prismo™

Platform Overview

Active Cyber Risk Management

Build a Unified Active Cyber Risk Program with Prismo

Powerful Risk Management • Insightful Analytics • Proactive Threat Handling

The gap between risk and response widens day by day. As environments increase in complexity, silos and blind spots ramp exponentially. Lacking systematic ways to detect and prevent risks from escalating to threats, security teams focus on efficient threat response. As threats evolve in sophistication and volume however, the focus must move to proactive and efficient risk handling.

The vast majority of enterprise risk is composed of two kinds of risk, Inherent Risk and Imminent Risk. Inherent Risks are created by factors such as missing controls and configuration drift, while Imminent Risks largely stem from vulnerabilities present in the environment. As both risk types escalate , proactive handling is required to preempt threats.

Prismo is the first Cyber Risk Management platform that continuously exposes security blind spots, thoroughly minimizes attack surface, and actively handles risks and threats. Prismo provides comprehensive active risk management across the entire organization including users, assets, and software (applications and codebases). Prismo's automation and efficiencies provide overworked security teams with the breathing room to actively manage risks across the spectrum of Workforce, Workloads and Workflows:

Workforce Risk Management

The solution is designed for the borderless workforce consisting of remote workers, BYOD devices and temporary workers. Prismo provides a security overlay for all flavors of VDI deployments. The unique approach provides administrators with end-to-end visibility, fine-grained controls needed to enforce user access to data, detection of VDI specific attacks, and unique insights into user behavior that are not available from the VDI implementation.

Workload Risk Management

The solution is designed to comprehensively protect the integrity of workloads across the entire lifecycle of Provisioning, Execution, Operations and Maintenance. Prismo blocks Malware before install, fingerprints the software supply chain to protect against backdoors, enforces transactional chain-of-trust to stop lateral movement, and provides a single source of truth for replay and rollback.

Workflow Risk Management

The solution is designed to secure applications and APIs deployed in private data centers or newer cloud-native and container-based microservices. Prismo automates the DAST process, pinpoints the line of code to remediate vulnerabilities early in design, and blocks OWASP application and API exploits in production. The implementation is woven into the fabric of Enterprise DevOps and CI/CD pipelines.

Highlights

Active Risk Management
Assess, Control, Contain And Assure Workforce, Workloads and Workflows

Transactional Data Lake
Infrastructure agnostic platform with Open APIs

Single Source of Truth
Provides complete audit trail and assurance for all interactions for 3-5 years

User Behavior Analysis (UBA)
Provides rich insights into user behavior that are not available from the VDI implementation

Workforce: Borderless Enterprise
- End-to-end visibility
- Fine-grained control for data access
- User Behavior

Workloads: Lifecycle Integrity
- Blocks malware before install
- Ensures integrity of enterprise software supply chain
- Stops lateral movement
- Replay and rollback servers

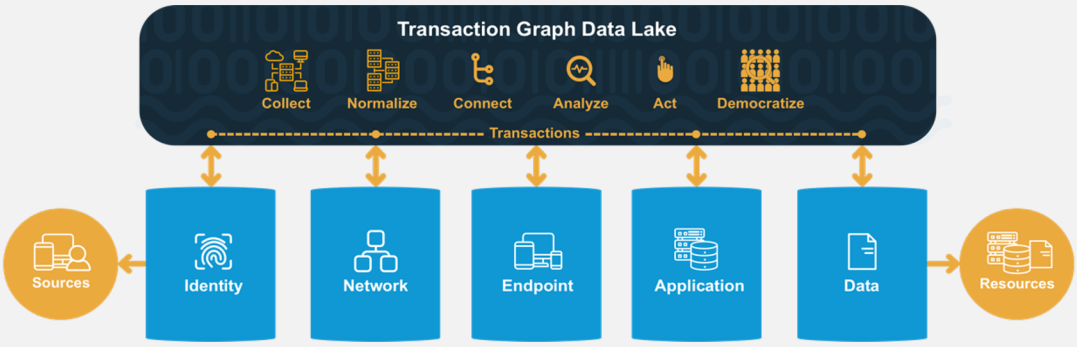
Workflows: Secure by Design
- Application and API Security
- DAST Automation
- OWASP coverage
- Woven into DevOps and CI/CD

prismo™

Platform Overview

Prismo transforms siloed security data into powerful end-to-end transactions

Prismo's transactional data model and data lake fundamentally transform the collection, analysis, and storage of security telemetry providing enterprises with unprecedented visibility, accuracy, and control to reduce costs, increase operational efficiency, and enable true risk-centric governance.



The Prismo Transaction Graph™ data lake weaves siloed event data into powerful end-to-end transactions.

Unique Capabilities

Powered by Prismo's Transaction Graph Security Data Lake, Prismo is the first security platform to provide actionable and automated cyber risk management at enterprise scale. Unlike inaccurate and inefficient SIEMS and static GRC approaches, Prismo provides a comprehensive, active, and automated approach to detecting, assessing, and mitigating enterprise cyber risk.

In real time, Prismo diagnoses the issue and takes the appropriate automated response in real time:

Controls Inherent Risks: Inherent risks are caused by configuration drift, manual error, and missing controls such as privilege consistency across network hops. In addition to enforcing the overall integrity of servers, workloads, and software development, Prismo proactively creates intent-based policies to prevent existing risks from being exploited.

Contains Imminent Risks: Imminent risks arise from vulnerabilities in the environment such as known software exploits. Prismo proactively creates intent-based policies that provide "protect until patched" flexibility.

Stops Threats Early: Prismo actively blocks malicious behavior, stopping risks being actively exploited (e.g. installation of malware) or triggering (e.g. ransomware attempting to encrypt files) at the earliest stages of an attack.

In contrast to static, alert-centric security approaches, the Prismo platform provides:

Consistent View of Risk

Risk is assessed across users, assets, and software, evaluated against NIST, MITRE, and OWASP frameworks, and ranked to prioritize action across the entire enterprise.

Comprehensive Coverage

Infrastructure agnostic with sensors for all platforms, (including subsystems such as VDI.) Open full-stack APIs ensure seamless integration into any environment creating a single source of truth with transaction level playback for audits available for 3-5 years.

Continuous Assessment

Maintains a continuous history of risks, compliance metrics, and automated responses in near real-time across even the largest distributed environments. What-if and scenario simulations predict the effects of proposed policy changes to maximize intent accuracy and relevancy.

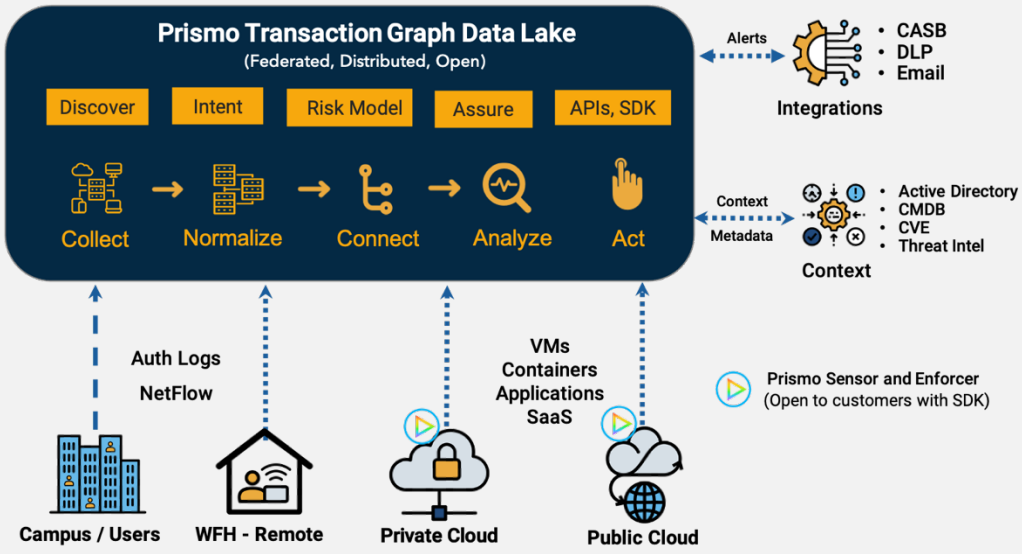
Actionable Insights

Proactively mitigates Inherent and Imminent risks by automatically pushing intent-based policies and blocking risks in real time when they are triggering into threats.

prismo™

Platform Overview

How it works



A Cloud-native, Real-time Risk Platform:

- **Discover:** Gathers rich telemetry data from multiple sources
- **Transaction:** Weaves events into a Transaction, adds Context, and normalizes into a Chain-of-Trust
- **Risk Model**: Leverages Chain-of-Trust analytics to identify Imminent and Inherent Risks in real time and provide an automated response
- **Intent:** Intent-based policies minimize Inherent Risk and flex along with environment
- **Assure:** Displays rolling Compliance risk assessment in Dashboard
- **APIs, SDK:** Integrates with enterprise offerings and can be embedded into custom applications

Building the Transactional Chain-of-Trust

To enable robust threat analytics, a Transaction is first transformed into a Transactional Chain-of-Trust using:

Enrichment: Each step of the transaction is enriched with context including:

- **Identity:** Identity of the end user and administrator even across network hops.
- **Provenance:** Validity of Origin (e.g. golden master), provider (e.g. sanctioned service account), and more.
- **Logs:** Security information from each silo such as Firewall logs.

Validation: Prismo validates the context for each step resulting in a Transactional Chain-of-Trust that provides a definitive answer to the questions of "Who, What, Why, When, How?" for every aspect of the Transaction.

Storage: Each Transactional Chain-of-Trust is stored in the Data Lake.

Risk Management Workflow with Chain-of-Trust

The Risk Management Workflow evaluates highly complex, multistep transactions as sanctioned or suspicious and mitigates automatically:

Deep Analysis: Each new transaction is scrutinized with deep behavioral and anomaly detecting analytics (including NIST and MITRE frameworks) for deviation from the Transactional Chain-of-Trust.

Active Mitigation: For detected risks, the Risk Management Workflow provides automated risk mitigation and efficient handling in real time:

- **Proactive Control:** For inherent risks such as a known vulnerability, a policy automatically is created and pushed to protect against an exploit.
- **Automated Containment:** For imminent risks such as malware that is triggering, the malicious behavior is blocked automatically.
- **Efficient Handling:** All risks are ranked by severity and long-term mitigation (such as blacklist) can be selected with a single click.

Platform Benefits

Secure Complex Processes
Prismo uniquely secures complex processes end to end

Preempt Inherent Risks
Automated policies (such as "protect until patched") control inherent risks

Deliver "Zero Click" Containment
Imminent risks are contained (blocked) automatically in real time

Rank Risk Globally
Global risk ranking helps prioritize the threats that need immediate attention

Assess Compliance in Real Time
Rolling metrics transform compliance from static into a live assessment

Maximize Team Productivity
Role-specific workflows maximize productivity across the security team

Prismo Risk Management Workflow

Prismo provides comprehensive active risk management across the entire organization including users, assets, and software (applications and codebases). Interactive dashboards provide real-time actionable insights and active controls tailored to role. The risk management workflow follows the lifecycle of Assess, Control, Contain and Assure. While many responses are automated, the workflow provides extensive analysis and customization capabilities. Security teams can analyze, play back, and explore the data. Further, customized policies and exceptions such as whitelisting are fully enabled by the workflow.

Assess

- **Continuously assesses Inherent and Imminent risks** through the comprehensive discovery of users, devices, applications, and data and the transactional interactions between them.
- **Connects, aggregates, and normalizes fragmented data** in enterprise silos across heterogeneous domains for discovered entities and transactions.
- **Enriches sources and resources at both ends of the transaction** with enterprise specific context from AD, DNS and CMDB making all data interpretable and insights actionable.
- **Provides a clear security roadmap** to minimize attack surface based on prioritized Inherent risks. Imminent risks are triaged as Alarms, Alerts and Advisories for immediate response to active threats.

Control

- **Provides real-time preventive controls** including proactive threat blocking (e.g. attempt to install malware) and proactive threat prevention (e.g. policy to “bubble wrap” exploit until patched).
- **Enables provisioning just-enough privileges for extended workforce** to access data with intuitive Intent-based policies.
- **Ensures Lifecycle Integrity of Servers and Workloads** with sanctioned provisioning, fingerprinted operations, cross-scope micro segmentation and least privilege assignment for administrators.
- **Eliminates configuration errors and drift** with advanced “outlier” behavioral and excess privilege analysis inputs to What-If and Dry-Run recommendation engine.

Contain

- **Helps contain Imminent Risk using precise transaction tracing** and innovations like chain-of-trust, entity risk profile, and ML-toolkit.
- **Detects low and slow threats** immediately after perimeter intrusion by amplifying weak signals (MITRE tactics and techniques.)
- **Eliminates dwell time and slashes false positives** by auto-mapping signals to the kill chain
- **Enables 1-click response for analysts** with tools to support Alert Validation, Root-Cause, and Impact Analysis and supports automated actions without requiring runbooks.

Assure

- **Maps all controls to NIST** Core (800-171 and 800-53) and risk to NISTIR 8286. Risk mapping to other compliance standards (PCI, SOX, CMMC, ISO etc.) is also available.
- **Risk Registry integrates with ticketing systems** and provides real-time status of Alarms and Alerts to help organizations stay on top of Imminent Risk.
- **Transactional data lake provides detailed 3-5-year audit trail** that can be replayed or queried for compliance.
- **Role-based dashboards and reports** summarize risk for C-Suite, Architect, Analyst, and other roles.

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 Systems Inc. | 2350 Mission College Blvd, Suite 215, Santa Clara, CA 95054 | info@prismosystems.com | www.prismosystems.com

© Copyright 2021 Prismo Systems. All Rights Reserved