ANOMALI

SOLUTION BRIEF

Implementing Zero Trust with Anomali

Implementing Zero Trust with Anomali

Advancing Identity, Visibility, and Continuous Verification for Modern Security Architectures

Zero Trust is an operational model grounded in one principle: never trust, always verify. As infrastructures become more distributed and identities more fluid, organizations struggle to enforce Zero Trust at scale. Most environments remain hindered by blind spots, disconnected controls, inconsistent enforcement, and data that cannot be analyzed fast enough to detect identity misuse.

Zero Trust takes more than segmentation and multi-factor authentication (MFA). It needs accurate identity and threat intelligence, real-time visibility across all your data, and continuous verification powered by analytics and automation. Legacy architectures and siloed tools simply weren't built to do this.

Anomali modernizes Zero Trust without re-architecting your environment. By combining threat intelligence, high-speed security analytics, and a scalable security data lake, Anomali gives organizations the contextual insight, identity correlation, and continuous monitoring foundation required to operationalize Zero Trust across hybrid, cloud, and multi-vendor environments. Anomali transforms Zero Trust from a set of disconnected controls into a unified, intelligence-driven security strategy.

Anomali ThreatStream acts as the intelligence layer for Zero Trust, providing the real-time knowledge needed to continuously verify identities, devices, and access requests.

Core Zero Trust Principles

To operationalize Zero Trust effectively, organizations must translate its high-level philosophy into actionable principles and capabilities. These principles guide how access is granted, how activity is monitored, and how risks are mitigated in real time. By embedding these concepts into people, processes, and technology, security teams can enforce consistent, intelligent policies across all users, devices, and resources. This supports a dynamic, adaptive security posture that scales across hybrid and cloud environments. These core principals are:

Verify Explicitly: Authenticate and authorize all available data — identity, device posture, location, and context. Every access request, whether internal or external, is evaluated continuously against risk signals to ensure only trusted actions are allowed.

Least Privilege Access: Grant users and systems only the minimum access they need, for the minimum time necessary. By limiting permissions dynamically, organizations reduce the potential impact of compromised accounts or malicious activity.

Assume Breach: Operate as if attackers are already inside the network. Segment systems, continuously monitor activity, and enforce adaptive policies to limit exposure and reduce the potential blast radius of any compromise.

Core Components

- **Identity and Access Management (IAM):** Enforce strong authentication and adaptive access policies through MFA, single sign-on (SSO), and contextual verification.
- **Device Security:** Ensure endpoints meet compliance and security posture requirements before granting access.
- **Network Segmentation:** Isolate critical systems, enforce micro segmentation, and control access paths.
- **Visibility & Analytics:** Continuously monitor user, device, and application behavior to detect anomalies, risky activity, and potential threats.
- **Automation & Orchestration:** Leverage AI-driven risk scoring, dynamic policy enforcement, and automated responses to maintain security at scale.

Why It Matters

- Reduces the attack surface and limits the impact of breaches.
- Protects hybrid, cloud, and remote work environments.
- Strengthens compliance with frameworks such as NIST 800-207, ISO 27001, and the CISA Zero Trust Maturity Model.
- Aligns with modern, AI-driven, identity-centric security operations that scale with enterprise complexity.

Threat Intelligence as Zero Trust Enabler

Anomali ThreatStream acts as the intelligence layer for Zero Trust, providing the real-time knowledge needed to continuously verify identities, devices, and access requests. While traditional security tools rely on static policies or manual correlation, ThreatStream feeds actionable intelligence into your security operations, enabling risk-informed decisions at machine speed.

How It Works:

- **Dynamic Risk Scoring:** Continuously ingests and analyzes Indicators of Compromise (IoCs) such as malicious IPs, domains, file hashes, and TTPs. Every access request is evaluated against this intelligence to assign a real-time risk score.
- **Continuous Verification:** Access decisions are dynamically enforced, with high-risk activity triggering automated mitigation, adaptive access controls, or additional authentication steps.
- **Contextual Awareness:** Threat intelligence enriches internal telemetry, providing analysts with the broader adversary context necessary for informed decision-making.
- **Accelerated Response:** Automated workflows integrate with existing policy enforcement and orchestration tools, enabling immediate containment, endpoint isolation, or policy adjustments.
- **Policy Optimization:** Security teams can refine Zero Trust policies continuously, based on emerging threats, intelligence updates, and anomalous activity trends.

Outcome: ThreatStream transforms static access policies into adaptive, risk-aware controls. Organizations gain the ability to enforce continuous verification, reduce exposure to threats, and act on intelligence-driven insights without disrupting existing infrastructure or workflows.

Security Analytics & Data Lake as Zero Trust Enabler

Anomali's Security Operations Platform combines high-speed security analytics, a scalable data lake, and integrated threat intelligence to serve as the operational brain of a Zero Trust architecture. By unifying telemetry from endpoints, networks, cloud apps, and identity systems, the platform provides complete visibility and actionable context for every user, device, and connection.

Ultimate Context & Visibility:

- Centralizes and normalizes security and IT telemetry in a single repository, eliminating blind spots and data silos.
- Retains 7+ years of hot, searchable data to support threat hunting, investigations, and compliance audits.
- Supports structured and unstructured data for richer correlation and analysis.

Dynamic, Risk-Based Access:

- Correlates internal telemetry with threat intelligence to calculate precise risk scores in real time.
- Enforces adaptive, least-privilege access: MFA prompts, restricted access, or full denial based on risk context.
- Applies historical and behavioral analytics to detect anomalous activity, insider threats, or compromised accounts.

Automated Detection & Response:

- AI/ML-driven analytics identify deviations from behavioral baselines and correlate them with known threats.
- Integrated security orchestration, automation, and response (SOAR) capabilities allow automated actions such as revoking credentials, isolating endpoints, or updating firewall and micro segmentation rules.
- Agentic AI surfaces relationships and patterns across datasets, assisting analysts in making rapid, accurate decisions.

Outcome: The combination of a high-speed security data lake, security analytics, and threat intelligence operationalizes Zero Trust at scale. Every access request, session, and connection is continuously verified, dynamically scored, and enforced in real time. With Anomali, organizations have proactive, intelligence-driven control across hybrid and cloud environments.

Anomali: Powering Zero Trust with Intelligence, Analytics, and Scale

Zero Trust succeeds when organizations can continuously verify every identity, device, and action while enforcing least-privilege, risk-based policies. Anomali delivers the intelligence, analytics, and automation to make this a reality, without re-architecting environments or disrupting workflows. Anomali helps enable Zero Trust with:

- **AI-Native Platform:** Agentic AI prioritizes threats, accelerates response, and enriches alerts for smarter decision-making.
- **High-Speed Security Data Lake:** Consolidates all telemetry and intelligence at scale for instant queries and insights.
- **Integrated Threat Intelligence:** Correlates internal and external signals for actionable context.
- **Flexible Deployment:** Augment existing stacks or consolidate into a single platform — no disruption, just enhanced outcomes.
- **Proven Results:**
  - Achieve 300× faster search performance
  - Investigate threats 50% faster
  - Store petabyte-scale data at a fraction of SIEM costs
  - Gain immediate value without disrupting workflows

By unifying threat intelligence, high-speed analytics, and a security data lake, Anomali transforms Zero Trust from a set of disconnected controls into an operational, intelligence-driven security strategy, enabling secure access, proactive threat containment, and improved outcomes across hybrid, cloud, and multi-vendor environments.

Security and IT Operations Done Differently.

Anomali delivers the leading AI-Powered Security and IT Operations Platform. Only Anomali integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one powerful platform. At the center is the Anomali Copilot that navigates a proprietary cloud-native security and IT data lake to drive first-in-market speed, scale, and performance at a fraction of the cost. Modernize security and IT operations to protect and accelerate your organization with better analytics, visibility, productivity, and talent retention.

Be Different. Be the Anomali. **Request a demo** to learn more.

ANOMALI