

Zero-Trust Network, not just access.

Access-first ZTNA checks who is connecting, opens a tunnel, and is finished. FCI Unified Control continuously [*inspects*] every session in both directions, for as long as it lasts.



Decides once, at connect.

A stolen credential passes. A payload rides the session unread.

Every network transaction is evaluated.

Clean content reaches the app. Threat Defense removes the exploit; the rule blocks the rest.

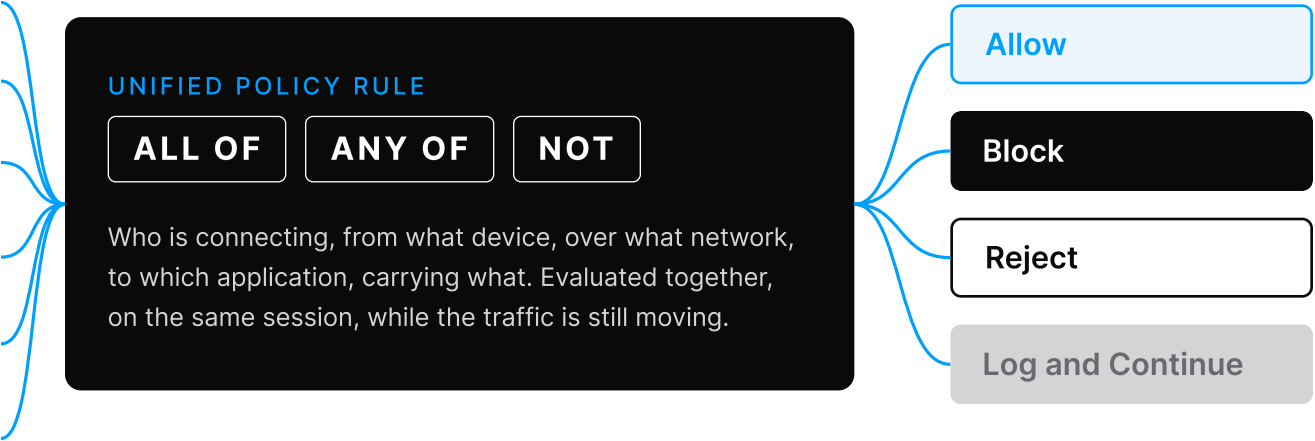
39% of breaches involve credential abuse¹

~90% of investigations found identity weaknesses²

72 min from access to exfiltration, fastest quarter²

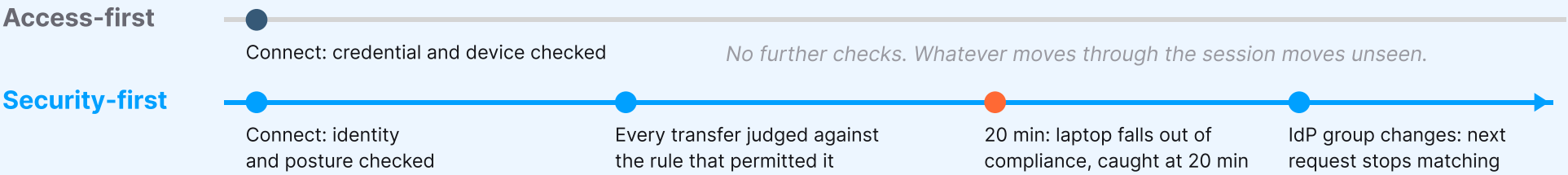
RULES SEE THE WHOLE SESSION

- Session content
- File type, name, hash · HTTP method, URL, headers
- Session context
- Address, port, direction, TLS, domain category
- Enrichment
- Source and destination country, URL category
- User identity
- Group membership and attributes from your IdP
- Device identity and posture
- Managed, domain-joined, OS version, encryption
- Schedule and AI
- Days and UTC hours · AI Governance conditions



Threat Defense is always on, for all traffic.
Policy rules layer your controls on top.

RULE DECISIONS ARE CONTINUOUSLY RE-EVALUATED, EVEN WITHIN THE SAME NETWORK SESSION



SECURITY-FIRST ZTNA IN PRACTICE

Finance reaches the ERP system from managed devices, carrying nothing that runs. Contractors reach the vendor portal only. Everything else is denied.

A controller opens the ERP system from a managed laptop, then drags a ZIP archive into its import screen.

SESSION ALLOWED

ARCHIVE BLOCKED

An attacker inside the network uses the controller's stolen credential from an unmanaged machine.

SESSION BLOCKED

DEFAULT-DENY

Malware on the controller's laptop fires an exploit through the live ERP session, pulls an archive out, then probes HR.

EXPLOIT REMOVED INLINE

ARCHIVE BLOCKED HR PROBE DENIED

Human resources moves the controller to Marketing in the identity provider.

ERP ACCESS ENDS

NO RULE EDITED

1. Verizon, 2026 Data Breach Investigations Report. 2. Palo Alto Networks Unit 42, 2026 Global Incident Response Report. © 2026 Trinity Cyber, Inc. Full Content Inspection™ is a trademark of Trinity Cyber, Inc.