DATA SHEET

Terniion™ for Security Operations Centers and MSSPs

The Challenge: Visibility Without Risk, Response Without Limits

Every SOC and MSSP operates under a core tension. To defend everything else, your analysts need broad visibility across the environments you protect, plus the ability to respond the moment something goes wrong. Attackers know this, so they don't necessarily target the SOC directly; they try to blind it, outpace it, or route around it entirely. The moment your detection and response capability loses ground, your clients lose their defender.

The constraints are real:

- Detection typically requires read-only access, but remediation and response require far more. Those privileged response paths are exactly what a sophisticated attacker wants to disrupt.
- Under assumption of breach, CSIRT needs something specific: uninterrupted access to the resources under active attack, while simultaneously shutting out the rest of the world to stop the attack in its tracks.
- MSSPs manage hundreds of tenants through shared infrastructure, where one compromised client can cascade into a portfolio-wide incident.
- AI is accelerating both sides: detection gets smarter, but so does reconnaissance, lateral movement, and automated exploit generation.

Perimeter defenses, VPNs, and bastion hosts were never designed for this. Even mesh VPNs fall short because of their single layer of encryption and lack of authenticated encryption. Xiid's Terniion is secure by design.

Terniion protects the SOC's infrastructure, enabling the SOC to do its job more securely and effectively. Analysts maintain constant, secure access to environments under active attack. The CSIRT can contain a breach while staying in the fight. And for MSSPs, Terniion is the engine to bring to every client, making their environments genuinely undiscoverable.

Business Outcomes

Maintain Access to Environments Under Active Attack

The most critical moment in incident response is what happens after detection. CSIRT needs uninterrupted access to the environment under attack while the attacker loses theirs. Pre-positioned SealedTunnels let designated responders connect to affected assets at machine speed, while Terniion closes every other inbound path. The attack stops, but the response effort continues without interruption.

The Monitoring Paradox, Eliminated

SIEM, SOAR, data lakes, and detection platforms operate behind closed inbound ports. Telemetry flows in through outbound-only tunnels, so the SOC sees everything while disappearing from the attack surface itself.

Tenant Isolation That Holds Under Breach

MSSP client environments connect through process-isolated paths rather than flat VPN meshes. A compromised tenant cannot pivot into shared infrastructure or reach any other tenant, breaking the chain that turns one client's incident into a portfolio-wide breach.

Containment, Then Controlled Return to Service

When an incident is active, CSIRT tightens access from within the Terniion platform by scoping connectivity to the affected environment down to specific authorized processes. Everything else is shut out. Once remediation is complete and the resource is cleared, it comes back online outside the secure platform, on the SOC's terms with no emergency firewall changes and no network rebuilds.

5 Ways Terniion Enables SOCs and MSSPs to Protect Their Clients

Best Practice	Key Actions	Xiid Terniion Solution
Maintain Uninterrupted Access During Active Incidents	Guarantee CSIRT can reach environments under attack while simultaneously shutting out the rest of the world, all without waiting on emergency firewall changes or VPN re-provisioning.	Pre-positioned SealedTunnels bind responder access to specific authorized processes and workstations. When an incident is declared, CSIRT connects immediately. Every other inbound path is already closed.
Remove the SOC from the Attack Surface	Stop SIEM, SOAR, detection platforms, and analyst workstations from becoming a point attackers can blind, disrupt, or pivot through.	SealedTunnel closes inbound ports on all SOC tooling. Telemetry flows outbound-only from monitored assets, so the SOC ingests data without exposing itself as a return path for attackers.
Extend Process-Level Isolation to Every Client	Give each tenant its own path with no shared credentials and no flat mesh that lets one compromised environment reach the next.	Each client environment connects through dedicated, process-isolated interaction paths.
Enable Programmatic Containment and Staged Return to Service	Revoke, scope, and restore access by policy during and after an incident rather than by physically unplugging infrastructure.	Terniion Commander centralizes "who can talk to what" as maintainable policy. CSIRT tightens access to specific processes during containment, then stages a controlled return to service from within the SealedTunnel as assets are cleared.
Harden AI-Enabled Detection and Response Tooling	Protect the models and knowledge bases powering modern detection, and defend against attackers using AI to automate reconnaissance and exploit generation.	Triple-layer, post-quantum encryption and process-level isolation protect AI-driven detection tooling, training data, and model weights from tampering and poisoning. Closed inbound ports block the machine-speed reconnaissance AI-powered attackers rely on.

Key Components

- **SealedTunnel**
  Executed via STLink, a lightweight software agent on either end, these are outbound-only, triple-encrypted, process-to-process tunnels that perform reliably even over unstable networks, ideal for multi-tenant monitoring across hostile and segmented networks.
- **Commander**
  The control brain coordinating secure connections across cloud, on-prem, and hybrid environments. It centralizes policy so "who can talk to what" becomes maintainable rules instead of 10,000 firewall exceptions.
- **Connector**
  Joins two outbound-only communication halves without ever decrypting traffic. It serves as a secure rendezvous where quantum-encrypted messages are dropped off and picked up by authorized STLinks, keeping critical infrastructure undiscoverable.
- **Aclave Authentication Management**
  Credential-less authentication that lets staff and partners access systems without usernames, passwords, or long-lived credentials.

How Terniion Works in SOC and MSSP Environments

Terniion is a secure network access control platform deployed as an overlay. It does not require replacing SIEM, SOAR, EDR, ticketing, or identity systems.

What This Looks Like in Practice

In-House Security Operations

- SIEM, SOAR, XDR platforms, and analytics data lakes run with all inbound ports closed.
- Analyst workstations connect to investigation tooling through outbound-only, process-scoped tunnels instead of flat VPNs that expose the entire SOC subnet.
- A compromised analyst workstation cannot pivot into the detection pipeline, the data lake, or the ticketing system.

Managed Security Service Providers

- Client telemetry flows one-way from the customer environment into the MSSP's analytics stack through outbound-only SealedTunnels.
- Each tenant's ingestion, enrichment, and response workflows run in process-isolated tunnels, so a rogue or compromised tenant cannot reach another.

CSIRT Response and Recovery

- Backup repositories, immutable storage, golden images, out-of-band management, and IR consoles run as non-addressable, undiscoverable resources.
- Pre-positioned access policies let CSIRT reach these assets from designated responder workstations immediately when an incident is declared, wihtout the need for emergency firewall changes or VPN re-provisioning.
- Containment runs from within the SealedTunnel. Once the affected environment is cleared, the resource returns to service outside the tunnel, on the SOC's terms, with full connectivity restored.

FAQS

Does Terniion replace our SIEM, SOAR, or EDR?

No. Terniion is an overlay. It sits around your existing SOC stack (SIEM, SOAR, EDR, ticketing, and identity) to make those platforms non-routable from the broader network while keeping them fully functional for analysts, automations, and integrations.

How does multi-tenancy work for MSSPs?

Each client tenant gets its own dedicated, process-isolated SealedTunnel path. Commander centralizes policy so analyst access is scoped per-tenant and per-investigation.

What does maintaining access during an active incident actually look like?

CSIRT holds pre-positioned SealedTunnels to crown jewel systems like backups, forensic archives, out-of-band management, and golden images, all running with inbound ports closed. When an incident is declared, responders connect immediately. Terniion simultaneously closes every other inbound path into the affected environment, containing the breach while keeping the response running.

Can we use Terniion during active incident response?

Yes. Policy changes in Commander take effect immediately. CSIRT can programmatically tighten access around compromised processes, preserve forensic state, and stage a controlled return to service as systems are cleared. No physical unplugging. No rebuilding networks.

The Bottom Line

Your clients expect you to see everything, respond without hesitation, and never become the breach that starts with you. That's the SOC's job, and it's harder when your own tools are exposed and your response capability can be disrupted. **Terniion gives you a way to:**

- Maintain uninterrupted access to the environments you're defending, even when the attack is underway.
- Keep your detection and response infrastructure out of the attack surface while it watches everything.
- Isolate every tenant at the process level so one client's incident never reaches the next.
- Contain active breaches and stage recovery programmatically, without ripping out infrastructure.
- Extend genuine, deterministic protection to every client you serve.

When everything else is compromised, your SOC still has the access it needs, and the attacker has none.

Ready to see how Terniion enables your SOC to do its best work?
Request a briefing | See a live demo