# Unit 42 Zero Trust Advisory

## Forge A World-Class Security Foundation, Unleashing Superior Cyber Resilience With Zero Trust.

### Zero Trust is a Journey

Zero trust is a powerful security strategy, but moving from intention to execution is where many organizations get stuck. Visibility gaps, operational complexity, and organizational friction often create barriers that slow progress and drain momentum.

#### Limited Visibility and Incomplete Understanding of the Environment

Visibility gaps leave critical blind spots. Without a complete view of users, assets, and data flows, it's nearly impossible to apply effective zero trust controls. In 75% of the incidents Unit 42 investigated, the logs showed critical evidence of initial intrusion. However, this evidence wasn't readily accessible or effectively operationalized, allowing attackers to exploit these gaps undetected.[1] Shadow IT, cloud sprawl, and legacy infrastructure make it difficult to map the environment and define trust boundaries. The result is both persistent security gaps and policies based on assumptions rather than reality.

#### Operational Complexity and Inconsistent Enforcement

Defenders are already stretched thin, relying on manual processes like firewall rule updates and network segmentation that are both time-consuming and prone to error. Legacy systems further complicate enforcement, often lacking support for modern controls such as multifactor authentication (MFA). As organizations expand into hybrid and multicloud environments, the challenge grows, introducing enforcement inconsistencies, integration hurdles, and additional layers of operational complexity.

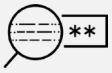
#### Organizational Misalignment Undermines Momentum

Even with the right tools, zero trust initiatives often lose momentum due to a lack of strong cross-functional support and shared ownership. This challenge is particularly urgent given that 86% of the incidents Unit 42 responded to in 2024 involved business disruption, spanning operational downtime, reputational damage, or both.[2] Unclear or misaligned priorities, siloed teams, and fear of disrupting business operations stall progress. Without a cohesive plan, cross-functional support, and sustained executive engagement, zero trust can lose traction before it delivers results.

### Unit 42 Zero Trust Advisory Benefits

#### Gain foundational visibility

See the full picture—identities, data flows, and systems—so you can ground your zero trust strategy in reality, not assumptions.



#### Navigate zero trust complexity

Cut through the noise. Focus your zero trust efforts where they'll have the biggest impact, with guidance rooted in real-world experience.

#### Reinforce strategic alignment

Connect zero trust to outcomes that matter. Secure executive support and long-term investment by tying strategy to business impact.

## Unit 42 Zero Trust Advisory

Unit 42 Zero Trust Advisory turns strategy into action. Whether you're starting from scratch or advancing an existing zero trust program, we guide you through every step. Our Unit 42 experts work alongside your team to align stakeholders, identify priorities, and build a practical roadmap tailored to your environment and business goals.

## Cut Through Complexity To Make Zero Trust Real

### Architecture Review

Uncover your current security posture across identity and network layers in expert-led working sessions that bring cross-functional stakeholders together and expose the silos that block zero trust progress.

### Identify Architectural Gaps

Pinpoint the blockers that stand in your way, across legacy systems, disconnected controls, operational bottlenecks, and policy blind spots. Fix what matters most without slowing innovation.

### Map Zero Trust Readiness

Measure what's in place, what's missing, and where to go next. We provide an intelligence-informed and prioritized view of your zero trust maturity to help you move forward with clarity.

### Build A Zero Trust Plan

Translate strategy into execution with a tailored roadmap. Align your zero trust goals to business priorities and roll them out in practical, achievable phases.

## About Unit 42

Palo Alto Networks Unit 42® brings together world-renowned threat researchers with an elite team of incident responders and security consultants to create an intelligence-driven, response-ready organization passionate about helping customers more proactively manage cyber risk. Our consultants serve as your trusted advisors to assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time. For the latest threat intel and research, please visit https://unit42.paloaltonetworks.com.

1. Unit 42 2025 Global Incident Response Report, Palo Alto Networks, February 2025.
2. Ibid.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com



unit42_ds_unit-42-zero-trust-advisory_072125