ZERONORTH™

WHITE PAPER

The True Total Cost of Ownership (TCO) for Vulnerability Management Across Applications & Infrastructure

Organizations are pursuing digital transformation initiatives, ranging from the adoption of microservices to the Cloud to DevOps. For these initiatives to be successful, rapid development and delivery of software capabilities is crucial. The challenge, however, is finding ways to offer up these new products without sacrificing security.

Companies today are deploying a range of tools to find bugs, flaws and security vulnerabilities across their applications and infrastructure, including SCA, SAST, DAST, artifact/registry scanning, container scanning, pen testing, network scanning and infrastructure vulnerability scanning, among others. These tools are critical to the success of any vulnerability management program—but at what cost?

Understanding the Total Cost of Ownership (TCO) requires the consideration of many factors, such as acquisition, implementation, maintenance and support costs. As a vital part of the ROI calculation, the TCO is essentially the sum of all direct and indirect costs associated with vulnerability tools that goes well beyond the expense of software licensing.

This paper highlights the timeframes needed to support the comparison, selection, deployment, and on-going management of the tools and techniques inherent to a comprehensive vulnerability management program, across applications and infrastructure, as they will significantly impact the TCO of that program. The findings presented here are based on hundreds of hours of research by industry experts, with years of customer consulting engagement experience related to application security.

Stage 1: Tool Identification, Comparison, Procurement & Deployment

Choosing a new vulnerability scanning tool requires some organizational cost of resources, from testing various options (both open source and commercial) to analyzing results to deploying the selected product.

- Product Vetting / Bake Off: 1 – 3 months
- Solution Architecture & Deployment: 1 – 3 months
- Average Timeframe for Stage 1: 2 – 6 months

Stage 2: Tool Comparison and Vetting

Companies often test two or more tools to better assess how each option meets their business requirements. Even if not competitive, organizations will often vet tool effectiveness on their tech stack before proceeding. These comparison and vetting processes are important because they ensure businesses move forward with the best capability for their environment. That said, the process takes time, anywhere between 1 – 3 months to vet and compare options.

Stage 3: Tool Swap Out

While not always the case, a selected tool is often chosen to replace an existing one. For example, a company may begin their program with an open source tool before deciding to move on to a commercial option, or vice versa. However, this type of "rip-and-replace" process can be time consuming. New environments must be procured, replacement scanning regimes tuned for relative parity and operations adjusted, a process lasting anywhere from 6 – 12 months.

Stage 4: Application Onboarding

Once a scan or test tool is deployed, companies must onboard target applications, such as associating the applications and assets they wish to review with the new vulnerability discovery tool. Although timeframes vary by tool, they can be substantial. Average timeframe per application:

- SAST: 1 – 4 weeks
- SCA: .5 – 1 day
- DAST: 1 – 2 weeks

Timeframe estimates for organizations onboarding five applications:

- DAST: 5 – 10 weeks
- SAST: 5 – 20 weeks
- SCA: 2.5 – 5 days

Stage 5: Execute Scan & Triage Results

After the tool is deployed and applications are onboarded, scans must be executed and results triaged. Average timeframe for 300 applications, the typical number for a mid-size enterprise company:

- SAST: 1 – 5 days per app
- SCA: .25 – 1 day per app
- DAST: .5 – 2 days per app

Stage 6: Remediation and Verification

After results have been triaged, development and security teams are tasked with rectifying any issues and verifying remediation. The average timeframe for 300 applications:

- SAST: 1 – 5 days per app
- SCA: .25 – 1 day per app
- DAST: .5 – 2 days per app

Board and Executive Reporting

Given the higher level of visibility afforded to cybersecurity issues today, executive management and Boards of Directors are expected to understand risk in the context of the business. To address these requirements, security teams will be required to develop and deliver vulnerability and risk reporting, often on a monthly basis. Each report can take anywhere from 4 – 8 hours per month, which can lead to nearly two work weeks per year.

The following table summarizes typical timeframes for selection through on-going management of vulnerability tools.

	Stage 1: Identify, procure and deploy tools	**Stage 2:** Compare tools	**Stage 3:** Swap out tools	**Stage 4:** On-board applications to scanning tools (each app)	**Stage 5:** Execute scans and triage results (each app)	**Stage 6:** Verify remediation (each app)	**Board & executive report**
Manual process without Zeronorth	3-12 months	1-3 months	6-12 months	**SAST:** 1-4 weeks **SCA:** .5-1 day **DAST:** 1-2 weeks	**SAST:** 1-5 days **SCA:** .25-1 day **DAST:** .25-2 days	**SAST:** 1-5 days **SCA:** .25-1 day **DAST:** .5-2 days	4-8 hours per month

How ZeroNorth Can Reduce Your TCO

A risk-based vulnerability orchestration platform, ZeroNorth can significantly reduce the TCO of your security management program across applications and infrastructure. The ZeroNorth platform can:

- Facilitate comparison, selection and onboarding of security scanning tools
- Deliver a single platform for managing different vulnerability scanning tools, including identifying scan targets and scheduling and executing scans
- Create fast, frictionless integration with the development pipeline (secure DevOps)
- Provide a continuous, consolidated and prioritized view of vulnerabilities, together with remediation recommendations, in units of developer or operator work
- Maintain an executive-level view of how security and risk align with critical business assets

See how the process of selecting, onboarding and managing a vulnerability program compares when performed the ZeroNorth platform.

	Stage 1: Identify, procure and deploy tools	**Stage 2:** Compare tools	**Stage 3:** Swap out tools	**Stage 4:** On-board applications to scanning tools (each app)	**Stage 5:** Execute scans and triage results (each app)	**Stage 6:** Verify remediation (each app)	**Board & executive report**
With Zeronorth	Less than 1 month	Less than 2 weeks	Less than 1 month	**SAST:** Less than a week **DAST:** 1-2 days **SCA:** .5 day	**SAST:** .5 day **DAST:** .25 days **SCA:** .25 day	**SAST:** 0 day **DAST:** 0 days **SCA:** 0 day*	30-60 minutes per month

*ZeroNorth automatically detects and verifies when a previously identified vulnerability is remediated.

To learn more about how ZeroNorth can help optimize your security vulnerability management program and reduce cost, watch this 20-minute speed demo or contact us for more information.