WHITEPAPER

Strengthening zero trust (NIST 800-207) with human risk detection.

www.netclean.com

NetClean.

Table of contents

Introduction

As organizations adopt the Zero Trust Security Model (NIST 800-207), they recognize the need to continuously verify every access attempt, device, and identity. However, even the most robust Zero Trust implementations face a critical challenge: post-authentication risk. While Zero Trust governs access and network segmentation, it does not inherently detect or respond to human risk factors—such as insider threats, compromised accounts, and compromising illegal user activity—once access is granted.

This is where NetClean ProActive steps in. By providing real-time Human Risk Detection, NetClean ProActive strengthens Zero Trust by identifying and mitigating risks beyond initial authentication. This whitepaper explores how Zero Trust and Human Risk Detection work together to close security gaps.

Part 1: Zero trust (NIST 800-207) overview

The NIST 800-207 publication defines Zero Trust as a framework that assumes no implicit trust in users, devices, or network segments. Instead, access is continuously verified based on real-time risk assessments.

Key zero trust principles:

1. Verify Explicitly – Always authenticate and authorize based on multiple risk factors.
2. Least Privilege Access – Users and devices receive only the permissions they need.
3. Assume Breach – Monitor, log, and segment networks to limit potential threats.
4. Continuous Monitoring & Analytics – Detect anomalies to prevent post-authentication compromise.
5. Threat Intelligence Integration – Use internal and external signals to enhance security decisions.

These principles create a robust security foundation, but they primarily address access control—not ongoing user behavior and human risk factors.

Zero zrust for endpoints: Securing devices within the framework

While Zero Trust is a security framework, its implementation often involves protecting endpoints, as they serve as critical access points to corporate networks, applications, and data. Ensuring that endpoints are continuously verified, monitored, and protected is a key pillar of Zero Trust security.

How zero trust protects endpoints

Zero Trust assumes that no endpoint is inherently trusted and must be continuously validated through multiple security controls:

1. Device posture & compliance checks

- Ensures an endpoint meets security compliance policies before allowing access.
- Verifies OS version, patches, antivirus status, and security configurations.
- If a device is untrusted or outdated, access may be restricted or denied.

2. Endpoint Detection and Response (EDR/XDR) agents

- Many EDR/XDR solutions install an agent on endpoints to monitor for suspicious activity.
- These agents provide real-time threat detection, behavioral analysis, and automated responses.
- If an endpoint is compromised, the EDR system can quarantine the device, kill processes, or isolate it from the network.

3. Zero Trust Network Access (ZTNA)

- ZTNA solutions replace traditional VPNs by ensuring endpoints only access specific resources based on identity, device posture, and contextual risk.
- Unlike VPNs that grant broad network access, ZTNA enforces least privilege connectivity on a per-app or per-resource basis.

4. Continuous monitoring & adaptive security

- Even after an endpoint gains access, Zero Trust ensures ongoing monitoring for risk signals.
- If a previously trusted endpoint starts behaving abnormally, access permissions can be revoked dynamically.
- Security teams can respond in real time to potential insider threats or compromised accounts.

How does this relate to NetClean ProActive?

- EDR and ZTNA focus on endpoint security but primarily detect traditional cyber threats (e.g., malware, ransomware, exploits).
- NetClean ProActive focuses on a critical but often overlooked risk: human-driven compromising illegal activity (CSAM detection).
- By integrating with Zero Trust frameworks, NetClean ProActive enhances endpoint security by detecting post-authentication risks with 100% accuracy related to user behavior.

Part 2: The missing piece – Human risk detection

While Zero Trust reduces attack surfaces, it does not inherently detect insider threats or compromised users. This is where NetClean ProActive enhances Zero Trust strategies by adding human risk detection beyond access control.

Why human risk detection matters in zero trust:

1. Post-Authentication Threats: Many threats emerge after authentication, making access control insufficient.
2. Insider Threats: Employees and contractors with legitimate access can still misuse or abuse their privileges.
3. Behavioral Shifts: A user who passed authentication may later engage in illegal compromising activity that Zero Trust controls do not detect.

How NetClean ProActive strengthens zero trust

Zero trust principle	How NetClean ProActive enhances it
Continuous verification	Detects post-authentication risks, such as deliberate acts of CSAM consumption, ensuring that trust is continuously evaluated and not static.
Context-aware access	Detects abnormal user behavior indicative of insider threats, delivering actionable intelligence for security teams.
Adaptive authentication	Assists in triggering step-up authentication or access revocation upon detecting high-risk activity.
Microsegmentation & isolation	Provides real-time risk assessments that can dynamically isolate compromised accounts.
Threat intelligence feeds	Integrates with security platforms to inform broader risk-based access decisions.

Part 3: Closing the zero trust gap with NetClean ProActive

By integrating Human Risk Detection into Zero Trust security policies, organizations can ensure that their Zero Trust architecture remains dynamic, resilient, and capable of addressing modern security challenges.

Key takeaways:

- Zero Trust (NIST 800-207) governs access but does not inherently detect insider threats.
- NetClean ProActive fills the Zero Trust gap by detecting illegal activity and compromised users after authentication.
- Integrating Human Risk Detection into Zero Trust strategies enhances security beyond traditional access controls.
- For more information on how NetClean ProActive can complement your Zero Trust strategy, contact us today.