prismo

SOLUTION BRIEF

Operationalizing NIST Zero Trust Architecture

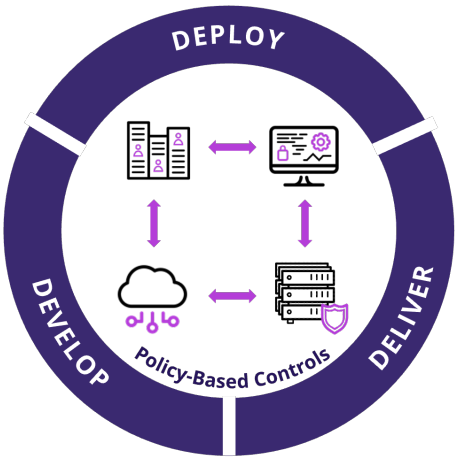
The Need to Move Beyond Perimeter Trust-based Security

As organizations embrace cloud platforms and technologies, adopt increasingly flexible remote and Work from Home (WFH) policies, and integrate temporary workers, suppliers, and partners into business-critical workflows, the concept of a well-defended security perimeter has become obsolete. Attackers have exploited these changes with advanced attacks such as Solar Winds-style supply chain attacks, impersonation of trusted employees, and compromise of mobile and IOT devices to gain entry to the enterprise network. Similarly, identity-based and device attacks now make typical one-time authentication per session or per connection inadequate. This fundamentally changes how organizations must approach security design as subjects, assets, and resources within the enterprise cannot be implicitly trusted, even after user authentication.

NIST Zero Trust - A New Standard for Security Architecture

Since 2014, the NIST Cybersecurity Framework has become the standard by which many organizations globally measure their security programs. In August 2020, NIST released SP 800-207, evangelizing NIST Zero Trust as its recommended security architecture. In contrast to traditional perimeter-based security "Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource."* Consequently, there is no implicit trust, and all interactions must be verified.**

Prismo Zero Trust Model



HIGHLIGHTS

Built for Zero Trust
Prismo delivers functionality that exceeds NIST Zero Trust guidelines out of the box

True Continuous Protection
Prismo continuously validates Resources in real time based on a Dynamic Risk Profile

Policy-based Controls
Flexible policies control Inherent Risks such as software vulnerabilities

Automated Containment
Imminent Risks such as malware installation are contained automatically

Prismo Operationalizes NIST Requirements for Zero Trust

Prismo is the first Cyber Risk Management platform that continuously exposes security blind spots, thoroughly minimizes attack surface, and actively contains threats. Prismo is cloud-native, works in real-time across all platforms including hybrid cloud environments, and meets or exceeds NIST reference architecture and guideline recommendations by providing:

- **Continuous Authorization** for all Subjects, Assets, Resources and all communications
- **Dynamic Risk Profiling** across the entire environment for all subjects and resources
- **Real-time Response** including proactive mitigations based on granular, current risk assessments

* NIST SP 800-207, Aug. 2020, https://doi.org/10.6028/NIST.SP.800-207

** https://csrc.nist.gov/CSRC/media/Presentations/zero-trust-networks-brief/images-media/2-4Kerman - Zero Trust Architecture - NCCoE - 2019 - ISPAB.pdf

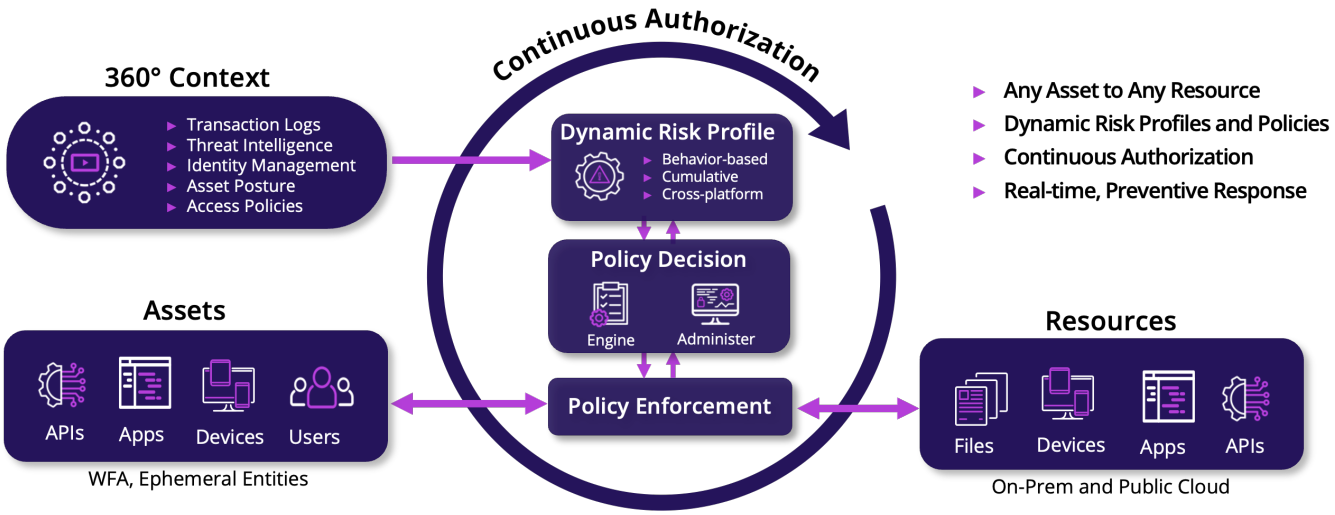
prismo

SOLUTION BRIEF

The Prismo Platform - Real-time, Zero Trust Architecture

The Prismo platform enforces Zero Trust principles in real-time. Users, devices, applications and APIs are treated as Assets, and files / objects, applications, devices, and APIs – whether intermediate or end target – are secured and authorized. Authorization is continuous rather than once per session or connection and based on Prismo's Dynamic Risk Profile - a unified, continuous, event-driven assessment of risk measured across the entire IT environment. This unique capability enables rapid, early detection of long-term, subtle, multistage attacks (such as Supply Chain) based on a high cumulative risk score, with Resources targeted by multiple low impact attacks prioritized for attention.

Prismo Zero Trust Architecture



Dynamic Risk Profile: The Dynamic Risk Profile is a real-time score of the risk of that Asset or Resource. A rich set of data is analyzed to construct a 360° view of the imminent and inherent risk that is impacting or potentially could affect that Asset or Resource. The profile is leveraged by the Policy Decision Point. The profile is:

- **Behavior-based:** Utilizes behavior observed by Prismo such as within and across sessions for end users.
- **Cumulative:** Accumulates risk over time and across sessions.
- **Cross-platform:** Aggregates across platforms, across subsystems (such as VDI), and across locations.

Policy Decision Point (PDP): A PDP consists of a Policy Engine and a Policy Administrator. The Policy Engine interprets intent-based policies that are managed by the Policy Administrator and determines a response to a high-risk score. Policies are either defined automatically by Prismo to guard against inherent risk such as a known vulnerability or by the Security Analyst to specify a desired response to a Risk. For a high-risk score, the PDP specifies an active response.

Policy Enforcement Points (PEPs): PEPs enforce the decision made by the PDP. For example, the decision can be to proactively block malware from installation (Imminent Risk) or to enforce a policy to protect against a vulnerability (Inherent Risk).

prismo

SOLUTION BRIEF

Prismo Meets and Exceeds NIST Zero Trust Guidelines

NIST has specified seven core architectural design principles. The Prismo Platform meets or exceeds all NIST reference architecture and guideline recommendations as summarized in the table below.*

NIST Guideline *	Prismo Capabilities vs Guideline
1. All data sources and computing services are considered resources.	✓ **Exceeds** **Discovers and monitors** computing services such as VMs, Containers, running Windows or Linux, on-premises or in the public cloud. **Catalogs both applications and data** and tracks access to data in file shares, custom applications and SaaS applications.
2. All communication is secured regardless of network location.	✓ **Exceeds** **Continuous authentication and authorization** for all communications – inside or outside the organization. **Authenticates and authorizes communications** between Users, Devices, Applications, APIs and Data Objects, located on-premises and in the cloud.
3. Access to individual enterprise resources is granted on a per-session basis.	✓ **Exceeds:** **Scrutinizes each resource request with deep analytics** by enabling least-privilege authorizations and providing time-limited authorizations.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application / service, and the requesting asset	✓ **Exceeds** **Access to resources is granted or denied in real-time** based on risk profile of every Entity using both intrinsic attributes (group, role, importance, vulnerabilities etc.) and runtime attributes (location, time, risk posture etc.). **Enhances observed behavior with rich context** from multiple sources including; provenance of files, sanctioned service accounts, and more **Fingerprints complex tasks end-to-end,** and grants or denies access in real-time.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.	✓ **Exceeds** **Analyzes each asset with deep analytics** to prevent impersonation by a hostile user or device. **Provides "Protect until Patch" capabilities** for assets with known vulnerabilities until a patch can be applied **Fingerprints the software supply chain** to pinpoint and automatically block unauthorized assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	✓ **Exceeds** **Authenticates every transaction,** user, asset (server, service account, etc.), and software executable prior to allowing access **Extends identity capabilities** by tracking authentications across network hops to ensure precise authentication **Enables time-based authentication** for situations such as debugging an asset **Policy Engine supports a broad range of access controls** (RBAC, ABAC and Intent-Based Access Control) **Provides protection** even when none has been explicitly configured via a recommendation engine (using Discovery) and out of the box access-control policies
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.	✓ **Meets** **Discovers all Enterprise Assets:** Users, Servers, Networks, Applications **Assesses Inherent Risk:** Vulnerabilities, CIS Configuration, Configuration and Inventory Drift, Missing Controls, Misconfigurations, Excess Privileges etc. **Provides recommendations and automated controls** to mitigate risk **Collects rich information and context** **Keeps a current picture of security** across the organization **Creates and enforces policies** to protect against risk automatically **Monitors all aspects of operations** to automatically tune compliance metrics, policies, and risk profiles

* NIST SP 800-207, Aug. 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final

prismo

SOLUTION BRIEF

Making A Zero Trust Architecture Fully Operational

Prismo enables efficient operation across environments of all sizes based on Zero Trust principles.

Continuous Authorization:

- Controls access between all sources and resources including users, devices, applications, APIs, and objects.
- Provides real-time analysis and control of all elements prior to granting access
- Delivers risk-based segmentation limiting North-South and East-West movement.

Cumulative Risk Profiles:

- Maintains dynamic risk profiles of all subjects and resources, using multiple criteria including behavior.
- Detects long-term, subtle, multistage attacks (i.e., Supply Chain) with event-level granularity
- Prioritizes resources targeted by multiple low impact attacks for attention based on cumulative risk score.

Real-time Response:

- Automatically creates policies to protect assets against vulnerabilities and blocks hostile behavior
- Enforces controls consistently across platforms, locations, and environments
- Continuously assesses risk and compliance, eliminating inefficient manual spreadsheet-based processes

Benefits

A Zero Trust approach to security positively impacts your core business goals and performance.

Stay Ahead of Threats

Prismo enables organizations to move faster than Threat Actors, reducing risk and proactively eliminating threats.

Increase Agility

The removal of security limitations enables organizations to pursue new business opportunities and respond more quickly to fast changing markets.

Slash Costs

Prismo's implementation of Zero Trust leverages real-time automation to keep direct and indirect security costs in check.

We're here to help you on your Zero Trust journey

With the release of NIST SP 800-207 in August 2020, the Zero Trust model has rapidly become the new standard. The Prismo Active Cyber Risk Management Platform is the first security platform architected from the ground up to meet and exceed NIST reference architecture and guideline recommendations for Zero Trust. If your organization is evaluating the Zero Trust Security Model or planning a Zero Trust migration, Prismo can help streamline, accelerate, and cost optimize your Zero Trust journey. Contact us today at www.prismosystems.com/demo to schedule a demo.

prismo

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.

Contact us to schedule a Demo!

www.prismosystems.com

info@prismosystems.com