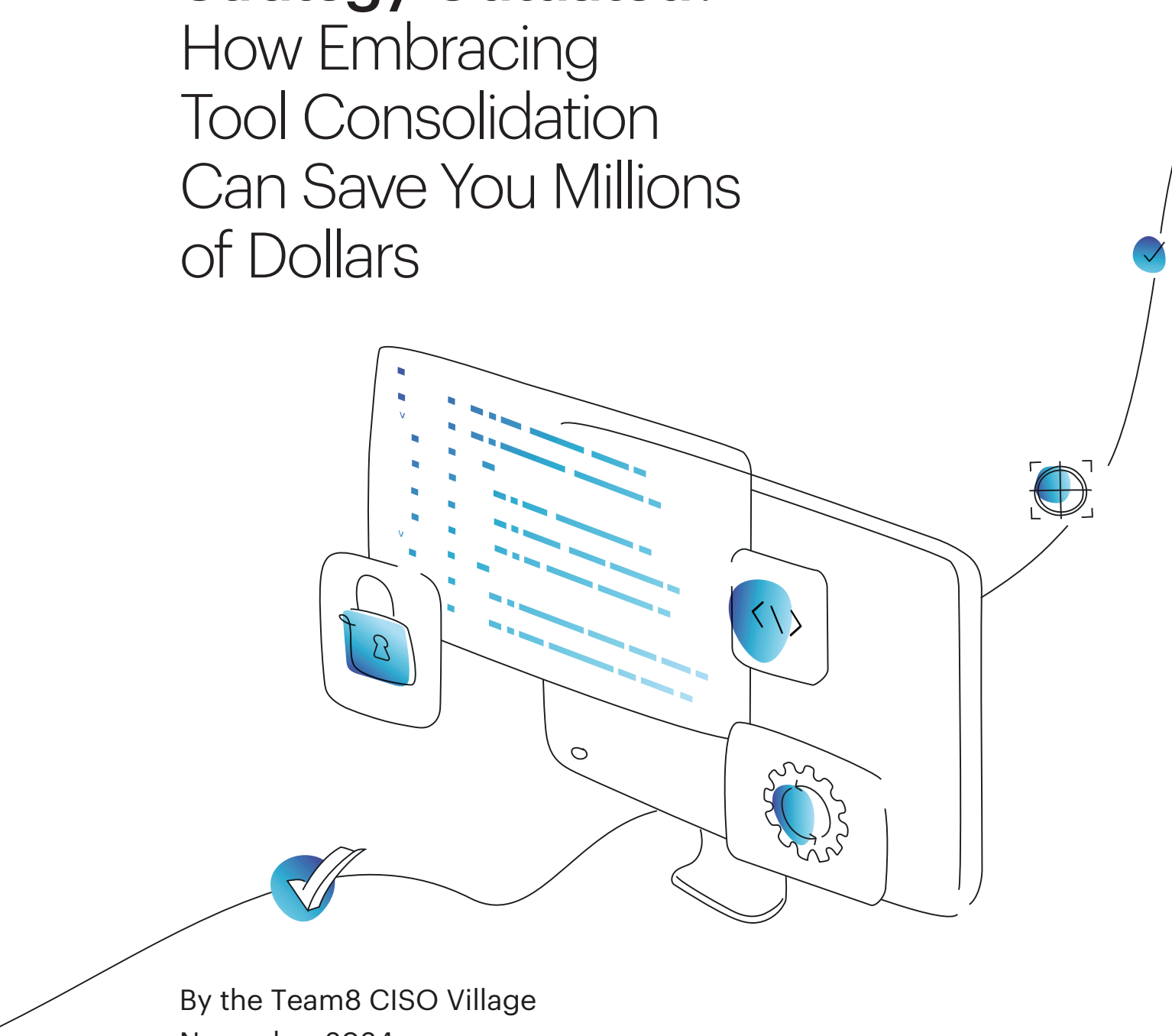
TEAM8™

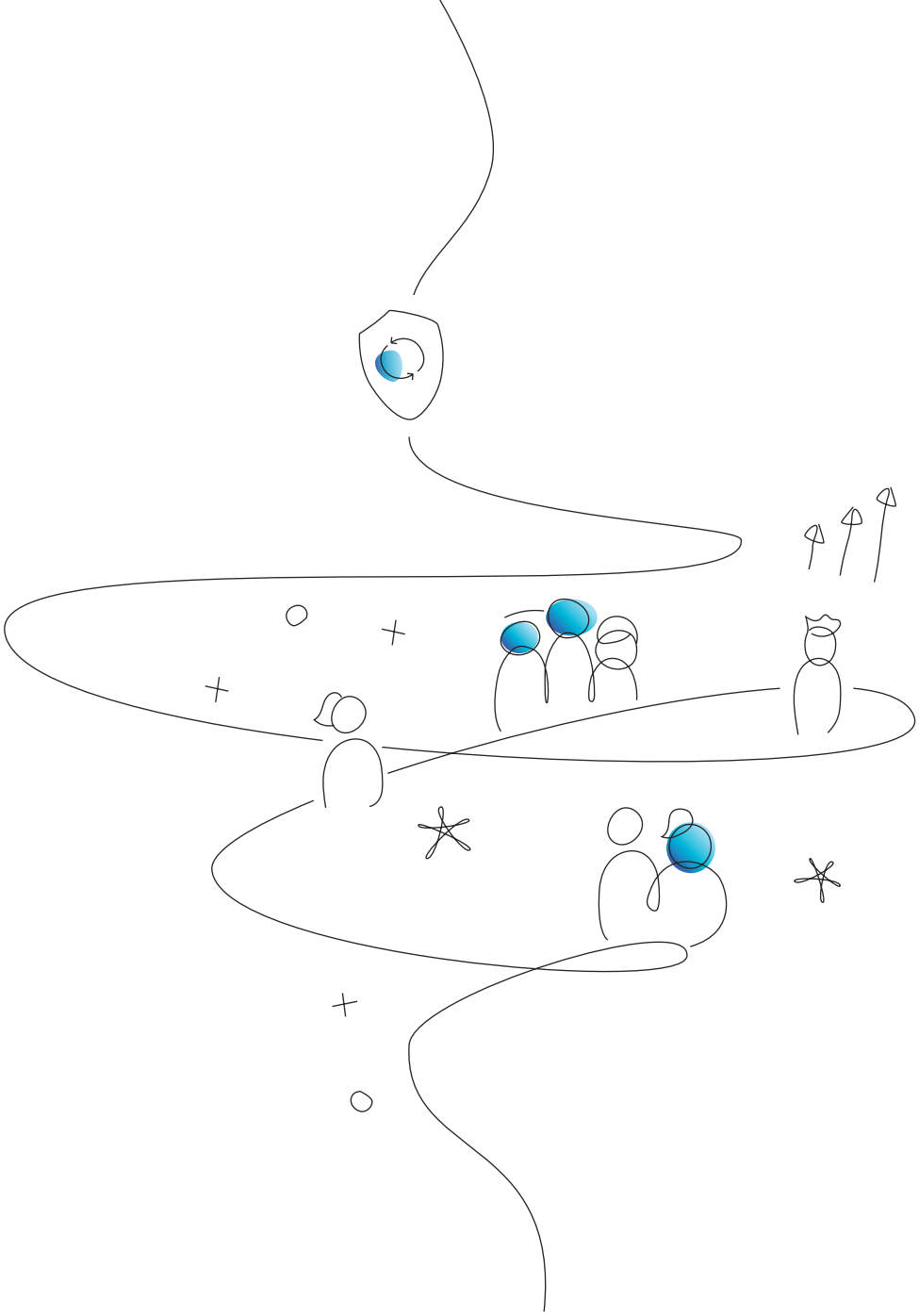
Is Your AppSec Strategy Outdated?

How Embracing Tool Consolidation Can Save You Millions of Dollars



By the Team8 CISO Village

November 2024



The Team8 CISO Village is a community of CISOs from the world's leading enterprises. The primary focus of the Village is to facilitate collaboration among the world's most prominent companies with the goal of sharing information and ideas, conducting intimate discussions on industry and technology trends and needs, and generating value and business opportunities for all parties.
By helping Team8 to identify real pain points and understand the requirements of large organizations, members of the Village are first in line to leverage solutions that are purpose-built by Team8's portfolio companies to support their needs.

To contact the Team8 CISO Village, please email **cisovillage@team8.vc**

WRITTEN BY

Ross Young
CISO-in-Residence
Team8

CONTRIBUTORS

Adam Arellano
Strategic Advisor and Cybersecurity Consultant

Pieter VanIperen
Chief Information Security Officer, Own Company

Andrew Wilder
Member, Board of Directors; Information Security Executive Education Washington University in St. Louis

Renana Friedlich
Senior Director, Global Head of Cyber Threat Management, PayPal

Heather Hinton
Cybersecurity Advisor, Former CISO at PagerDuty, Harvard Lecturer

Samir Sherif
CISO at F5

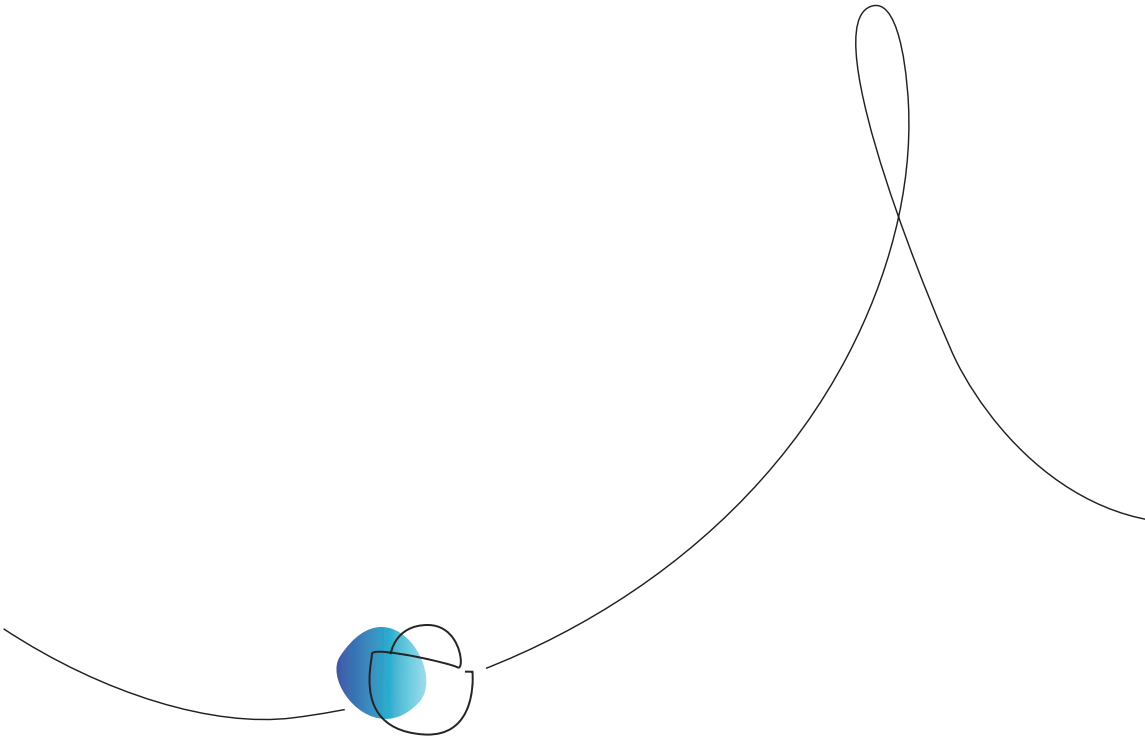
Jason Richards
VP, Information Security, Privacy & Identity, CHG Healthcare

Vesko Pehlivanov
Director of Security Engineering, ID.me

Karl Galbraith
Independent Security Consultant / Virtual CISO

Yabing Wang
VP, Chief Information Security Officer, Justworks

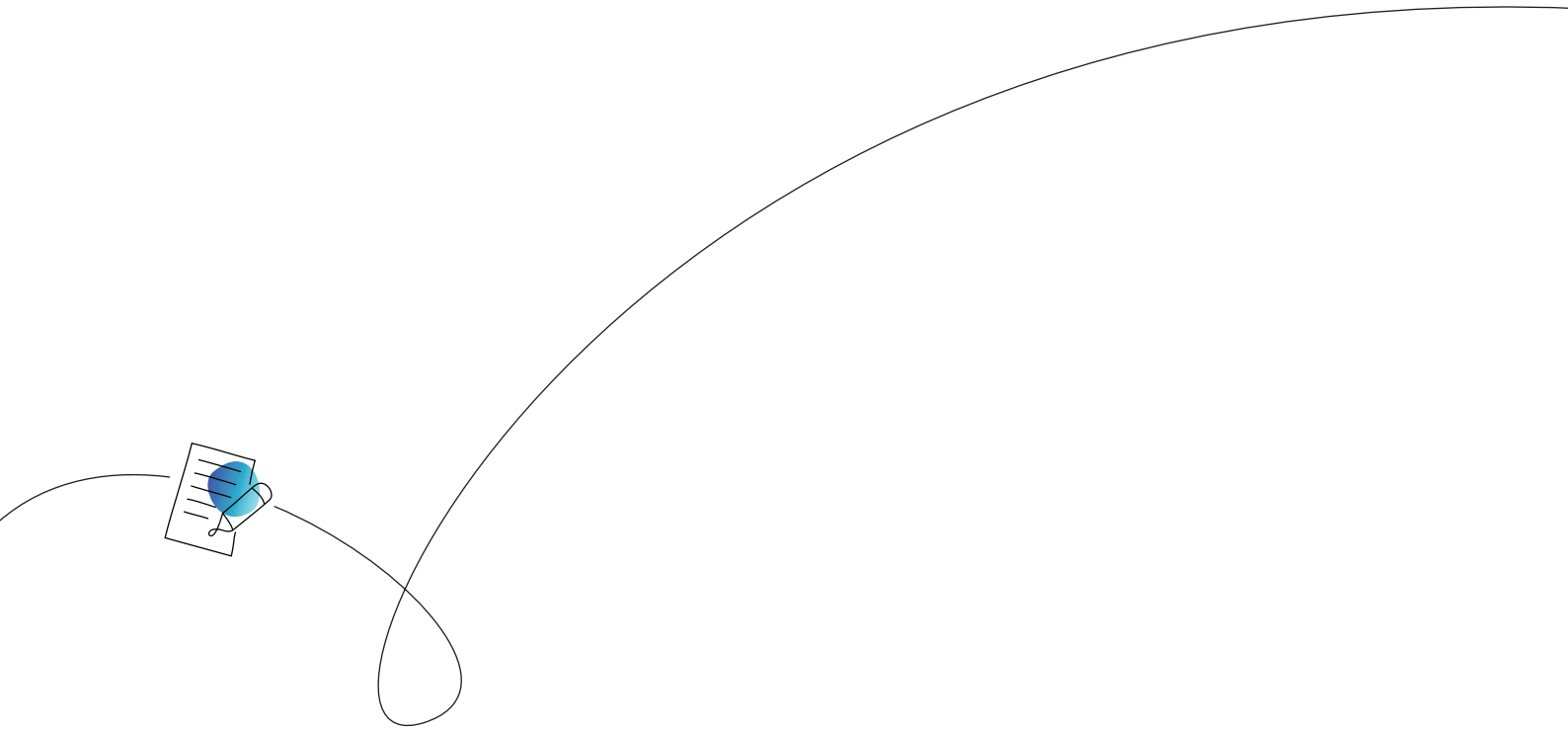
CONTENTS



INTRODUCTION

In today's cybersecurity landscape, one trend is clear: the number of tools used by companies continue to grow year after year. However, many of these tools, especially legacy ones, are no longer as effective or cost-efficient as they once were. These outdated tools often struggle with providing sufficient programming language, technology, and hybrid/multi-cloud coverage, diminishing the value they once offered.

As a result, companies face rising operations and maintenance costs, which is unsustainable. Alongside an increase in vulnerability sprawl and noise. In contrast, newer, modern tools that are fit-for-purpose offer better performance and cost-efficiency, making a strong case for their adoption.



Background

Let's look at the history of Application Security Tools to further illustrate this point:

- In the early 2000s, it was common for bad actors to scan IT systems to identify internet facing software that was unpatched and vulnerable to attack. The cyber industry created **Vulnerability Management Tools** (VM) such as Qualys, Tenable, and Rapid7 to help companies detect vulnerable software in their on-premises holdings. They initially focused on software used in Operating Systems, then applied the same approach to applications developed running on those OS.

- Quickly, "shift-left" became the approach of Application Security professionals. Finding vulnerabilities in production often leads to large remediation costs and additional risks, while detecting vulnerabilities in the early development phase can save money, effort and risk. This gave birth to **Static Application Security Testing** (SAST) tools such as IBM's Appscan, Checkmarx and Fortify.

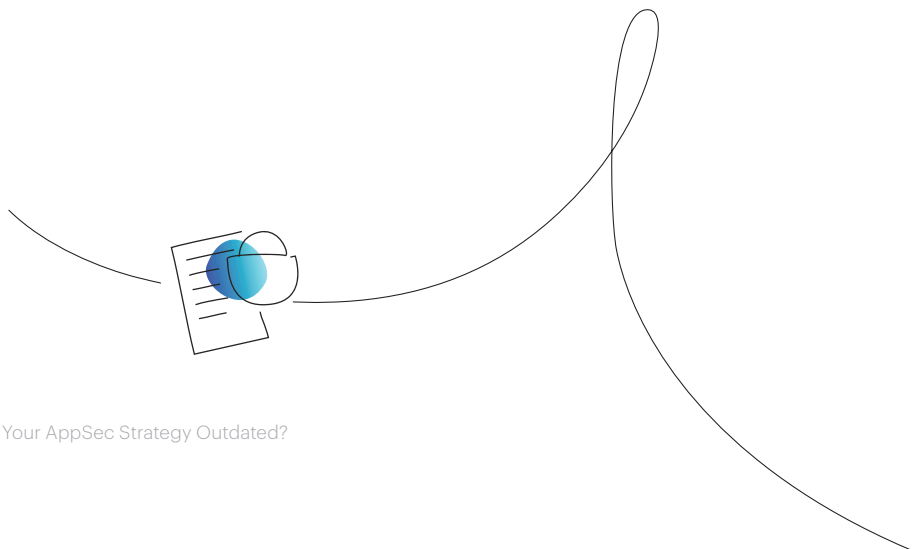
  · Initial languages were C, C++, C#, Java, Java script, etc.

  · As we added more and more languages to our products (Python, Rust, Ruby, Go, etc) we also needed to add more SAST tools to ensure complete coverage.

- Bad actors also started scanning websites for Web Application Vulnerabilities such as SQL Injection, Cross Site Scripting, and others. This gave rise to **Dynamic Application Security Testing** (DAST) tools. Vendors such as Web Inspect, Portswigger, and Acunetix created solutions in this space.

- **Software Composition Analysis** (SCA) emerged as a response to the growing use of open source software in the early 2000s. As an example, Equifax experienced a large-scale web application breach caused by running an outdated version of Apache Struts which was exploited. This focused the attention of the cyber industry to adopt SCA tools like Blackduck, Whitesource, and Snyk.

- Another way to approach app sec testing is to find vulnerabilities when the application is interacting with the program which is called **Interactive Application Security Testing**. IAST typically is conducted in a test or QA environment which still conducts testing before production. It no longer looked at the code itself, and it gave more contextual understanding of the code to reduce false positives. IAST is different from SAST which does not interact with the program and also differs from DAST which treats the program as a black box. Contrast Security and Synopsys are examples of a vendor who adopted this approach.



- Bad actors later began searching code repositories to steal API keys, passwords, and certificates within code. This led to the development of **Secret Scanning** tools like GitHub Secret Scanning, GitGuardian, Git-Secrets, and others.

- This list of Application Security Tools continues to increase as technologies evolve presenting new solutions that need defense. We see it in other areas such as container security tools, kubernetes security tools, cloud security posture management tools, mobile application security tools, API security, Software Bill of Materials, Infrastructure as Code, and others. See **7 Level Tech Stack** for an illustration of common security technologies used to identify application security findings.

7 Level Tech Stack

Layers	Examples	Application Security Tool
Custom Code	Java Source Code	SAST / DAST / IAST / Secrets Scanning
Application Libraries	JUnit, JDBC, ...	Software Composition Analysis / RASP Tool
Web Framework	Spring / Apache Struts	Software Composition Analysis / RASP Tool
Application Server	Tomcat	Vulnerability Management Tool
Runtime Environment	OpenJDK	Vulnerability Management Tool
Operating System	Linux / Windows	Vulnerability Management Tool
Cloud Environment	AWS / GCP / Azure	Cloud Security Posture Mgt Tool

Current Situation

With the growing need for multiple application security tools, large organizations can expect to allocate millions of dollars to their application security budgets. For large companies, the cost of these tools can vary significantly depending on industry and company size. On average, a major application security tool can easily exceed $650K per tool.

- Developer Costs: (500K) for two Systems Operators[1]
- Vendor Licensing Costs: (200K+) per tool

The resources necessary to deploy application security tools often exceed $700K per tool

For mature organizations that utilize at least six key application security tools (Vulnerability Management, SAST, DAST, SCA, Secret Scanning, and Cloud Security) each priced around $700K, the total investment quickly reaches $4.2 million. This figure can rise substantially if your vendor licensing costs are higher than 200K or if the large company purchases additional application security tools like container security, kubernetes security, cloud security posture management, mobile app security, API security, and more.

Most companies adopt a best-of-breed approach by combining application security tools from multiple vendors to ensure that all critical findings are surfaced. However, the tool sprawl to assure findings are not overlooked creates additional noise and additional costs from integrating these tools into a unified dashboard or custom single pane of glass to quell the noise. This integration typically requires internal staff to build dashboards and present metrics to leadership as well as deduplicate findings, triage and analyze an increased rate of false positives. As a result, when factoring in developers and licensing, an application security program budget is closer to $4.5 million.

Given the combined costs of running an Application Security program, we think the timing is right for organizations to consider how application security budgets might be spent differently in a way that promotes cheaper, faster, and most importantly more effective Application Security.

[1] It's essential to have two system operators/administrators in place to ensure that critical organizational knowledge is retained, even if one transitions to a new role or leaves the company.

Recommendations

Team8 Community members suggest that CISOs should focus on building a program that not only unifies the view of software vulnerabilities but also optimizes costs across developers, licensing, and hosting. Along the way, it's crucial to factor in additional security controls and ensure the budget reflects a clear ROI. Compensating controls to consider could include:

- Web application firewall (WAF) or RASP (Runtime Application Self Protection)
- External Penetration Testing service and Bug Bounty Program

Foundational discovery mechanisms which include inventory, data and asset mapping must be considered along with orchestrating the solutions in context, leveraging threat intelligence with business context and drive measurable results towards a common goal of identifying, measuring and reducing the real vulnerable attack surface.

To achieve this desired outcome, companies should evaluate whether to switch from a Best of Breed Approach to a Best of Suite approach which reduces the number of vendors, tools, and implementations to achieve cost savings.

For example

Best of Breed Approach	Best of Suite Approach
1. SAST	ASPM Tool
2. SCA	ASPM Tool
3. Secret Scanning	ASPM Tool
4. Custom Single Pane of Glass	ASPM Tool
5. Vulnerability Management	Modern CSPM/VM tool
6. Cloud Security	Modern CSPM/VM tool
7. DAST	Attack Surface Management (ASM) Tool
Estimated Yearly Costs • 14 System Admins - $3.5 Million • Licenses for 6 Technologies - $1.2 Million[2] **Total Costs = $4,700,000**	**Estimated Yearly Costs** • 6 System Admins = $1.5 Million • Licenses for 3 Technologies = $600 K **Total Costs = $2,100,000**

[2] Since the custom pane of glass is built internally there are no licensing costs paid by the organization

If we compare the two approaches to tool selection, we can see how a company might collapse four security tools (SAST, SCA, Secrets Scanning, and Custom Single Pane of Glass) into a single Application Security Posture management (ASPM) Tool that consolidates multiple tooling (shown in green). Vulnerability Management and Cloud Security tools could also be combined into a single vendor solution that covers Cloud Security Posture Management and Vulnerability Management for on-premises applications hosted on VMWare. Finally, CISOs can replace DAST with a modern replacement category called Attack Surface Management (ASM) that performs DAST Scanning capabilities and assists with creating software asset inventories. ASM Vendors can also rent service via external best of breed vendors such as Flashpoint, Authentic8, or Risk Reconn.

By taking this modern approach to tool selection, organizations can reduce procurement, third party risk management, and integration costs from six external vendors to three. Further, modern tools that can see across the stack can lend better context to findings, helping to deprioritize findings that are mitigated further in the stack and reducing false positives (findings for code that is never used or never accessible).

This helps teams target findings that are truly a risk while reducing pipeline inefficiencies and developer burdens. Many of the emerging tools provide flexibility to work with existing tools and transition slowly to a new paradigm. Moreover, the system operation costs of supporting a smaller number of distinct vendor solutions would also decrease.

For example

Streamlining seven tools into just three empowers organizations to significantly reduce the number of system operators from 14 to 6. By maintaining two administrators per vendor solution, this approach drives down operational costs from $3.5 million to $1.5 million. Instead of cutting headcount, many organizations choose to redeploy these skilled employees to other critical cybersecurity initiatives, maximizing their investment in talent and technology.

Large organizations embracing tool consolidation across 5+ security tools can save Application Security costs by $2.6 Million

The $2.6 million difference between your current spending of $4.7 million and a more optimized $2.1 million highlights a clear opportunity to revamp your application security program. Imagine uncovering significant savings that could reshape your budget and drive greater impact. By reevaluating your strategy, you could unlock efficiencies and redirect resources to critical areas while reducing your attack surface. Think about the possibilities: expanding your bug bounty program to attract top-tier ethical hackers, investing in broader penetration testing across your application portfolio, or enhancing red team assessments to identify new risks.

But the benefits don't stop there. The savings could also be redirected to other vital areas within your cybersecurity program, such as enhancing your Security Operations Center (SOC) capabilities or strengthening your Governance, Risk, and Compliance (GRC) efforts. Alternatively, some or all of these funds could be returned to the business, directly contributing to increased profitability of the company. It’s a great way to start showing the CISO is an executive business leader in the company.

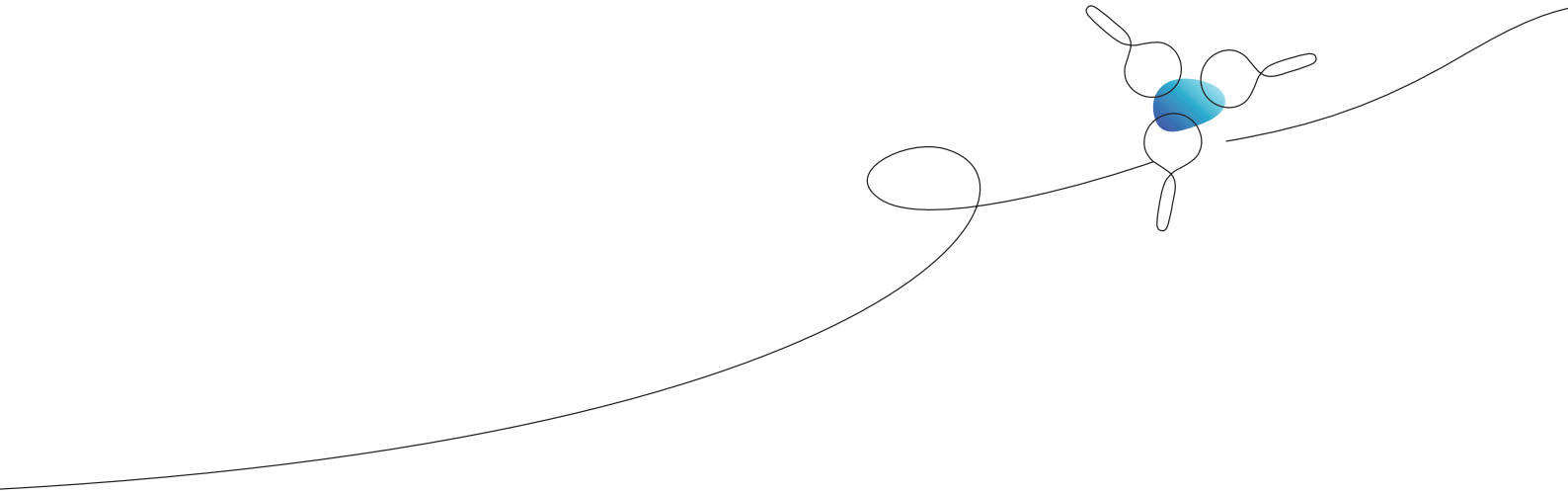
In essence, this opportunity is not just about cutting costs, increasing efficiency and reducing attack surface—it's about strategically reinvesting in areas over time that can drive even greater value for your organization.

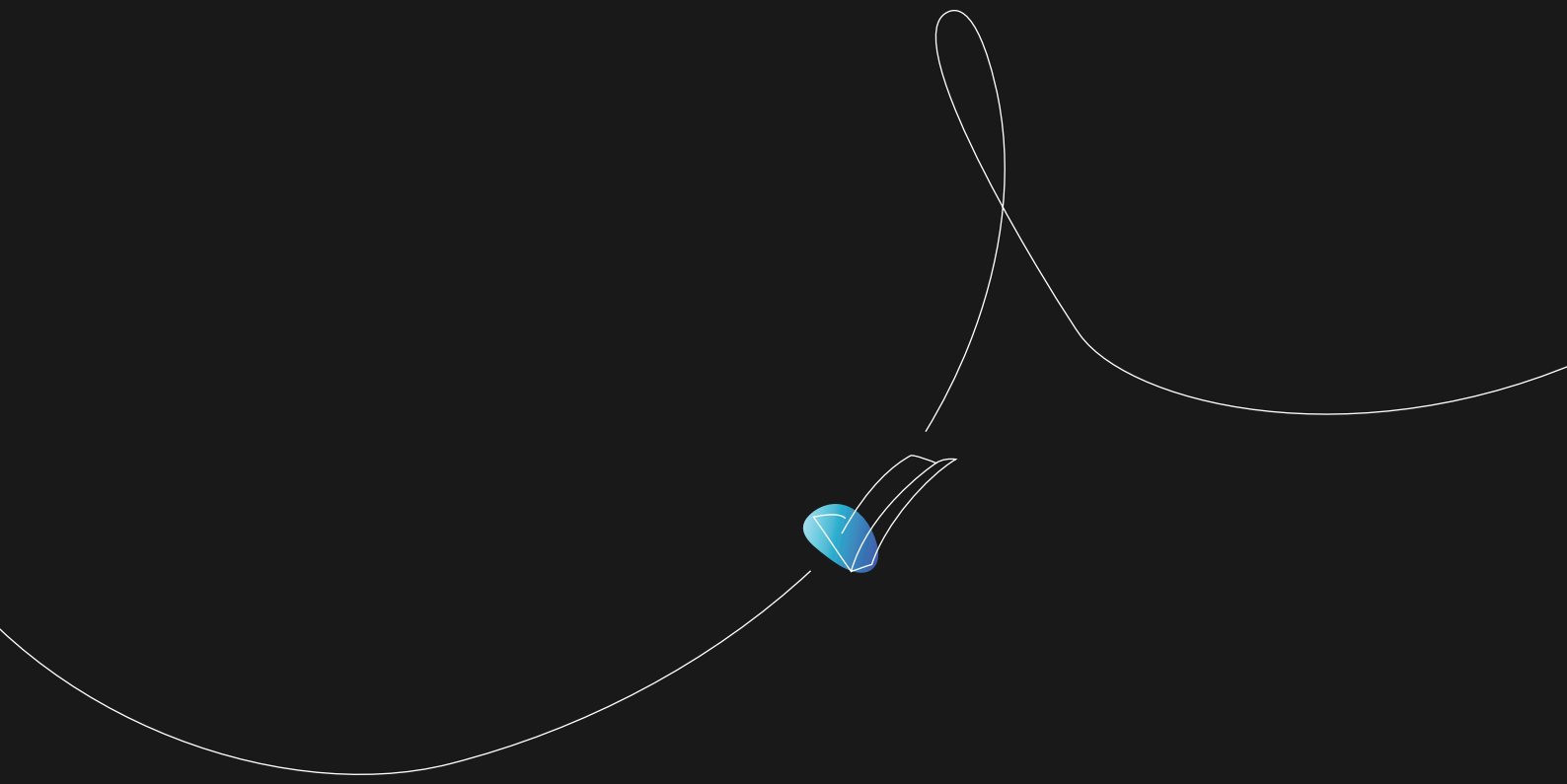
CONCLUSION

It's time to rethink how we invest in application security. The landscape is changing, and so are the tools we rely on. By consolidating legacy tools and adopting modern, purpose-built solutions, you can significantly reduce costs, minimize operational complexity, and drive more impactful results. Streamlining your tools not only cuts down vendor management and integration headaches, but it also helps your teams focus on what truly matters—reducing risk and enhancing security.

Imagine repurposing millions in savings towards more strategic initiatives, from expanding bug bounty programs to advancing red team assessments. This isn't just about trimming the fat; it's about driving innovation in your security strategy. By optimizing your application security program, you're not only protecting your organization but also creating a competitive edge that contributes to the bottom line.

Now is the moment to act. Take a proactive approach, revamp your tooling strategy, and unlock the full potential of your application security program. The future of cybersecurity is smarter, faster, and more cost-efficient—let's seize it together.





For more information

Contact us at: cisovillage@team8.vc | www.team8.vc

TEAM8™