prismo™

Solutions Brief

Security Excellence

Enterprise Security Challenges

- Enterprise IT is in the midst of massive transformation with the addition of public cloud services, ephemeral resources and custom applications in distributed deployments. Work-from-home, mobility, BYOD and edge computing are fundamentally changing enterprise access. Cloud and mobility reduce visibility, exposing a much broader attack surface. Growing reliance on contractors, partners and other 3rd parties creates a new risk vector.
- Functional security silos are not aligned with enterprise governance models. The complexity of integrating these security tools results in blind spots, misconfigurations and lax privileges. Siloed security misses key connecting events, reports false positives and increases cost.
- Application complexity is growing with monolithic applications being modularized into microservices. These ephemeral microservices have lifespans in the order of seconds. Securing them requires event-driven discovery, dynamic policy and instantaneous learning of behaviors.
- New data protection and privacy regulations are emerging in response to digital enterprises capturing personal information. The growing sophistication of actors and complexity of threats increases risk to enterprise data and intellectual property. There is a severe shortage of technical security staff to deal with these challenges.

We need a new approach

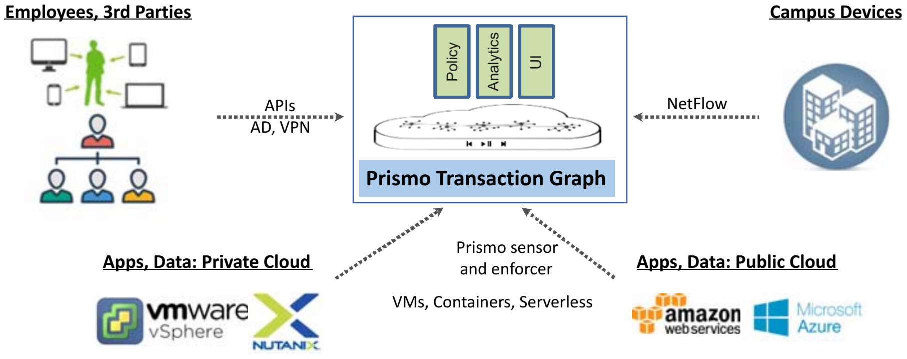
Prismo stops breaches right where they start

Prismo has developed an industry-first, patented software that provides end-to-end security and breaks the functional silos. Prismo uniquely connects all enterprise events to provide complete visibility across all layers of the IT stack: User, Network, System, Application and Data.

Introducing the Prismo Transaction Graph™

Transaction Graph links events into an end-to-end transaction, from an access request to the final response. Related transactions are further connected to form a graph. With transaction graphs, formerly challenging security use cases become trivial to solve. Our platform seamlessly integrates Identity Access Management, Privileged Access Management, Micro-Segmentation, Application Security including Assessment, Insider Threat, Vulnerability Management, SOC Automation, Threat Hunting and Cyber Risk Management.

The Prismo Platform



Key Challenges

- Ephemeral cloud resources
- Work-from-home, BYOD
- Functional security silos
- 3rd party risk
- Blind spots
- Application complexity
- Threat sophistication
- Skills shortage

Key Benefits

- End-to-end security
- Complete visibility
- Just-Enough Privileges
- 100M transactions/sec
- Multi-year history
- Ease-of-use
- Simplified security stack
- 75% reduction in spend

Transaction Graph implements the NIST functions to achieve security excellence: Continuous Risk Model powered by Event-driven Discovery, Intent-based Policy, Real-time Enforcement, Detection of MITRE Tactics and Techniques, Automated Response and Remediation with a feedback loop to reduce the attack surface.

prismo™

Security Excellence

Unlike other products that operate on individual events, Prismo Transaction Graph precisely links events into transactions to piece together the complete picture of every request. By constructing and storing entire transactions indefinitely, Prismo cuts across silos to provide the missing pieces of the puzzle to fill security knowledge gaps. Blind spots are thereby eliminated.

Transaction Graph offers a better approach to authorization: "Just-Enough Privileges". Users don't get complete access to all resources, they only get access to the right resources in the right context to get their job done. Just-Enough Privileges is preventive and shifts the focus away from chasing false alerts. Reliance on reactive detection technologies and human SOCs is reduced.

Transaction Graph enforces security for every request. The product is battle tested in large F500 implementations and proven to scale to over 100M transactions/sec while adding less than 2% overhead. It provides a multi-year history that can be queried in real-time.

Transaction Graph is easy-to-use. User intent is automatically translated into fine-grained access control, eliminating human error. Armed with the power of enriched and connected data,Transaction Graph greatly simplifies the enterprise security stack. IT spend is cut by 75%.

Customer Benefits

Transaction Graph solves the 5 biggest security challenges:

1. Attackers cannot propagate laterally. Transactional chain-of-trust prevents use of stolen admin credentials.

2. Users and APIs cannot exploit application vulnerabilities. Application security logic is validated for misconfigurations and authorization errors.

3. Malware is blocked early at install time. Only fingerprinted accounts can install packages and executables.

4. Insiders cannot exfiltrate data or intellectual property. They have "Just-Enough Privileges".

5. Audit and compliance is effortless. Prismo records every access to enterprise resources.

Transaction Graph unlocks enormous business value and gives peace of mind to various stakeholders: Board, Regulators, Employees, Business Units, IT and Customers

- Board, internal audit and external regulators gain transparency from precise and comprehensive transactional visibility. Responding to stakeholder expectations is just a click away.

- Employees can be productive and can work from literally anywhere, using the device of their choice. Contractors can be added confidently. Enterprise security posture is not diminished.

- Business Units can rapidly innovate and deliver new cloud-native applications using open source code. Their customer-facing platforms can safely extend to include customer and partner plug-ins.

- IT can flex seamlessly to scale on demand or reduce spend when appropriate. On-premise and hybrid-cloud deployments are equally secure.

- Customers can be assured that their data is safe and secure. Enterprises can use this competitive advantage to build brand loyalty.

Prismo's Transaction Graph enables Granular Discovery, Identity & Access Management, Privilege Access Management, Micro Segmentation, RASP, Automated Penetration Testing, Cyber Risk Management

prismo™

Security Excellence

Use Case	Prismo Unique Capabilities	Realized Business Value
Just-Enough Privileges (includes IAM, PAM and Micro-Segmentation)	Intent-based policies powered by what-if, dry-run and recommendation engines implifies granular segmentation. New controls for work-from-home users, software installations and updates.	With only four intent rules, gaming vendor granularly segmented VPN access for 1K users and 500 VMs after Covid. Provenance control blocked malware at install. Vulnerability control mitigated security exposure until patched.
Customer-facing Applications (RASP with integrated Assessment)	Comprehensive OWASP protection including 0-days. Pin-point vulnerable line of code. Continuous application assessment using code flow analysis. Runtime protection for ephemeral containers including dynamic policy and instantaneous anomaly detection.	F100 SaaS provider safeguards brand which is synonymous with application. Faster time to revenue with safe use of open source and integrating security early into DevOps life-cycle. Significant cost savings in people, tools and time.
Insider Threat (Lateral Movement and Privilege Escalation)	DNA profile and entity risk model amplify low-and-slow attacks. Early warning for every step in MITRE. Transactional audit trail & 3+ year history.	#1 energy services provider has complete Insider traceability to detect intellectual property theft. Reduced 'Dwell Time' from months to minutes.
Discovery and Risk	Compare configuration with activity to uncover blind spots. Seamless insertion into existing networks. Real-time CXO risk dashboard and risk over time	Top 10 SI offers cloud migration and cost reduction service. Compliance for 3rd party risk in banking and supply-chain risk in secure manufacturing.

About Prismo Systems

Prismo Systems is changing how security is applied to the new Enterprise IT architecture. The Prismo Systems approach, developed by some of the industry's premier technologists, unlocks unprecedented capabilities for the Enterprise to discover, protect, detect and respond to the most sophisticated threats. Prismo Systems backed by Sequoia Capital.

Transaction Graph Yields Better Results @ Lower Cost

Eliminate Blind Spots
Any-to-Any interactions provide full visibility across the enterprise.

Slash False Positives
End-to-End transactions record precise causation not correlation.

Minimize Dwell Time
Authentication & Authorization on every Request blocks at Entry point.

Reduce CAPEX and OPEX
Converge the stack and automate operations to lower costs.

Comply per NIST4
Elevate to NIST4 "Adaptive" compliance.

Assure with Confidence
Obtain evidentiary proof from the data lake's 3-year storage.

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

Contact: info@prismosystems.com
www.prismosystems.com

Copyright 2020 Prismo Systems All Rights Reserved