

WHITEPAPER — FCI UNIFIED CONTROL · SECURITY-FIRST ZTNA

Full Content Inspection. Total Control.

Zero Trust Network Access that **expects** the attacker.

CONTENTS

01	Access-first ZTNA verifies the credential, not the content	2
02	Every rule reads the content and the context	3
03	Inspection and decision on every transaction	4
04	Credentials open the door. Content decides what passes.	5
05	In practice — scenarios and what the rules do	6
06	Closing — Zero Trust Network, not just Access	7

OVERVIEW

FCI Unified Control is security-first zero trust network access (ZTNA). ZTNA decides who reaches which application and from what device, access-first ZTNA focuses on authenticating and authorizing the session. Once a connection is established, traditional controls let traffic flow without further inspection. FCI Unified Control takes a different approach. inspecting every session for threats before applying access rules, evaluating what each session carries as well as who sent it, and decides every transaction, not just the connection.

SECTION 01

Access-first ZTNA verifies the credential, not the content

An access-first broker authenticates the user and the device, authorizes the session, opens the connection to the application, and moves on. It sees context once, at connect time, and never sees the content. Inside the session, a spreadsheet, an archive, an exploit, or an executable all look alike.

Verizon's 2026 Data Breach Investigations Report finds credential abuse in 39 percent of breaches when counted at any stage of the breach progression.¹ Unit 42's 2026 incident response report finds that identity weaknesses played a material role in nearly 90 percent of cases, and the fastest 25 percent of intrusions reached exfiltration in 72 minutes.²

A stolen credential passes the authentication and authorization check because the credential itself is real. A payload rides the permitted session because nothing reads it. Reading the session is one check that neither can pass, and it is the check FCI Unified Control runs on every transaction.

BY THE NUMBERS

39%

of breaches involve credential abuse at some stage of the breach progression.

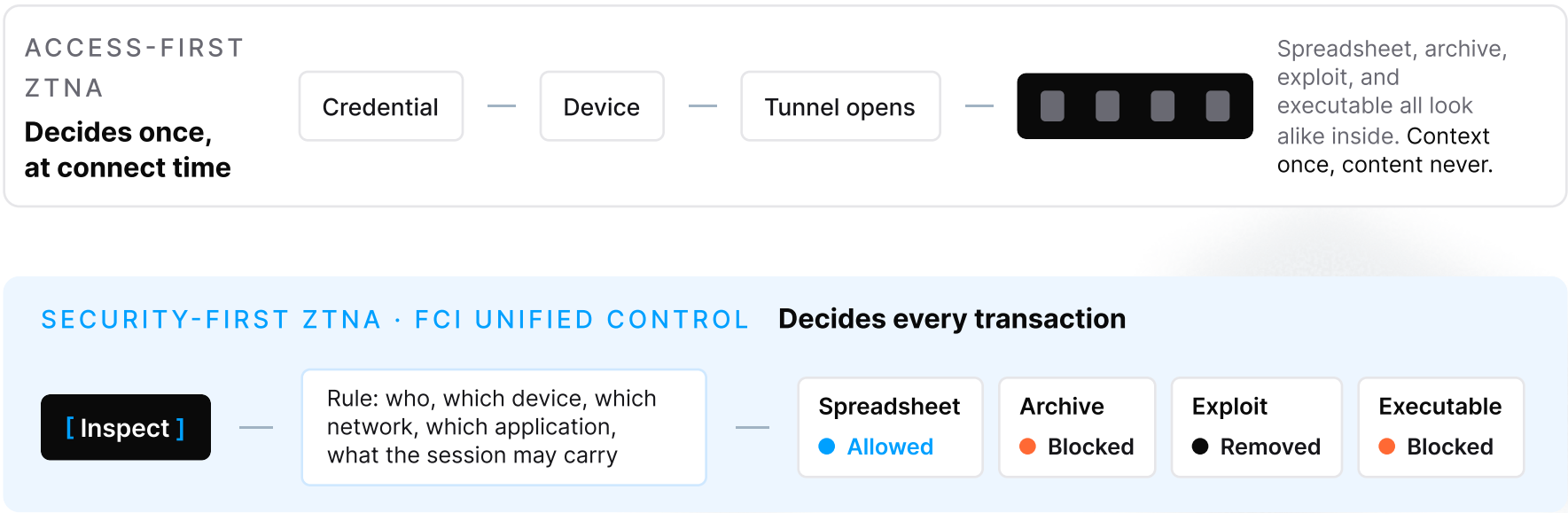
~90%

of incident response cases involve a significant identity weakness.

72 min

from intrusion to exfiltration in the fastest 25% of cases.

TWO WAYS TO DECIDE ACCESS



SECTION 02

Every rule reads the content and the context

Content is what a transaction carries. FCI extracts content from the traffic itself: the file’s type and hash, the request’s method and URL, and the protocol and payload as they are, not as they are labeled. Context is everything around the transaction: who sent it, from what device, on which network, where, and when. Access-first ZTNA reads context once, at connect time, and never reads content. FCI Unified Control reads both on every transaction. That is why a single rule can require a managed device and a member of Finance while forbidding an executable, and why a rule can combine those conditions with ALL OF, ANY OF, and NOT.

CONTENT · WHAT IT CARRIES

Files
The MIME type, name, and SHA256 hash of any file, in either direction, parsed as an endpoint would see it.

Requests
HTTP method, URL, status, and headers of every request, so a rule can tell an upload from a page load.

Protocols
FCI parses every protocol in depth and sees the traffic for what it is, as an endpoint would.

Sessions
FCI reassembles and reads every session in both directions, so a rule sees what moved, not a tunnel.

Payloads
FCI decodes and parses every payload to what it is, whether archive, script, or exploit, as an endpoint would see it.

**UNIFIED
RULE**

**ALL OF
ANY OF
NOT**

CONTEXT · WHAT SURROUNDS IT

Identity
Group membership, or any attribute the identity provider supplies, matched by name and value.

Device and posture
Device group plus posture: OS, managed status, drive encryption, VM detection, custom attributes.

Network
Addresses, ports, direction, TLS version, domain, and one of 79 domain categories, all available without decryption.

Country and category
Source and destination country and URL category, looked up as the session flows.

Time and AI
A Schedule of weekdays plus a UTC time range, and AI Governance conditions.

WHY IT MATTERS · OPERATIONS

One rule replaces three products

Today a firewall reads the network, an identity broker reads the user, and an endpoint agent reads the file. None of them see what the other two see. FCI Unified Control lets one rule carry all three: it checks the whole rule on every transaction and matches encrypted sessions by domain and category without decryption. The identity provider stays the source of truth, so a group change takes effect on the next transaction without editing the rule.

WHY IT MATTERS · SECURITY

The attacker must pass every check, every time

A stolen credential still fails the device test. A permitted user still cannot transfer an executable. Inspection strips malware out of a live session before any rule runs, and a laptop that drifts out of compliance is caught on its very next transaction. Because the platform judges content and context together, there is no single check to steal, spoof, or wait out. The same inspection covers traffic between internal servers, so an attacker that’s already inside faces the same checks.

SECTION 03

Inspection and decision on every transaction.

1

BEFORE ANY RULE

Inspection covers every session

Trinity Cyber’s managed threat protection covers every session before any access rule runs, and every transaction inside a permitted session gets the same inspection. Identity never exempts content from inspection, and a valid credential never launders a payload. The platform also inspects east-west traffic between internal servers.

2

PER TRANSACTION

An Allow is a decision the platform keeps making

A transaction is one request or one file transfer, and each one is decided independently. The platform re-evaluates posture on every transaction, so a laptop that falls out of compliance twenty minutes into a session is caught on its next transaction, and a group change in the identity provider takes effect on the next one too. Every transfer inside a permitted session must satisfy the rule that permitted it.

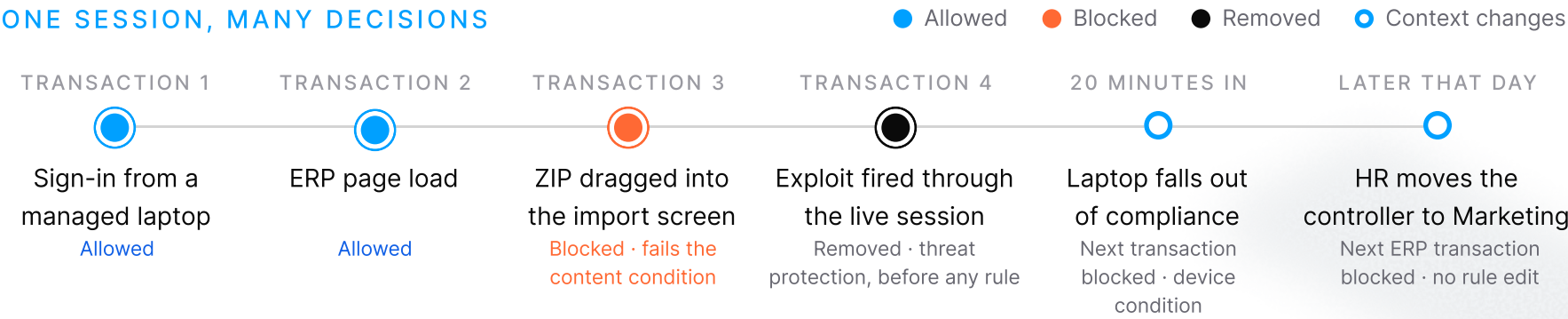
3

LOG AND CONTINUE

A new rule shows its matches before it blocks

If a new rule runs as Log and Continue, it records every match and blocks nothing, so the team can see what the rule would stop before it stops anything. Policy Logs capture each match in a filterable and exportable log; with the entity path the rule applied through and whether the traffic was east-west included. The Details view lists every rule with a hit count for the last 24 hours.

ONE SESSION, MANY DECISIONS



[INSPECTED] Full Content Inspection™ runs on every transaction in both directions, before any access rule runs and no matter which rule allows the traffic.

SECTION 04

Credentials open the door. Content decides what passes.

THE SECURITY TEAM WRITES

Two allow rules and one default-deny

The credential gets a person in, and the content decides what they can bring. One rule covers Finance, one covers contractors, and default-deny sits beneath both: anything not covered by a rule is blocked.

FINANCE RULE

ALLOW

Allow Finance into the ERP system with nothing that runs

Enforcement: Mandatory · Action: Allow · Logging: Lite

ALL OF

User Identity → Groups → Exact → "Finance"
Device Posture → Managed Device → True
Network → Internal Traffic → True
Network → Domain → Exact → "erp.internal.oscuradynamics.com"

NOT ANY OF

File → File MIME Type → application/zip
File → File MIME Type → application/vnd.microsoft.portable-executable

Controller, managed laptop

ALLOWED

Sign-in and page loads meet every condition of the Finance rule.

Same session, ZIP import

BLOCKED

The archive fails the content condition. Each transfer is its own decision.

Stolen credential, unmanaged machine

BLOCKED

Identity matches, the device does not, and default-deny takes over.

CONTRACTOR RULE

ALLOW

Accounts with a Contractor employee type can only reach the vendor portal from managed devices within the United States.

Contractor in Ohio

PORTAL

ERP

The platform allows the portal and blocks the ERP system. The Contractor attribute matches the contractor rule and no other, so the ERP request falls to default-deny.

DEFAULT-DENY

BLOCK

Every transaction that no allow rule covers.

SCENARIOS: WHAT THE RULES DO

● Allowed ● Blocked ● Removed ● No rule changes

SCENARIO	OUTCOME
A controller opens the ERP system from a managed laptop, then drags a ZIP archive into its import screen.	● ● The platform allows the sign-in and blocks the transfer. Each is its own decision, and the archive fails the content condition.
An attacker on an unmanaged machine inside the network uses the controller's stolen credential.	● The platform blocks the attempt. The credential is real, so identity matches, but the device does not, and default-deny takes over.
Malware on the controller's laptop fires an exploit through the live ERP session, pulls out an archive, and then probes HR.	● ● The platform stops all three. Threat protection removes the exploit first, the archive fails the content condition, and no rule covers HR, so default-deny blocks the probe.
A contractor opens the vendor portal from a managed device in Ohio, then tries the ERP system.	● ● The platform allows the portal and blocks the ERP system because the Contractor attribute matches only the contractor rule.
Human resources move the controller to the Marketing group in the identity provider.	● The next ERP transaction no longer matches the Finance rule and is blocked. The group is the condition, so no rule changes.

One platform, one rule language

CONTENT PLUS
CONTEXT

Fewer blind spots

What a user carries is as visible as who the user is.

Fewer rules

A firewall entry, an identity rule, and a device-management condition become one policy.

Fewer products

Access control, content inspection, and firewall conditions use one platform with one rule language.

Evidence

Policy Logs record every match inside the permitted session, with domain, ports, entity path, and direction.

CLOSING

Zero Trust Network, not just Access.

Access-first ZTNA reads context once, at connect time, never reads content. FCI Unified Control reads both on every transaction, so a stolen credential still fails the device test, and a permitted user still cannot transfer an executable. One rule language covers access control, content inspection, and firewall conditions, and every decision is made again on the next transaction.

SEE IT ON YOUR
OWN TRAFFIC

Ready to see it on live traffic?

VISIT US AT trinitycyber.com

SOURCES

- 1. Verizon, 2026 Data Breach Investigations Report, May 2026.
- 2. Palo Alto Networks Unit 42, 2026 Global Incident Response Report, February 2026.