BLACK DUCK®

WHITE PAPER

ACHIEVING TRUE SCALE APPLICATION SECURITY IN A REGULATED, AI-DRIVEN WORLD

THE CHANGING SOFTWARE WORLD

- Bigger applications
- More applications
- More regulations
- More attacks

60%

Percentage of organizations

60%

Percentage of tests produce that noise

60%

Percentage of organizations that say security delays development

Software continues to drive growth and innovation in every industry around the world. And as businesses and industries evolve, so too does the software they're running on. The average application contains three times more code today than it did four years ago. And by 2030, there will be three times more applications than there are today.

It's not just the size and number of software applications that's growing; it's also the complexity and the speed at which it's being developed. Thanks to artificial intelligence (AI), new code is being generated at a record pace. By 2030, AI-generated code is projected to increase by 400%—compounding the growth in the size, number, and complexity of applications.

At the same time, thanks to global software regulations, accountability and compliance are now core requirements for doing business. Customers, vendors, and regulatory bodies demand that organizations attest to the safety and security of their software applications. This means that just as software development is becoming faster and more complex than ever, the need to ensure that software applications perform safely, securely, and transparently is also more important than ever.

And all this is happening while global cyberattacks continue to proliferate at an alarming rate. 2024 saw a 30% increase over the previous year, reaching a staggering 1,600 attacks per organization per week on average.

ELIMINATE TRADEOFFS

If organizations are going to manage the explosive growth in size, number, and complexity of their software, while ensuring trust and maintaining compliance, they need to solve the friction that persists between security and development. According to Black Duck's 2024 "Global State of DevSecOps" report, 60% of organizations say that up to 60% of their security tests produce noise. It's no surprise then that the same 60% say that security either moderately or severely delays development.

When you add AI to the mix, the challenges compound. Ninety percent of organizations use AI tools, but only 24% are very confident in their ability to secure AI-generated code.

Clearly, the traditional tradeoffs between speed and accuracy, innovation velocity and compliance rigor, budget realities and integrity assurance, and security and time to market are no longer tenable. These compromises are outdated and leave organizations at risk.

What can they do to adopt AI-generated code securely without adding more friction or the need to choose between speed and quality?

For starters, organizations need to ensure that security is meeting developers where they are. That means adopting application security testing (AST) solutions that are easy to onboard and use. The solutions need to scale across teams, applications, and projects, and be able to expand test requirements to keep pace with future business growth. And to further reduce friction and improve collaboration, organizations need a uniform way to define, measure, and prioritize software risks at every stage of the software development life cycle (SDLC).

ELIMINATE TRADEOFFS

- Meet developers where they are
- Enterprise-grade AST
- Scalable security
- Uniform risk management

Meeting Developers Where They Are

In the modern world of software development, it's crucial for AST solutions to integrate seamlessly into the existing workflows and tools that developers use every day. This means integrating with popular integrated development environments (IDEs), source code management (SCM) systems, and continuous integration / continuous deployment (CI/CD) pipelines. This ensures that developers can perform security testing without leaving their familiar environments, reducing friction and improving adoption.

It also ensures that developers receive real-time security feedback on code changes, automatically generated pull request comments, and instant notifications of security issues. These all help maintain the speed and efficiency of the development process while ensuring that security remains a top priority.

Automation is key. Automatic bulk onboarding of applications, projects, and branches from different repositories reduces the time and effort required to set up and maintain security testing. It also ensures that all code is consistently tested and monitored for security vulnerabilities. The automated approach not only streamlines initial setup but also ensures that new projects and branches are seamlessly integrated into security testing workflows, maintaining a high level of security coverage and compliance.

Enterprise-Grade AST

Although it's vital that AST solutions meet developers where they are, they still need to meet the rigorous demands of large organizations. They must be comprehensive *and* fast. This means providing a full suite of testing capabilities, including static application security testing (SAST), software composition analysis (SCA), and dynamic application security testing (DAST). The solutions must support all test types, from ad hoc to point-in-time to fully automated, with predefined policies to streamline the process.

Large organizations require security tests to run concurrently across an unlimited number of applications and projects, regardless of the number and types of tests. By leveraging concurrent, unlimited scanning, teams can achieve faster feedback cycles and more efficient use of resources, enhancing both productivity and security.

Organizations need the flexibility to define and enforce security policies that align with their specific needs and compliance requirements. These policies can be tailored to different stages of the SDLC and applied to various types of applications and projects. Custom rules and thresholds ensure that security testing is not just comprehensive but relevant. Customized policies also ensure that all applications meet security benchmarks, as defined by the organization.

Scalable Security

Security solutions need to fit the needs of today—and tomorrow. They also need to support large, complex organizations with extensive and diverse development environments. They must handle the increasing volume of code being produced by AI, at the speed AI is producing it, within large and complex development environments, without compromising performance. This scalability is crucial for organizations that need to maintain a high level of security while rapidly expanding their software portfolio.

These abilities—concurrent scanning, seamless integrations, and automatic onboarding—also enhance scalability, allowing security to be baked into the development process without causing bottlenecks.

POLARIS DELIVERS

- Easy onboarding and deployment
- Concurrent scanning
- AI-driven remediation assistance
- Customizable policy management
- Development and DevOps toolchain integrations
- Real-time collaboration, reporting, and risk insights

Uniform Risk Management

Organizations need a centralized and consistent approach to identifying and mitigating security risks across all applications and projects. The approach must align with business goals so that security policies are tailored to the organization's specific needs and compliance requirements. This will help focus security efforts on the issues that matter.

Unified dashboards centralize and consolidate security findings from multiple testing methods (SAST, SCA, DAST) across third-party tools and vendors. They also provide centralized visibility to ensure that risk assessments are standardized and security policies are uniformly enforced everywhere code happens.

Dashboards should also be tailored to teams and roles. Executives should receive high-level insights and analytics to make informed decisions. Security teams should be able to drill down into detailed findings and prioritize risks. Developers and DevOps teams benefit from real-time visibility into which issues are critical and how to fix them. Unified dashboards help ensure that security is not an isolated process but a coherent part of the development life cycle, simplifying risk management and facilitating collaboration.

TRUE SCALE APPLICATION SECURITY

Today's organizations need to deliver secure, safe, high-quality software at the speed their customers demand. This requires application security that can handle the many complex pressures that enterprises face. This means ensuring

- **Speed at scale.** Rapidly develop, deploy, and manage applications regardless of size or volume of data and users.
- **Accuracy at scale.** Maintain high levels of precision and reliability across applications of all types and sizes.
- **Volume at scale.** Safeguard that speed and accuracy won't be compromised when large volumes of data, users, and applications need to be secured.
- **Compliance at scale.** Establish consistent and rigorous compliance practices that adhere to all relevant legal, regulatory, and industry standards as your organization's applications grow and multiply.

Black Duck Polaris Platform

Black Duck Polaris™ Platform is an integrated, cloud-based AST solution that delivers True Scale Application Security. It provides market-leading security analysis engines in a unified platform, offering intelligent risk management capabilities. It automates any scan, anytime, anywhere, all at once, at any stage of the SDLC, and integrates with the development and DevOps tools that organizations are already using. Polaris offers actionable summaries of detected vulnerabilities, AI-generated code fix recommendations, and other insights to help organizations build secure software better and faster.

SEE POLARIS IN ACTION

Watch the on-demand demo to see how Polaris integrates market-leading SCA, SAST, and DAST engines in a unified platform to offer the most comprehensive and intelligent risk management solution. The demo covers capabilities such as seamless IDE, SCM, and CI/CD integrations; automated policy and workflow management; and AI-powered analytics and trends reports.

Watch the demo now

ABOUT BLACK DUCK

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.