CrowdStrike + Dispersive

Continuous Authorization and Real-Time Threat Containment

KEY BENEFITS

Prevent Insider & Impersonation Attacks
Detect and contain suspicious behavior across employees, contractors, and vendors.

Protect Sensitive Transactions
Enforce identity-aware access for high-value financial and customer data.

Real-Time Containment
Turn detection into immediate defense with automated isolation.

Adaptive Zero Trust
Extend Falcon protection with dynamic authorization throughout the user session.

Trusted Control
SOC and IT teams stay in command with whitelists, overrides, and full audit trails.

Executive Summary

CrowdStrike and Dispersive have partnered to close the gap between threat detection and network response. The Dispersive Continuous Trust Authorization Network for Falcon integration extends CrowdStrike Falcon® endpoint and identity protection into the network layer using Dispersive Stealth Networking's adaptive, identity-aware networking.

By uniting device, identity, and network intelligence, the solution delivers continuous authorization, Patient Zero isolation, and real-time containment, stopping threats before they spread.

The Challenge

Detection is fast, but containment is not.

- SOC teams still rely on manual isolation workflows that take minutes or hours.
- High-risk endpoints remain connected during response delays.
- Impersonation and insider threats often bypass endpoint-only controls.
- SOAR playbooks are brittle and require heavy customization.

The result: increased risk of lateral movement, data exfiltration, and costly breaches.

The Solution

The CrowdStrike–Dispersive integration automates network response based on real-time device and identity risk scores.

- **Continuous Monitoring –** Device and identity risk signals from Falcon are continuously evaluated.
- **Adaptive Enforcement –** Dispersive dynamically adjusts network access policies using "maximum risk wins" logic.
- **Patient Zero Isolation –** High-risk endpoints are segmented or isolated instantly; trusted endpoints remain connected.
- **Zero Trust in Action –** Access is continuously verified, not just at login.

This closes the critical gap between detection and response, turning automated containment into a practical, trusted reality.

Customer Spotlight

New American Funding (NAF) is piloting the integration to protect against impersonation-based attacks and secure sensitive financial operations.

"With Dispersive and CrowdStrike deployed together, we gain the ability to see and act on user and device risk in real time. We can now provide risk-based access to network resources based on zero trust principles. It's a powerful competitive advantage for us in both security and trust."

Jeff Farinich, SVP Technology & CISO
New American Funding

Benefits of Dispersive Stealth Networking

The Dispersive Advantage

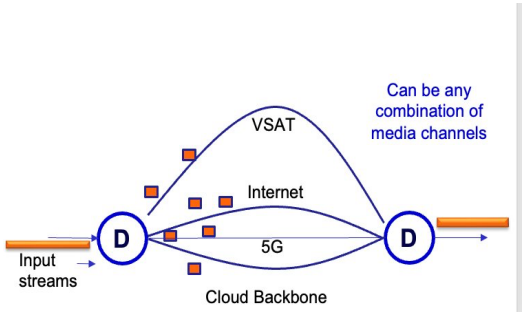
The integration unites endpoint, identity, and network intelligence to contain threats before they spread. Patient zero isolation proactively identifies and isolates risky behavior at the first sign of compromise.

With on-demand endpoint isolation, SOC teams can instantly segment or disconnect devices showing elevated risk.

Dynamic authorization ensures access rights continuously adjust in real time, while granular policy enforcement applies attribute- and score-based rules to protect sensitive networks, applications, and services.

Together, these capabilities deliver faster containment, stronger Zero Trust enforcement, and reduced operational risk.

Dispersive doesn't just protect your network, we hide it. Our quantum-resilient architecture encrypts, scatters, and obfuscates data-in-motion, making interception and reconstruction infeasible – quantum-ready, military-proven.

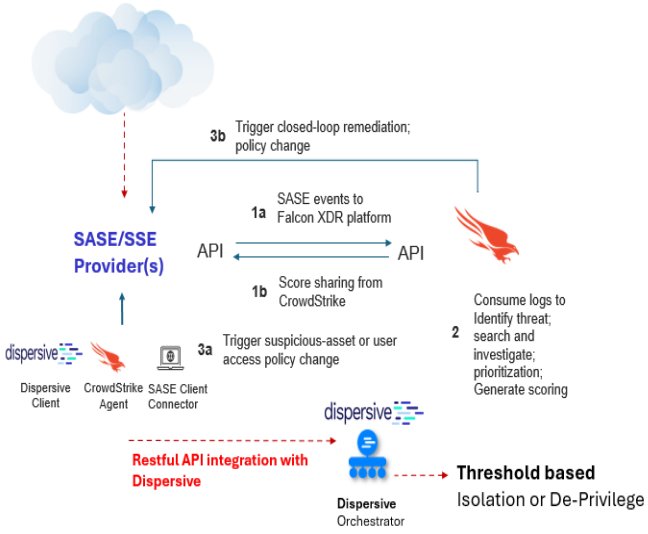


Dispersive's Secure Multi-Channel, Multi-Path Technology

CrowdStrike + Dispersive set a new standard for continuous authorization and real-time containment.

- **SOC Analysts:** Reduce mean time to containment with automation that is visible, explainable, and reversible.
- **IT Administrators:** Gain visibility, whitelists, and control to ensure security automation never disrupts critical systems.
- **Enterprises:** Reduce breach risk, lower incident costs, and strengthen customer trust.

Accelerate Investigation and Response with Dispersive + Falcon XDR & SASE



How it works

CrowdStrike Falcon XDR consumes SASE context for telemetry correlation, opening rich potential for threat investigation and triaging, scoring consumed by Dispersive

Orchestrated cross-platform remediation triggered by newly identified threats based on scoring

Dynamic access policy enforcement to manage device and user risk

Benefits to Customer

Full spectrum visibility and response with telemetry from endpoint, network to cloud applications, everywhere

Context sharing maximizes cross-platform effectiveness and speed

About the Technology

Dispersive Stealth Networking delivers military-grade quantum-ready networking that makes enterprise communications and data-in-motion invisible, resilient, and secure by design.
Learn more: www.dispersive.io