon*
>
> Information Security Manager,
> Information Security Technologies,
> McKesson University

3. **Affordability**: The solutions needed to be cost effective. McKesson expected its continued growth would lead to increased security costs, which could have spiraled out of control if not carefully monitored.

“The more the company grew, the more opportunities we saw to streamline and optimize our existing internal security process,” added Dixon. “By leveraging industry best practices and front-line security technology strategies, we would be able to build a new system that would benefit compliance, security, and our internal operations.”

> “All of the external auditors that were assessing our network were using Nessus to get a snapshot of our vulnerability status. We needed to know the answers before our auditors showed up on site, which is why we decided to deploy the vulnerability management tool they leverage for their assessments.”
>
> ***Eric Dixon***
>
> Information Security Manager,
>
> Information Security Technologies,
>
> McKesson University

The Tenable Solution

After a detailed and extensive evaluation, McKesson deployed several technology solutions and implemented best practices that would streamline and optimize its security process. The company selected Tenable SecurityCenter and the Nessus vulnerability scanner, which helped them gain enterprise-wide visibility and insight into vulnerability status, all from a single management console.

Tenable’s integrated approach to vulnerability management and assessment met all of McKesson’s top business requirements. The technology gave the medical giant a clear picture of its vulnerability status with actionable information that helped the security team prioritize known and emerging vulnerabilities on its vast network.

Since deploying the technology, McKesson has been able to significantly expedite its track to meeting PCI compliance. The company’s internal teams are never caught off guard by findings from third-party auditors. They know what the results will be in advance and have the opportunity to remediate any potential issues in accordance with the PCI guidelines.

Also, SecurityCenter has given the company detailed visibility into the entire new environment of acquired businesses and has quickly brought to light fundamental administration issues.

“We have been able to use Tenable to demonstrate shortcomings or to verify information from management consoles of other products like antivirus and patch management tools,” said Dixon. “Tenable can provide answers that the other tools cannot provide – specifically hardware and software asset management.”

Next Steps and Bottom Line

McKesson continues to use Nessus and SecurityCenter to uncover vulnerabilities across its network and ensure it’s meeting key compliance initiatives. As a part of its PCI compliance initiative, McKesson’s security team has recently been leveraging Tenable’s technology to pinpoint rogue personally identifiable information (PII) on endpoint systems.

“We’re in the process of creating a shortlist of systems that need to be investigated for PCI,” said Dixon. “Our daily scans enable us to quickly identify unencrypted social security numbers and credit card information on various systems — helping us locate and prioritize risks to our compliance status.”

For More Information

Questions, purchasing, or evaluation:
sales@tenable.com or 410.872.0555, x500
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com

tenable™ network security