prismo™

Solution Brief

Application and API Security

Securing Modern Applications and APIs

As Microsoft CEO Satya Nadella says, "all companies are now software companies." Enterprises across all industries are embracing this new reality, as software and APIs are increasingly the primary drivers of business innovation, competitiveness, and growth. The vast majority of data breaches, however, start with the exploits of applications and operating systems from 3rd parties and APIs. With modern SaaS applications often synonymous with the brand, securing enterprise applications and APIs is critical to protecting brand reputation and developing a comprehensive cyber risk management strategy.

Modern applications and infrastructure are hard to secure, however. The advent of DevOps and CI/CD methodologies, containers, cloud-native and hybrid infrastructures, and microservice architectures has exposed the limitations of traditional endpoint, network, and application security solutions and demonstrated the need to detect and block exploits at all layers to effectively prevent breaches and protect brand reputation.

Challenges with exploits in Enterprise applications:

- **Expanding Attack Surface.** Exploits are usually the first stage for entry of malware, RAT tools, and threat actors and WFH, BYOD, IOT, cloud-based and hybrid environments all contribute to a rapidly expanding attack surface.
- **3rd party risk is growing** and regulations now require enterprises to ensure the integrity of the entire supply chain.
- **Web Application Firewalls (WAFs) offer limited protection.** WAFs are rule-based, need constant tuning to reduce false positives, are prone to evasion and lack context, and are often configured to block just base cases due to false positives.
- **DAST.** Enterprises sill face significant challenges with application testing due to manual, imprecise, and incomplete DAST processes and tools that only look at the application entry points
- **No solution for some attacks.** There's no solution for exploits such as insecure deserialization, SQL stored procedures and XML entity attacks. Similarly, there is no good solution for many other exploits in the OWASP Top 10 such as Broken Access Control, Parameter Tampering etc.

Prismo provides a comprehensive infrastructure agnostic solution for securing all enterprise applications and APIs.

KEY CHALLENGES:

- Expanding Attack Surface
- Zero Day Vulnerabilities
- 3rd Party - Supply Chain Risk
- Open Source Risk
- Integration with CI/CD
- Increasing Regulation
- Ineffective Legacy Solutions
- No Solution for Some Attacks

Prismo Detects and Blocks at Application Execution Points:

Detect and Block Exploitation of both Known and Zero-Day Vulnerabilities. Works at the application (home grown, 3rd party, open source code or plugin), API, OS and Hypervisor layers.

Comprehensive OWASP Coverage Provides full coverage of OWASP Top10 and more by integrating behavioral and ML-based anomaly detection.

Massively Scalable Architecture With Prismo, detection and enforcement are fully distributed at the application edge for maximum scalability.

Precise High Fidelity Detection and Blocking. Complete coverage of known and zero day exploits with zero false positives or negatives.

Full Kill Chain Protection Protection encompasses the full Kill Chain (all MITRE Tactics) from vulnerability exploit to malware to threat actor.

Simple Streamlined Operation With Prismo there's no rules to configure or manage and no detection algorithms to fine tune

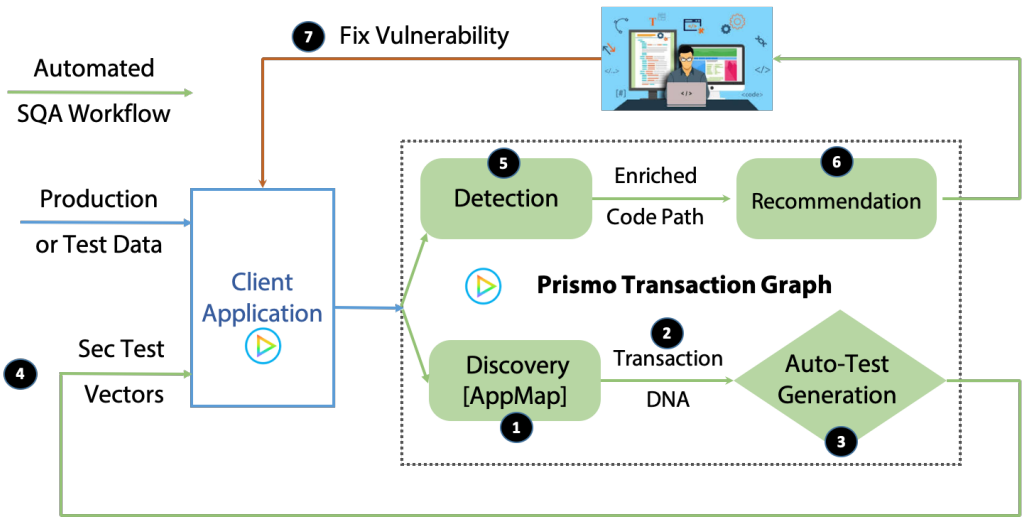
prismo™

Solution Brief

Comprehensive and Automated Pen-test Process

1. **All application entry points cataloged**
   - URLs, APIs…
2. **Entry point parameters that pass-through to exit points identified**
   - Relationship from entry point keys to exit point keys built
3. **Types of exit points discovered**
   - SQL, System, Network, REST…
4. **Automatic test vectors generated per OWASP exploit**
   - SQL, OS Command, SSRF, XSS, Deserialization, RCE, WebShells, LFI/RFI…
5. **Vulnerable code paths identified**
   - Incident is raised; Transaction traced with one-click
6. **Identified vulnerability is contextually enriched with metadata**
   - Developer knows where and how to fix vulnerabilities
7. **Single workflow from Pen-test to Testing to Staging to Production**
   - Continuous feedback loop

Prismo - A single tool for your entire DevOps pipeline



DevSecOps: Continuous Protection and Improvement

Prismo Benefits:

Reduce Risk

- Comprehensive code coverage
- Zero-day protection in production
- Every exercised code path secured - human error eliminated
- 3rd party risk eliminated by ensuring the integrity of the supply chain

Reduce Cost

- Automated test generation and validation
- Substantial savings in time, people, tools
- Actionable alerts pin-point the exact lines of vulnerable code
- Single tool across the entire DevOps Pipeline

Increase Profits

- Faster time to revenue
- Agile development, instant assurance/certification
- Leverage open source and partner plugins

Prismo Advantages:

Fast Adoption
No application code change required and minimal performance overhead.

Protects all applications from legacy monoliths to cloud-native and microservices based architectures, on any OS and any infrastructure.

Automatic discovery of app topology at runtime with correlation of input parameters to the place where they are used in the backend (SQL, Socket, System Call etc).

Operational Simplicity
No rules to configure or manage and no detection algorithms to fine tune.

Full DevOps and CI/CD Integration
Fix vulnerabilities early in test/staging in addition to production

Massive Scalability
Detection and enforcement are fully distributed at the application edge for maximum scalability

For more information or to schedule a demo, please contact us at:

Prismo Systems Inc.
2350 Mission College Blvd, Suite 215
Santa Clara, CA 95054

www.prismosystems.com

info@prismosystems.com