

SLICK SHEET — FCI UNIFIED CONTROL · HIERARCHICAL POLICY

Full Content Inspection. Total Control.

Hierarchical multi-tenancy solution
for [managed service providers](#).

CONTENTS

01	One standard drifts across many client consoles	2
02	The hierarchy answers all four questions	3
03	Set the standard once for every client	4
04	Example of a Mandatory policy and a Standard policy	5
05	Where each policy stands — scenarios and outcomes	6
06	Closing — one standard, every client	7

OVERVIEW

A managed service provider (MSP) keeps one security standard and many clients, and every client keeps its own exceptions. Enforcing that standard, stripped down to what it decides, comes to four questions: where a policy applies, what every client must have, what each client may change, and who may see and change what.

FCI Unified Control, the policy layer of Trinity Cyber’s Full Content Inspection™ (FCI) platform, answers all four with hierarchical multi-tenancy, which means each client is its own tenant and every tenant sits beneath its MSP in one hierarchy. A policy written at the top flows to every client beneath it, its Enforcement level draws the line between required and recommended, and Policy Logs, reporting, and operator access follow the same hierarchy.

SECTION 01

One standard drifts across many client consoles

An MSP writes its standard once and enforces it many times, once per client. One line of it, no file uploads to AI services, lives as a firewall rule at one client, a browser extension at a second, and a line in the onboarding checklist at a third. Every copy drifts, and when a client asks what the standard did for them last month, someone on the MSP's team assembles the answer by hand.

In Kaseya's 2026 State of the MSP report, about 71 percent of MSPs report year-over-year growth in cybersecurity revenue, and 61 percent say most or all of their clients turn to them for cybersecurity advice. The barriers sit on the delivery side, where 50 percent cite the complexity of security products as a top barrier, up from 38 percent a year earlier, and the share unable to demonstrate value to clients quickly has nearly doubled, to 19 percent.¹ Clients feel the same sprawl. In Barracuda's 2025 MSP Customer Insight Report, 52 percent of organizations with 50 to 2,000 employees want an MSP to help them manage a spiraling number of disconnected security tools and vendors.²

One flat policy for every client is too blunt for the differences between them, and each exception granted to one weakens it for all. A separate policy set per client is exact, and someone maintains every copy by hand. The right model needs both at once, a policy that holds everywhere and room for each client to differ within it, with a record of what held where.

BY THE NUMBERS

71%

of MSPs report year-over-year growth in cybersecurity revenue

50%

cite the complexity of security products as a top barrier, up from 38% a year earlier

52%

of organizations with 50 to 2,000 employees want an MSP to manage disconnected tools

BETTER WAY TO SET THE STANDARD

ONE FLAT POLICY

Too blunt for the differences between clients

Each exception granted to one weakens it for all.

A POLICY SET PER CLIENT

Exact, and maintained by hand

Someone maintains every copy, and every copy drifts.

[Write it once]

FCI Unified Control holds both at once

A policy that holds everywhere, room for each client to differ within it, and a record of what held where.

SECTION 02

The hierarchy answers all four questions

Where a policy sits in the hierarchy, and how its Enforcement level is set, answers each question, and the platform enforces what the hierarchy records.

01

THE MSP DECIDES

Where a policy applies

THE HIERARCHY ENFORCES

A policy sits on an entity, the platform’s name for any point in the hierarchy: the MSP, a client, a site, or a team. Written on the MSP, it flows to every client beneath; written on a client or a team, it holds there and below. The Details view on any entity lists its own policies beside the ones it inherits.

02

THE MSP DECIDES

What every client must have

THE HIERARCHY ENFORCES

With Enforcement set to Mandatory, the policy applies everywhere beneath the entity it was written on, and no client that receives it can change it. One update takes effect at every client, with nothing to redeploy.

03

THE MSP DECIDES

What each client may change

THE HIERARCHY ENFORCES

With Enforcement set to Standard, the policy arrives as a baseline the receiving client can tune, or override with a more specific policy of its own. The child policy takes precedence, and the rest of the set stays as it is.

04

THE MSP DECIDES

Who may see and change what

THE HIERARCHY ENFORCES

Access Management scopes operators and client administrators, and it follows the same hierarchy. A user’s Primary Entity sets which policy groups the user can see, and group permissions and scopes set what the user can do there, so an MSP’s operators see their customers and a client’s administrators see their own organization.

ENFORCEMENT LEVEL

Standard or Mandatory

Standard is for defaults that clients tune, such as a starting posture for a new business unit. Mandatory is for what must hold everywhere: a regulatory requirement, a block on a known-bad category, or a condition the security team calls non-negotiable.

SECTION 03

Set the standard once for every client

1

UNIFIED POLICIES

Seeing the client hierarchy

Unified Policies opens on the MSP's organization as an expandable hierarchy of entities. Entity types include Managed Service Provider, Resale Partner, Customer, Connector, Vertical, Department, and Team, so the hierarchy follows the way an MSP sells and delivers. The Details view on any entity lists every policy standing on it, own and inherited, with its enforcement level and a 24-hour hit count.

2

POLICY BUILDER

Writing the policy once

Create Policy on the MSP's own organization opens the builder, where a policy carries an Enforcement level, an Action (Allow, Block, Reject, or Log and Continue), and a Logging level. Conditions combine network, file, device posture, user identity, and AI terms with ALL OF, ANY OF, and NOT. Log and Continue records a match and blocks nothing, so a new policy written that way shows its matches at every client before it blocks anything.

3

BLOCK

Switching it on and observing the results

Changing the action to Block turns the policy on. Policy Logs record every match down to the session, with the path the policy took through the hierarchy to reach that client, so a client's question about last night is a filtered lookup and an export. Activity, Metrics, and Monthly Usage group by the same entities, so one screen reports per customer, per vertical, or per region.

SECTION 04

Example of a Mandatory policy and a Standard policy

An MSP writes two policies once: an Enforced Mandatory policy that blocks file upload to AI services and unapproved providers, and a Standard baseline that allows AI sessions on managed devices under company accounts. Client A's engineering team overrides the baseline; the Mandatory policy holds beneath it.

THE LEVEL YOU MANAGE MSP

Writes each policy once. Every client beneath inherits it.

The Mandatory policy holds beneath every client override.

ENFORCED

MANDATORY

Block file upload to AI services and any provider, model, or application outside the approved list.

No client can change it.

BASELINE

STANDARD

Allow AI sessions on managed devices under company accounts, code execution off. Deny the rest.

Each client tunes or overrides it.

Client A

ALLOWED

Company accounts on managed devices. Engineering override: code execution on.

Client B

BLOCKED

Personal subscription to the same assistant. Session denied. File-upload block inherited, Mandatory.

Every client

INHERITED

Same enforced policy and baseline the day it is added, nothing copied.

WHERE EACH POLICY STANDS

● Mandatory ● Standard ● Overridden

ENTITY	TYPE	BLOCK AI FILE UPLOAD (ENFORCED)	ALLOW APPROVED AI SESSIONS (BASELINE)
The MSP	Managed Service Provider	● Mandatory, written here	● Standard, written here
Client A	Customer	Inherited, enforced	Inherited. Company accounts on managed devices: allowed
Engineering	Team	Inherited	● Overridden: code execution on
Client B	Customer	Inherited, enforced	Inherited. Personal subscription: session denied

SCENARIOS: WHAT THE POLICIES DO

SCENARIO	OUTCOME
The MSP adds a new client, Client C, as a Customer entity.	Both policies are in force on day one , with nothing copied. Client C’s Details view lists them as inherited, one Mandatory and one Standard.
A Client B administrator asks to relax the AI file-upload block.	The policy is Mandatory, so Client B cannot change it. The Details view lists it as inherited, and the request goes to the MSP.
A Client B administrator signs in through single sign-on.	Single sign-on sets the administrator’s Primary Entity to Client B and maps their permissions. That administrator sees only Client B.

DEPLOYMENT

Nothing new to deploy

The policies need nothing beyond FCI Unified Control. Policies attach to the hierarchy, Activity and Metrics group by it, usage reports along it, and Access Management scopes users by it. Trinity Cyber’s managed threat protection keeps running beneath every policy.

CLOSING

One standard, every client.

A policy written at the top flows to every client beneath it. Its Enforcement level draws the line between required and recommended, and Policy Logs, reporting, and operator access follow the same hierarchy, so the MSP sets the standard once and every client keeps the room it needs.

SEE IT AT
EVERY CLIENT

Ready to see it at every client?

VISIT US AT trinitycyber.com

SOURCES

- 1. Kaseya, *2026 State of the MSP Report*, April 2026; survey of 1,061 MSPs, November 2025.
- 2. Barracuda Networks, *MSP Customer Insight Report 2025*, July 2025.