

Leading Fortune 100 Manufacturer Taps ZeroNorth's Scalable Platform for Unified View of Risk to Global Infrastructure

Background

As a leading manufacturer, the company highlighted in this case study operates facilities around the globe, with more than 150,000 employees worldwide. With a long and successful history of growth and acquisition, the organization continues to expand its product portfolio by focusing on the customer experience. But with this exponential growth comes considerable risk.

Through the consolidation of multiple brands under one umbrella, this organization has a large and highly-fragmented IT infrastructure. As a result, it's difficult to gain visibility into security across lines of business and technologies while also understanding the overall risk posture. Without a way to correlate, prioritize and address the vulnerabilities presenting the most risk, the organization exposes itself to potentially devastating data breaches and/or crippling service disruptions with inherent downtime, reputational harm and financial and regulatory consequences.

The sheer size and distributed nature of the organization's IT infrastructure makes identifying risk and tracking remediation of even basic vulnerabilities challenging. As this multinational enterprise continued to operate through lean innovation to bring products to market quickly, the company's Chief Information Security Officer (CISO) struggled with how to gain a consistent and unified view of risk, across both applications and infrastructure—until finding ZeroNorth.

At-a-Glance:

GOALS:

- Gain a consistent and unified view of risk across both applications and infrastructure
- Identify and prioritize vulnerabilities presenting the most business risk
- Provide stakeholders with a simplified view of their vulnerabilities

RESULTS WITH ZERONORTH:

- Centrally manage tens of millions of pieces of vulnerability data and hundreds of thousands of assets
- Correlate and aggregate infrastructure and application security data to gain actionable recommendations
- Filter security issues to pinpoint and accelerate remediation efforts
- Track the remediation of unpatched assets
- Mitigate the need for tracking and reporting via spreadsheets

Finding ZeroNorth

ZeroNorth demonstrated the scalability of its [risk-based vulnerability orchestration platform](#) and showcased how certain capabilities could be enhanced and customized to meet the company's unique security requirements, including the ability to filter application and infrastructure security issues by business unit, geographic location and vulnerability type. As a result, the organization selected the ZeroNorth platform for its ability to meet specific requirements around performance, speed, ease-of-use and comprehensive visibility. Best of all, the organization could now protect its security investments by enhancing the existing scanning tools already in place.

During deployment, the ZeroNorth team worked with the company to integrate its existing vulnerability scanning and penetration testing tools and centralize all vulnerability data into the ZeroNorth platform. It also showed the company's security team how to add new scanning tools themselves as they scale their security program.

Managing Risk with ZeroNorth

ZeroNorth correlates and aggregates infrastructure and application vulnerability data from several disparate feeds and provides specific, actionable remediation recommendations. This level of reporting allows the customer to quickly hone in on high-severity vulnerabilities—such as active exploits and their associated assets—so they can identify and remediate the unpatched assets creating critical security gaps.

Furthermore, rather than tracking down hundreds of stakeholders and providing them with information on their assets' vulnerabilities, the company now gives their stakeholders access to ZeroNorth's

platform, which provides a simplified view of vulnerabilities filtered by a specific application or line of business. Consequently, business leaders can check in anytime on global operations to prioritize actions and facilitate faster and easier remediation processes.

Today, with ZeroNorth's risk-prioritized intelligence, the company manages tens of millions of pieces of vulnerability data and hundreds of thousands of assets directly through the platform. This ability has not only accelerated remediation efforts, but it has also mitigated the need for tracking and reporting via spreadsheets.

Through its holistic view of security across applications and infrastructure, ZeroNorth allows this customer to speed the discovery, correlation and prioritization of vulnerabilities with the most business risk. This insight helps the company accelerate remediation efforts, simplify compliance and improve security across the organization's global operations.

Learn More:

ZeroNorth is the industry's first provider of risk-based vulnerability orchestration across applications and infrastructure. By coordinating scanning tools throughout the entire software lifecycle, ZeroNorth provides a comprehensive, continuous view of risk and reduces costs associated with managing disparate technologies. ZeroNorth empowers customers to rapidly scale application and infrastructure security while integrating seamlessly into developer environments to simplify and verify remediation. For more information, follow ZeroNorth on [Twitter](#) and [LinkedIn](#) or [contact us](#) directly.