BSIMM12 Digest: The CISO’s Guide to Next-Gen AppSec

Introduction

As the rate of software development accelerates, organizations are forced to adopt new practices and undergo cultural shifts. DevOps, with its focus on rapid service delivery, was born of these needs. When done right, the DevOps approach helps organizations build reliable software quickly, with fewer roadblocks than agile or waterfall methodologies.

But with change comes challenges. Many organizations have struggled to adapt and improve their application security (AppSec) practices to keep pace with development cycles. Even after shifting left and investing in tooling integrations, many continue to push vulnerable code into production. Getting the right mix of tools, people, and processes is a constant challenge. Using too few tools leaves gaps in the security posture, while using too many tools leads to friction and tool fatigue for developers.

How can security leaders know how much is too much when it comes to their AppSec activities? How little is too little? What investment makes sense for their organization? What investment is overspending or duplicating efforts?

These are the questions that Synopsys Building Security In Maturity Model (BSIMM) and its annual report were created to answer.

What is BSIMM?

In 2008, consultants, researchers, and data experts in what is now the Synopsys Software Integrity Group set out to gather data on the various paths that organizations take to address the challenges of software security. Their goal was to examine organizations that were highly effective in software security initiatives, conduct in-person interviews on those organizations' activities, and then publish their findings.

The BSIMM report—now annual and in its 12th iteration—offers a unique perspective based on data gleaned from real-world observations. It provides CISOs and other security leaders with a model and framework to test, measure, and benchmark their own software security programs, including key activities, practices, and tools to consider implementing.

Regardless of how well-known the organization or how mature its AppSec program, executives can use BSIMM as a measuring stick to gauge themselves against industry trends, risks, priorities, and other factors. When used to its full capacity, BSIMM functions as a roadmap for creating or improving a successful AppSec program that is tailored to the specific needs of each organization. Executives can identify their own goals and objectives and then layer in BSIMM data to determine where additional effort and investment are needed.

Key AppSec trends in BSIMM12

Each year, BSIMM reveals key market trends and what they mean for AppSec leaders. These trends indicate overarching, or more holistic, shifts in how industries approach their software security programs. Executives can review these trends to help evolve their own programs by identifying any gaps and determining what activities would be beneficial to add or augment. Some of the key trends are listed below.

High-profile ransomware and supply chain disruptions spur scrutiny of software security

Over the past two years, BSIMM data shows a 61% increase in the "identify open source" activity and a 57% increase in the "create SLA boilerplate" activity among participating organizations.

Businesses are learning how to translate risk into numbers

Organizations are exerting more effort to collect and publish their software security initiative data, demonstrated by a 30% increase of the "publish data about software security internally" activity over the past 24 months.

Increased capabilities for cloud security

Increased executive attention, likely combined with engineering-led efforts, has resulted in organizations developing their own capabilities for managing cloud security and evaluating their shared responsibility models. There was an average of 36 new observations over the past two years across activities related to cloud security.

Security teams are lending resources, staff, and knowledge to DevOps practices

BSIMM data shows software security teams moving away from mandating security behaviors and toward a partnership role, sharing resources, staff, and knowledge with their development peers to ensure security efforts are included in the critical path for software delivery.

Continuous defect discovery and continuous improvement

BSIMM12 indicates that more organizations are implementing modern defect discovery approaches and favoring continuous monitoring and reporting rather than using a "point in time" defect discovery approach. While governing approaches remain mostly manual, governance-as-code is trending upward and currently observed in 15% of the organizations measured in BSIMM12.

Security testing in QA automation has doubled

Over the past two years, the "include security tests in QA automation" activity has doubled. In the same time span, the activity "integrate opaque-box security tools into the QA process" increased by more than 50%.

Building a software Bill of Materials

BSIMM data shows an increase in capabilities focused on inventorying software; creating a software Bill of Materials; understanding how the software was built, configured, and deployed; and on the organization's ability to redeploy based on security telemetry.

Emerging AppSec activities in BSIMM12

Activities tend to change over time as the software security environment and organizational priorities change. For example, BSIMM12 data indicates a 61% increase in the "identify open source" activity over the past two years, probably due to the prevalence of open source components in modern software and the rise of attacks using popular open source projects as vectors.

Highest growth activities over the past 24 months

The activities that showed the highest growth include the following:

- Use orchestration for containers and virtualized environments (560% increase)
- Ensure cloud security basics (555% increase)
- Use application containers to support security goals (214% increase)
- Include security tests in QA automation (100% increase)
- Perform design review for high-risk applications (69% increase)
- Include security resources in onboarding (64% increase)
- Identify open source (61% increase)

BSIMM12 findings by industry

Each year, BSIMM offers a glimpse into the current success, weakness, and maturity of organizations within specific industry verticals. This allows CISOs and other security leaders to compare data against their industry peers and pinpoint areas of specific need in their own AppSec programs. BSIMM12 represents 128 organizations across nine verticals.

Important industry comparisons

Key takeaways from every BSIMM report include which industries outperform their peers. In BSIMM12, FinTech, Internet of Things (IoT), cloud, and independent software vendors (ISVs) stand out.

- **The leaders in maturity.** IoT, cloud, and ISVs are the three most mature verticals represented in BSIMM12. IoT organizations show the highest level of maturity in practices related to front-loading design (i.e., decisions at earlier stages of the design process), including "training," "security features and design," and "architectural analysis." In the "architecture analysis" practice, IoT organizations are significantly higher than other verticals, perhaps because many IoT devices are expected to function in production environments for long periods of time. Cloud organizations are ahead in the "code review" practice, perhaps due to the explosion of code created by cloud firms over the past few years.
- **Regulated industries.** Financial services, healthcare, and insurance firms all operate in highly regulated industries. BSIMM12 found that large financial services organizations reacted to regulatory pressures by starting software security programs much earlier than their healthcare and insurance counterparts.
- **Healthcare.** Despite the similarity of compliance and regulatory drivers across the three verticals, healthcare generally trails insurance and financial services in its software security maturity.
- **FinTech.** Introduced in BSIMM11, the FinTech vertical exceeds in identifying open source and controlling its risk. IoT organizations are nearly identical in identifying open source, but FinTech organizations show more than double the observation rate in controlling open source risk.

Using BSIMM to improve AppSec programs

For CISOs new to BSIMM, the depth of data and wealth of information can be intimidating. But regardless of size, maturity level, or industry, security leaders can leverage BSIMM as a roadmap to help develop, improve, and mature their software security programs. The following activities provide a good foundation or starting point.

1. Identify maturity phase

BSIMM defines three maturity phases of an AppSec program. Identifying whether an organization is emerging, maturing, or optimizing is a necessary foundation from which to build. Executives should review the common markers of each phase (see chart below) to determine where they currently stand.

Emerging	Maturing	Optimizing
• An organization starting from scratch or formalizing current ad hoc security activities • Initial strategy is defined, foundational activities have been implemented, a rough roadmap might be developed • Restraints include budget, lack of resources, and lack of talent • Approximately 12 to 24 months needed for evolution	• An organization with an existing or emerging AppSec program that is working on scaling, streamlining, and meeting executive expectations • Key activity may include working to apply existing activities to a greater percentage of technology stacks, departments, or software portfolio • Security leadership might add fewer activities while increasing depth, breadth, and cost-effectiveness of current activities	• An organization that is fine-tuning its existing AppSec program • Security management has a clear view into operational expectations and associated metrics • Seamless adaptation to technology change-drivers • Risk management and business value are clearly demonstrated as differentiators • AppSec leader(s) may be undergoing personal career growth from technology executive to business enabler

2. Embrace DevSecOps

Executives must address the role of security within a DevOps environment, which means embracing DevSecOps. Focus should be placed on promoting security self-service for the development team, including automation in the software development life cycle (SDLC) and removing points of friction. But simply integrating and automating more security testing tools to test everything all the time isn't the answer; this approach doesn't scale to meet the demands of DevOps. Organizations need to adopt a new approach that includes risk-based priorities aligned to security policies, automated rulesets that govern how risk is managed, and an orchestration process that operates independently of the core DevOps pipeline.

3. Implement key activities

Activities form the backbone of BSIMM. Each year's report identifies what activities the various organizations in the data pool are performing. The activities are then rated based on frequency. This approach gives CISOs a snapshot into the most widely used activities of their peers.

Here are the top 10 activities observed among the 128 organizations represented in BSIMM12 and the percentage of organizations that engage in that activity:

- Implement life cycle instrumentation and use to define governance (92%)
- Ensure host and network security basics are in place (91%)
- Identify personally identifiable information obligations (89%)
- Perform security feature review (88%)
- Use external penetration testers to find problems (87%)
- Create or interface with incident response (84%)
- Integrate and deliver security features (80%)
- Use automated tools (80%)
- Ensure QA performs edge/boundary value condition testing (78%)
- Translate compliance constraints to requirements (77%)

4. Define roles and responsibilities

Identifying individuals and their roles in an AppSec program reduces confusion while empowering teams to be proactive and innovative. BSIMM reviews its study subjects each year to determine the key players responsible for application security. As always, success starts at the top; executive leadership is critical. CISOs should review the roles identified by BSIMM to determine if they can create clearer boundaries and expectations in their own organizations.

- **Executive leadership.** The most successful AppSec initiatives are those with executive sponsorship and oversight. Programs gain acceptance and support throughout organizations when they have executive buy-in. And having a single person (typically the CISO) in charge of security decisions allows the program to move forward without bottlenecks.
- **Application security team.** Virtually all 128 organizations observed in BSIMM12 have an established AppSec team in place, although their structure and the names they go by vary greatly. Without this team, organizations cannot be consistent in their AppSec efforts. Executives should prioritize and closely align with this team to help drive and deliver security goals.
- **Security champions.** Often referred to as "satellites" in BSIMM vernacular, security champions are employees outside the security team who help raise awareness and garner support of AppSec practices among different members of the organization. Executives should identify existing security champions within their organizations and foster relationships with potential champion recruits who can help ensure compliance with AppSec best practices throughout the SDLC.
- **Everyone else.** All employees play an indirect role in security. They can spread awareness, understanding, and support for security practices and development. Executives should encourage education, inclusion, and awareness across the entire organization to give their AppSec programs the best chance to succeed.

5. Getting started

For new CISOs or those in emerging organizations, consider the checklists below to help jumpstart your AppSec program. (For CISOs overseeing existing programs, see activity 3 above to fill in any gaps with the top 10 activities observed in BSIMM12.)

Governance-led checklist for getting started

✓ **Leadership.** Put someone in charge of software security and provide the resources they will need to succeed.

✓ **Inventory software.** Know what you have, where it is, and when it changes.

✓ **Select in-scope software.** Decide what you're going to focus on first and contribute to its value streams.

✓ **Ensure host and network security basics.** Don't put good software on bad systems or in poorly constructed networks (cloud or otherwise).

✓ **Do defect discovery.** Determine the issues in today's production software and plan for tomorrow.

✓ **Engage development.** Identify those responsible for software delivery pipelines, key design, and code, and involve them in the planning, implementation, and roll-out at scale of security activities.

✓ **Select security controls.** Start with controls that establish some risk management to prevent recurrence of issues you're seeing today.

✓ **Repeat.** Expand the team, improve the inventory, automate the basics, do more prevention, and then repeat again.

Engineering-led checklist for getting started

✓ **Inventory software.** Know what you have, where it is, and when it changes.

✓ **Select in-scope software.** Decide what you're going to focus on first and contribute to its value streams.

✓ **Ensure host and network security basics.** Don't put good software on bad systems or in poorly constructed networks (cloud or otherwise).

✓ **Choose application controls.** Apply controls that deliver the right security features and also help prevent some classes of vulnerabilities.

✓ **Repeat.** Expand the team, improve the inventory, automate the basics, do more prevention, and then repeat again.

Next steps

The CISO's mandate is to protect their organization from seen and unseen threats. This requires constant diligence to improve security best practices. BSIMM can be a helpful guide for starting, improving, or fine-tuning such practices as they relate to software security.

While addressing the five activities above, the CISO or security leader should consider diving into the full BSIMM12 report, which contains greater insight into the activities, practice areas, and domains of the most successful AppSec programs operating today.

BSIMM12
2021 INSIGHTS &
TRENDS REPORT

BSIMM 12

Download the BSIMM12 report now

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com