prismo

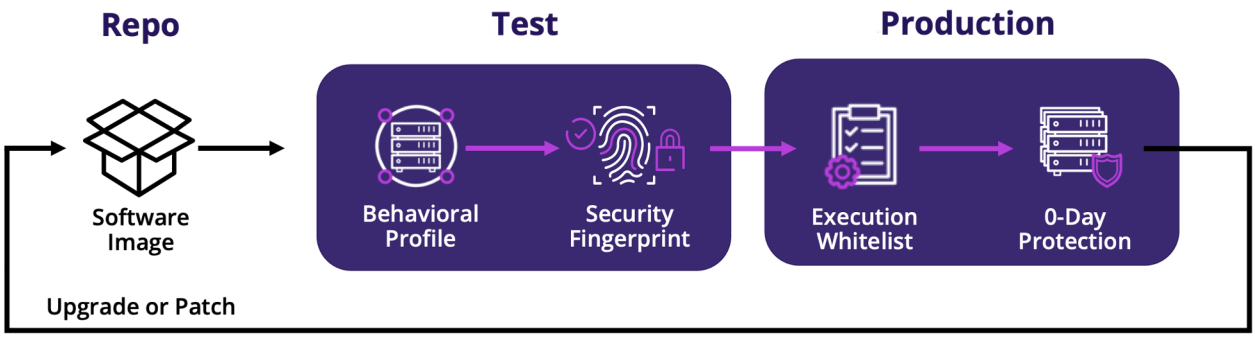
DATASHEET

Supply Chain Software Protection

Automate Protection for 3rd Party and Supply Chain Software

Prismo is the first unified solution for securing 3rd party and supply chain software across the entire lifecycle and automating manual software onboarding processes. Prismo's unique Supply Chain Sandbox automatically fingerprints, certifies, and whitelists software in Test and enforces certified images in Production. The result is reduced risk, continuous 100% compliance, and lower TCO from automation of software onboarding processes.

Prismo Supply Chain Sandbox certifies and verifies 3rd party software



FINGERPRINT

Fingerprint images against industry standard frameworks (CIS, MITRE, and NIST) using behavioral profiling

CERTIFY

Automatically build a whitelist of approved application security behaviors to onboard new software and updates

VERIFY

Protect against zero-days in production by verifying and enforcing fingerprints between upgrades and patches

Key Capabilities:

3rd Party Software Certification

Automatically fingerprints and certifies software in a sandbox and continuously verifies images in production

Lifecycle Workload Protection

Proactively protects workloads from zero-days across provisioning, operations, execution, and maintenance

Automated Vulnerability Management

Identifies, prioritizes, remediates, and manages the risk of unpatched vulnerabilities in production

Relational S-BOM

Quickly assess exposure and impact of new CVEs across enterprise from inventory, dependency and usage

Key Benefits:

Minimize Supply Chain Risk

Mitigate risk of backdoors and zero-day threats from open-source and commercial software

Rapid Software Onboarding

Onboard new software and updates in minutes instead of months by automating manual processes

Protection in Production

Proactively protect workloads against known and zero-day threats, and run-time attacks in production

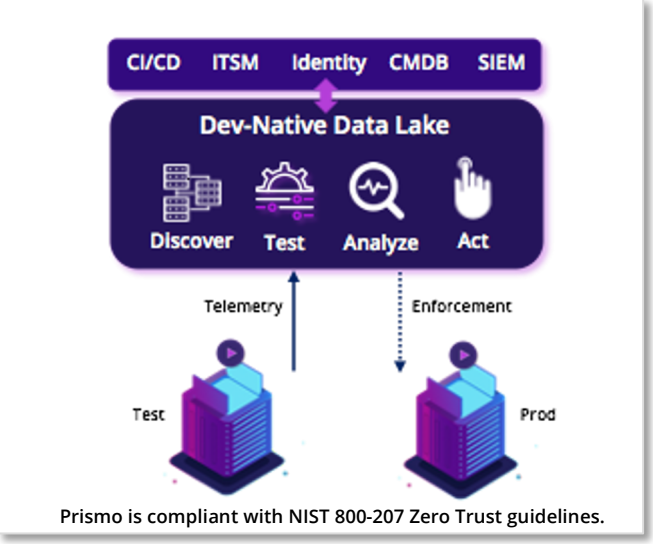
Lower TCO

Automate manual testing and certification processes to improve efficiency, accuracy, and TCO

Comprehensive Protection for Supply Chain Software

Prismo is a comprehensive unified solution for securing 3rd party and supply chain software. Its unique Supply Chain Sandbox automatically fingerprints, certifies, and whitelists software in Test and and continuously verifies images in production, automating manual software onboarding processes. Its unique Relational Software Bill of Materials (SBOM) provides a continuous assessment of the exposure and impact of new CVEs across the enterprise from inventory, dependency, and usage.

The Prismo Platform is NIST 800-207 Zero Trust compliant, providing proactive full-lifecycle workload protection from zero-days across provisioning, operations, execution, maintenance stages. Automated vulnerability management identifies, prioritizes, remediates, and manages the risk of unpatched vulnerabilities in production.



Prismo is compliant with NIST 800-207 Zero Trust guidelines.

SANDBOX SUPPORT

- **Operating Systems:**
  - **Linux:** RHEL, CentOS, Ubuntu, Debian, Oracle, AWS, GCOS, SUSE, SLES, SELinux, Scientific
  - **Windows Server:** 2016, 2019
  - **Windows Desktop:** 7, 10, 11
  - **Container:** Docker, LXC, CRI, containerd, Windows, Mesos

INTEGRATIONS

- **ITSM, SIEM, CMDB**: ServiceNow, Splunk
- **CI/CD:** Extensive including Jenkins, Azure DevOps, Git, Jira, Maven
- **Identity:** Various SSO, AD, VPN, IGA
- **Extensible:** Open APIs
- **Programmable**: Machine Learning SDK, Policy and Query APIs

DATA LAKE DEPLOYMENT

- **Private Cloud**: Containerized
- **Public Cloud**: AWS, Azure, GCP
- **SaaS**: Dev and Test Use Cases
- **Cluster Requirements**: 3 VMs:
  - 16 vCPUs
  - 96GB RAM
  - 500GB Disk

Compliance Standards

- NIST, MITRE, CMMC, COBIT, SANS, GDPR, PCI

Supply Chain Certificate

- Multi-Tier Hierarchical Application Topology
- Vulnerabilities and CIS Compliance
- Runtime Execution Graph inclusive of APIs
- MITRE Tactics TA01 through TA10, TA40
- Domains Accessed: Inbound and Outbound
- Ports Open: Active and Dormant
- Installation Services: Push, Pull, Self-update
- Service Accounts: Local and Network
- Directory, File and Registry access
- User Access at System and Application

Relational Composition Analysis

- Software-BOM includes application, 3rd party packages, open source, OS and system utilities
- Software dependency matrix and usage metrics
- Vulnerability risk and license compliance

Workload Protection

- Real-time enforcement of application fingerprint using programmatic whitelist from Test
- Zero-Touch Application Control and 360º Micro-Segmentation
- Blocks exploit of unpatched or 0-Day vulnerabilities and supply chain backdoors

prismo

2350 Mission College Blvd
Santa Clara, CA 95054
info@prismosystems.com

About Prismo

Prismo secures the software that powers modern enterprises. The Prismo Platform secures software development across the entire SDLC and deployment on any cloud or on-premises infrastructure. Prismo's Dev-Native approach enables dev, ops, and security teams to simplify, automate, and scale protection of both custom applications and supply chain software, accelerating release velocity, increasing software quality, closing coverage gaps and blind spots, and lowering total cost of ownership. Based in Santa Clara, Ca, Prismo is backed by Sequoia Capital.