

CUSTOMER CASE STUDY

Linedata Achieves Security, Compliance and Risk Reduction with NTT Application Security



The Challenge

Linedata is a global solutions provider operating in 50 countries. With more than 1,000 employees across the globe, they are dedicated to the investment management, the insurance and credit community.

Linedata believes growth in the financial industry will be driven by sustainability and innovation among its stakeholders.

Linedata was founded in January 1998 as the result of a merger of three firms. The corporate entity benefited at the outset from the best management, technology and operational expertise drawn from its three component companies, and wanted to ensure that its web applications were safe and secure across various implementations in the U.S. and abroad. With a long history and practice of acquisitions and integration, a standardization of vulnerability management across platforms is of primary importance.

Being in finance, Linedata is concerned with risk reduction and compliance in all facets of handling financial accounts and cardholder data, and sought out a best-of-breed solution for AppSec vulnerability management on a global scale.

The Use Case

Linedata is constantly rolling out new applications and interfaces for its customers, leading to the need for a robust testing program before any web application goes live. Although they looked at Qualys scanning solutions, their choice of Sentinel for application security fit prior to production: Linedata wanted more involvement with DevOps in the QA and implementation stages of the software delivery lifecycle (SDLC).

SENTINEL DYNAMIC KEY BENEFITS

- ✓ Fully-managed platform, with near zero false positives
- ✓ Advanced analytic capabilities to monitor trends and key statistics like remediation rate, time to fix vulnerabilities, and age of vulnerabilities
- ✓ Open API integration with bug tracking systems, SIEMs, GRC, RASP, VM, and WAF products
- ✓ Rule Packs identify and verify vulnerability defects
- ✓ Run scheduled assessments daily or on demand

SENTINEL SOURCE KEY BENEFITS

- ✓ Assess code at any point in the development cycle – even partial code
- ✓ Scan source code from any repository on premises
- ✓ Rule Packs identify and verify vulnerability defects
- ✓ Backed by Threat Research Center consultation
- ✓ Source Code Analysis and Directed Remediation

Linedata finds access to NTT Application Security experts in the Threat Research Center to be extremely valuable for helping their security team and its remediation efforts. They minimize the window of exposure through continuous scanning, creating a constant risk assessment program.

With integrations into the development environment, Linedata has been able to optimize developer time and free up resources to focus on their core business needs rather than constantly troubleshooting a laundry list of unverified vulnerabilities from other tools. Raymond Pompon, Director of Security at Linedata, said, "Having no false positives and engineers available for in-depth explanation of our vulnerabilities has been invaluable."

The Result

Sentinel's dynamic scanning prioritizes all issues found within Linedata web applications. Each finding contains detailed descriptions of the vulnerability, and advice on how to fix it. This saves the organization money by virtually eliminating false positives, and reducing the cost to fix. The remediation guidance and descriptive solutions offered up with every scan prove invaluable. Using Sentinel, Linedata's development team has reduced its time to remediate vulnerabilities over 75%.

Raymond Pompon rates NTT Application Security's Sentinel best in class for reliability, and best in class for scalability, performance, and ease of use.

Sentinel contains both executive-level reporting, including NTT Application Security Index for a cross-application view of security posture, and out-of-the-box PCI reports by application. DAST and SAST scanning have minimized disruption to the SDLC and maximized developer output.

NTT APPLICATION SECURITY KEY DIFFERENTIATION

- ✓ Sentinel exceeds requirements of PCI DSS by providing ongoing, verified vulnerability assessments for both internal and public websites with on-demand reporting.
- ✓ A Peer Benchmarking dashboard displays a comparison on key metrics comparing your web applications to industry and global averages.
- ✓ NTT Application Security Index is calculated from indicator data including window of exposure, number of vulnerabilities, time-to-fix, remediation rate, providing an instant, visual overview of all the websites monitored to prioritize remediation.



"Having no false positives and engineers available for in-depth explanation of our vulnerabilities has been invaluable."

- Raymond Pompon - Director of Security, Linedata

ABOUT NTT APPLICATION SECURITY

NTT Application Security is driving the future of application security. For nearly 20 years, organizations around the globe have relied on NTT Application Security to secure their digital footprint in an increasingly application-driven world. Bolstered by its award-winning, cloud-based application security testing platform, NTT Application Security delivers industry-leading accuracy by combining artificial and human intelligence to help security teams quickly identify and remediate potential vulnerabilities. Formerly WhiteHat Security, the company is an independent, wholly-owned subsidiary of NTT Ltd. and is part of NTT's security services portfolio.

For more information, visit www.whitehatsec.com.