prismo
Dev-Native Security

SOLUTION BRIEF

Automate DevSecOps processes across the SDLC with Prismo Dev-Native Security

Jan 2022

Digital Economy Challenges

Today, many organizations find themselves in hyper-competitive, fast changing markets driven by globalization, rapid technological innovation, and the digital transformation of business processes and commerce. While the evolution and rise of the digital economy has created spectacular opportunities and growth for many, it has also created new types of challenges that must be overcome if organizations want to compete and thrive in the future.

Digital Transformation and the Need for Speed

To compete in today's hyper-competitive global economy, organizations must be agile and able to adapt and innovate quickly. The rise of Agile development and adoption of cloud-native architectures have increased the pace of software innovation dramatically, but often at the expense of quality, security and privacy. To deliver on the business' ever-increasing need for speed, Dev and Ops teams need to remove bottlenecks in the SDLC by reducing tech stack complexity and automating manual processes such as software testing and security assessments.

Cyber Threats

Not surprisingly, cyber risk has grown hand-in-hand with digital business and transformation initiatives. As more data, applications, and business processes move to the cloud, attack surface expands exponentially, threat actors adapt, and legacy security stacks become less and less able to protect the business from more advanced and sophisticated attacks like Supply Chain and Ransomware. These new attacks target enterprise software and infrastructure by exploiting vulnerable business processes and logic flaws and exploiting the gaps between siloed security products and data. To counter these attacks, while also enabling security and compliance to operate at the speed of DevOps and business, organizations need to adopt a Zero Trust architecture, integrate security across the software development lifecycle, ensure the integrity of the supply chain, and automate manual error-prone processes.

Human Capital

Dev, Ops, and IT leaders face similar challenges in terms of the scarcity and high cost of top technical talent and the need to closely manage human capital. Today, forward-thinking leaders are investing in consolidation and automation initiatives to reduce tech stack complexity, eliminate manual processes, and recoup and re-deploy human capital to more strategic and productive uses. Adopting a DevSecOps approach is a good first step to enabling automation of typically manual processes like software testing, security assessments and vulnerability management.

Increasing Compliance Obligations

Enterprises today must be able to quickly adapt to new and evolving regulatory frameworks and an overall acceleration in the pace of business change. To keep up with this change, IT leaders need systems and solutions designed with native compliance and audit capabilities that enable continuous and automated policy enforcement and reporting.

prismo

Introducing Prismo Dev-Native Security

Prismo Dev-Native Security is a fundamentally new approach to securing enterprise applications, infrastructure, and data. Its unique architecture weaves security into the fabric of the software development lifecycle to provide complete end-to-end security and compliance automation for DevSecOps.

A Unified Open Security Platform

Prismo unifies many security functions currently spread across the disparate siloed point solutions that make up today's typical security stacks. It provides a single end-to-end solution for the protection of custom code, supply chain software, application workloads, and the management of user entitlements. Built on an open, scalable, purpose-built security data lake, its patented Transaction Graph architecture weaves siloed event data into powerful end-to-end transactions to provide a comprehensive, continuous, and automated approach to identification, prioritization, and mitigation of cyber risks.

End-to-End Automation

Prismo automates security functions across the SDLC from development to production. It provides automated "Build-over-Build" discovery of new code paths, generation and execution of new tests, and vulnerability management that's integrated with DevOps tools and ticketing systems for workflow and compliance management. The result is a streamlined development process with increased release velocity, improved quality, and reduced MTTR.

Secure from the Start and Protected in Production

Integration of security at every stage of the SDLC shifts security left, identifying and remediating vulnerabilities, bugs, and issues early to avoid the security and operational risks and exponentially higher costs of remediating in production. But Prismo also monitors and protects workloads in protection using "Protect until Patched" policies for new and zero-day vulnerabilities and detects and blocks application attacks that are only seen in production in real-time.

Continuous Verification and Compliance

Prismo leverages NIST, OWASP, MITRE, and other sources and frameworks to pinpoint vulnerabilities and assure compliance. Full OWASP coverage is provided out of the box, including Broken Access, Administration bugs, design issues, logic flaws, and Open-Source components that may not be actively maintained. Vulnerable code not flagged by Development tools is pinpointed by Prismo, reducing the time and effort required for remediation.

Built for Zero Trust

Built on Zero Trust principles, the platform enforces Zero Trust policies in real-time. Employing a Dynamic Risk Profile, a unified, continuous, event-driven assessment of risk measured across the entire IT environment, it provides rapid and early detection of low and slow, multistage threats like Solar Winds-style supply chain and advanced ransomware attacks. The platform meets and exceeds all NIST Zero Trust Architecture (ZTA) standards, providing a path and gateway for ZTA adoption.

prismo

Unified Security Platform for the Entire SDLC

Prismo Dev-Native Security Platform provides a unified, open, and integrated approach to security and compliance for custom code, supply chain software, and workloads across hybrid cloud environments. The platform is fully compliant with NIST 800-207 Zero Trust architecture.

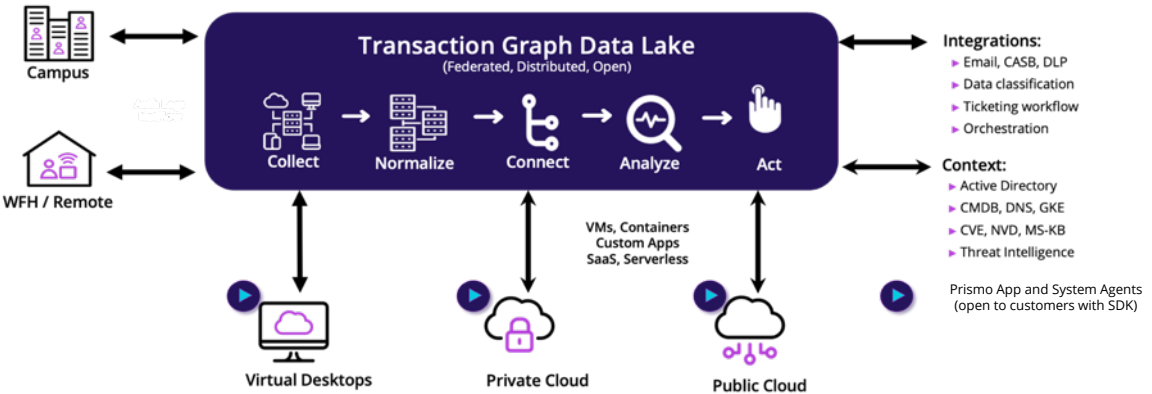

Figure 1. Prismo's Transaction Graph Data Lake supports on-prem, cloud, and hybrid environments

SINGLE PLATFORM

Secures Custom Code
- Production Applications
- Custom Extensions to IT Applications

Verifies Supply Chain
- 3rd party packages and tools
- Open-Source software

Protects Workloads
- VMs and Containers
- OS, Libraries, Drivers

OPEN AND INTEGRATED

Out-of-box Integrations
- CI/CD, ITSM, CMDB, IGA, IAM, Orchestration

Extensible Platform
- Sensors and probes
- APIs and SDKs (including Machine Learning modules)

360° VIEW OF RISK

Actively Manages Risk
- Continuous Assessment
- Contextual Prioritization
- Automated Actions

ML and Graph Analytics
- Anomaly detection
- Peer-Group Analysis and Clustering
- Prioritization, Recommendations etc.

End to End Automation for DevSecOps

Prismo automates security functions across the SDLC from development to deployment, securing custom developed code and ensuring the integrity of 3rd party and open-source software in the supply chain.

Automation for Custom Code

As enterprises adopt Agile and DevOps methodologies to support the development of production applications, legacy security and compliance solutions become an inhibitor to rapid development and innovation. Prismo Dev-Native Security solves this challenge by automating security functions:

- Discovers incremental Build-over-Build code paths and tags them with version, build, and regression run
- Automates generation and execution of security tests with no manual intervention
- Minimizes MTTR through precise pinpointing of vulnerabilities for developers and mitigates residual risk while a vulnerability is being remediated

Automation for Supply Chain Software

Open-Source software as well as that of established software vendors have been shown to be susceptible to backdoors and vulnerabilities making the enterprise vulnerable to supply chain and ransomware attacks. Prismo enables enterprises to ensure the integrity of the software supply chain by:

- Automatically build the execution profile of images that includes 3rd party applications, open source and OS
- Extract the security fingerprint and certify the image against industry standard frameworks CIS, MITRE and NIST
- Programmatically verifying that certified fingerprint is consistent between upgrades and patches, and in production

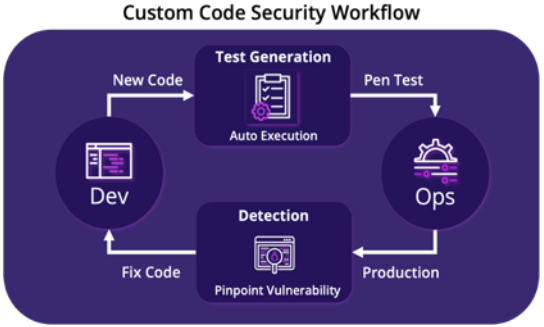

Figure 2. Prismo creates a continuous "build-over-build" security workflow

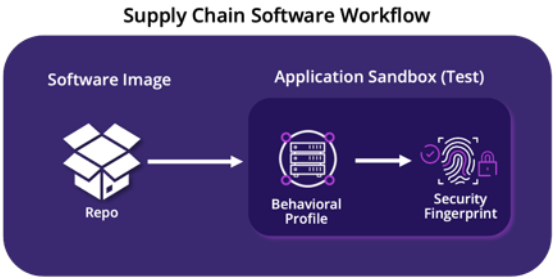

Figure 3. Prismo Application Sandbox fingerprints and certifies 3rd Party software

prismo

Secures the SDLC from Dev to Production

Prismo's Dev-Native Security Architecture is a comprehensive, automated, and risk-based approach to application security and vulnerability management. It provides a complete end-to-end DevSecOps workflow for identification, prioritization, and remediation of vulnerabilities, and continuous protection against zero-days and residual risk in production with no impact on application performance.

Precise and Comprehensive Identification of Vulnerabilities

Continuous "Build-over-Build" identification of new code paths enables speed, precision, and coverage

- **Precise identification** of vulnerable lines of code using data flow analysis speeds remediation and eliminates development time and effort to investigate false positives
- **Comprehensive coverage** of 100% of application code paths leveraging functional and regression tests against all classes and sub-types in OWASP

Contextual Prioritization and Risk-based Remediation

Use of runtime and environmental context prioritizes remediation efforts based on risk to the business

- **Automatically enriches** vulnerabilities with runtime and environmental context to prioritize
- **Recommends remediation workflow** to balance availability and security risks
- **Continuously verifies** systems and applications to test effectiveness of patch or remediation

Continuous Protection in Production

Protection policies and real-time attack detection and mitigation protect code in production

- **Creates and enforces policies** to protect applications from vulnerabilities until they have been remediated
- **Detects MITRE Tactics and Techniques** in real-time to prevent zero-day vulnerabilities from being exploited in production
- **Controls and certifies user access** based on roles and privileges to prevent excess privileges and unauthorized access

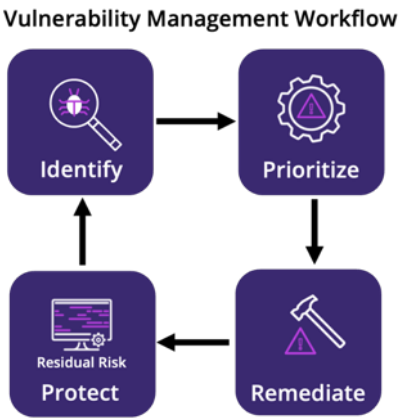

Figure 3. Prismo end-to-end workflow for automated vulnerability management

Why Dev-Native Security?

Prismo's Dev-Native Security Architecture is a game-changer for Dev, Ops, and Security teams that provides continuous 360° enterprise-wide risk visibility, automated policy-driven response and remediation, and compliance assurance for industry frameworks like NIST, MITRE, and OWASP. It's foundation of Zero-Trust principles coupled with its ability to weave security into the fabric of the SDLC make it ideally suited for digital-first organizations needing to protect online business operations.

Faster Release Velocity and Innovation

Weaving security and compliance into the fabric of the SDLC shifts security left to identify and remediate issues and vulnerabilities early and enables the automation of manual processes. The result is less human effort and errors, higher quality releases, and faster release and innovation cycles.

Risk-Centric Security and Compliance

By providing continuous enterprise-wide visibility of risk, Prismo enables prioritization of vulnerabilities and threats, automated real-time response and mitigation based on risk, and continuous, policy-driven compliance enforcement and reporting. With Prismo, organizations automate manual tasks and work associated with vulnerability management and audit and compliance reporting unlocking human capital that can be re-deployed to more productive work and strategic initiatives.

Cyber Resilience

The traditional approach to enterprise security was perimeter-based and prevention focused. As advanced threats began to bypass traditional security controls, the focus shifted to detection and response. Enterprises that want to compete and thrive in the digital economy must move beyond reactive detection and response approaches and embrace the design of Cyber Resilient systems and processes. The Prismo Platform enables this with:

- **Proactive early detection** and mitigation of active threats
- **Minimization of MTTR** for vulnerabilities
- **Reduction of RPO and RTO** by detecting and stopping advanced threats like ransomware and supply chain attacks early, before detonation, to avoid and minimize operational disruption and business impact.

Lower Total Cost of Ownership

Prismo's unified end-to-end approach and architecture enables significant reductions in total cost of ownership through:

- **Early Identification and remediation** of vulnerabilities and issues in the SDLC avoids up to 100X cost increase to remediate in production vs development.
- **Automation** of manual processes reduces the time and effort required for security testing, vulnerability management, and threat remediation and mitigation.
- **Consolidation** of the security stack by unifying tools such SAST/DAST/IAST/RASP, CWPP, CSPM, and CIEM under a single platform reduces stack complexity, human capital requirements, and license costs via the elimination of duplicative and unnecessary legacy tools.

About Prismo Systems

Prismo is the first security platform to connect fragmented data across silos, empowering enterprises to continuously expose blind spots, proactively reduce attack surface, automatically mitigate risk, and adhere to the NIST cybersecurity framework. With Prismo, enterprises transform the way they secure users, assets, and applications with an active risk-based approach that simplifies the security stack, streamlines operations, lowers costs, and dramatically reduces risk. Headquartered in Silicon Valley, Prismo is backed by Sequoia Capital. For more information, visit us at www.prismosystems.com and follow us on LinkedIn and Twitter.

prismo
Dev-Native Security

2350 Mission College Blvd, Ste 215
Santa Clara, CA 95054
650.417.5945
www.prismosystems.com