CASE STUDY

Nestlé Modernizes & Unifies Vulnerability and Risk Management with Brinqa Threat Exposure Management Platform

Nestlé's Blueprint to Consolidate, Prioritize, and Resolve Issues Faster

3X+ FASTER
Identification or Critical Vulnterabilities for Same Day Patching

80% REDUCTION
in Unassaigned Vulnerabilities

1 PLATFORM
Replaced Spreadsheets, PowerBI, Update Tasks & Remediation Assignment

100% ACCOUNTABILITY
with Complex Shared Ownership Model

Nestlé, a global leader providing nutrition and health products to hundreds of countries operates a vast, complex IT infrastructure. The company faced significant challenges in managing an overwhelming number of cybersecurity vulnerabilities across their organization. The team wanted to unify vulnerabilities and exposures from IT infrastructure, applications, and cloud systems for a single view of risk and the ability to prioritize and remediate efficiently.

The diverse range of technologies and the immense scale of operations at Nestlé put a strain on traditional vulnerability management processes. Spreadsheets and PowerBI could not support an operation of this scale, and Nestle leaders feared they would have to custom develop a solution. Instead they found Brinqa.

FRAGMENTED VULNERABILITY MANAGEMENT BOTTLENECKED MTTR & PATCHING

Nestlé's cybersecurity framework relied heavily on manual processes, which led to inefficiencies in managing vulnerabilities across their vast IT infrastructure. This manual approach increased the risk of human error and resulted in slow response times to emerging threats. Each team operated in silos, using different tools and procedures, which further compounded the difficulty of having a cohesive and timely reaction to security incidents.

The fragmented nature of their previous operational practices meant that information about vulnerabilities was often dispersed and inconsistent, leading to incomplete visibility and patchy threat management. This lack of integration hindered Nestlé's ability to prioritize and address the most critical vulnerabilities, leaving their attack surface that could have been mitigated with a more streamlined approach.

BRINQA STREAMLINED & UNIFIED NESTLÉ VULNERABILITY OPERATIONS

As the Nestlé team worked to modernize and improve the detection and management of exposures and vulnerabilities to reduce risk, they knew an aggregation and prioritization platform would be essential. They discovered the Brinqa threat exposure management platform known for its robust, flexible and enterprise-class risk-based vulnerability management.

ANNUAL REVENUE
$104B

GLOBAL ENTERPRISE

INDUSTRY
CPG, Food & Beverage, Retail Goods

SOLUTIONS
Unified Vulnerability Management, Threat Exposure Management, Vulnerability Prioritization and Remediation Automation

"Brinqa is a super flexible tool that's highly customizable to provide essential business context."

Angelo Punturiero
Vulnerability Management Senior Specialist in the Nestle' Cyber Security Operations Center (CSOC)

NESTLE'S RISK-BASED, AUTOMATED APPROACH ENABLED BY BRINQA YIELDS DRAMATIC RESULTS

The implementation of Brinqa yielded significant improvements in Nestlé's cybersecurity posture. By centralizing and automating vulnerability management, Nestlé achieved a more comprehensive and timely response to security threats, significantly reducing the risk of breaches. The new system enhanced visibility across all levels of the organization, allowing for faster detection, analysis, and remediation of vulnerabilities.

Ultimately, Brinqa's solutions empowered Nestlé to create a sophisticated shared ownership model to maintain a stronger, more resilient cybersecurity framework. The team is now well-equipped to handle the complexities of a modern global enterprise. With Brinqa, Nestlé maintains an efficient and automated vulnerability and exposure management operation that meet the specific needs of the business. The Brinqa platform integrated seamlessly with Nestlé's diverse technologies, automating crucial aspects of their vulnerability management process.

"With Brinqa, we increased the sophistication of this process over time, assigning the group of devices represented by their scope and so on."

Martin Karel
Leader Nestle' Cyber Security Operations Center (CSOC)

Brinqa enabled Nestle to take a continuous threat exposure management approach to reducing risk with a unified solution addressing the entire vulnerability risk lifecycle. By providing a solution that consolidates IT, cloud environments, and application vulnerabilities and exposures, Brinqa enabled the Nestle CSOC to view, prioritize, and act on vulnerabilities effectively.

The platform seamlessly integrated with existing security tools to consolidate findings, applying business context to prioritize risks and automate remediation. This comprehensive approach streamlines workflows and ensures that security teams can focus on the vulnerabilities that pose the most significant risk, enhancing the overall security posture at an enterprise scale.

SEE HOW BRINQA IMPROVES YOUR APPLICATION SECURITY POSTURE: BOOK A DEMO

Brinqa bridges the gap between security and IT operations, facilitating effective communication and collaboration. As the only platform that unifies and correlates data from IT, network, application, and cloud vulnerabilities, Brinqa ensures that every facet of an organization's infrastructure is protected from potential threats, making it the trusted choice for leading global enterprises seeking robust vulnerability management capabilities.

Watch the 5-minute demo

CUSTOMER BENEFITS

Consolidated IT assets, business context, exposures, vulnerabilities into a single system using the Brinqa Cyber Risk Graph to detect, understand, prioritize and resolve vulnerabilities fast.

Unlocked more value from historically disparate data sources with the visibility and context to prioritize security threats, respond to security audits, speed incident response and hold the business accountable for reducing risk

Operationalized a scalable and automated system to get ahead of mounting vulnerabilities, audits and reporting requirements to protect Nestle's complex global operations.

Eliminated frustrating and time-consuming tasks to speed MTTR by 80% and improve accuracy of detection and resolution of vulnerabilities, reducing human error and ensuring same day patching.

ABOUT BRINQA

Brinqa is the only company that orchestrates the entire cyber risk lifecycle — understanding the attack surface, prioritizing vulnerabilities, automating remediation, and continuously monitoring cyber hygiene — across all security programs. Brinqa Attack Surface Intelligence Platform is the source of truth for cyber risk. It empowers organizations to elevate the security conversation, hold risk owners accountable, identify security control coverage gaps, and manage and track all vulnerabilities in a single platform. Based in Austin, Texas, Brinqa is backed by Insight Partners. Learn more at **www.brinqa.com.**