



Dynamic, Intelligence-Aware Zero Trust Access

AppGate ZTNA integrates with CrowdStrike Falcon to close the gap between detection and enforcement

The Problem

Every organization faces the same fundamental challenge: securing access without slowing down the business. As enterprise environments grow more distributed and adversaries more sophisticated, the gap between detecting a threat and acting on it has become one of the most exploitable vulnerabilities in modern security architecture.

Most access tools were built around a static model: verify identity at the perimeter, then trust the session. That assumption no longer holds. Device posture degrades mid-session. Credentials get compromised. Threats move laterally before anyone intervenes. Security teams can see the risk in their detection tools, but access controls don't respond until a human does, creating a window attackers know how to use.

The result is a structural problem: the tools responsible for detecting risk and the tools responsible for enforcing access don't talk to each other in real time. Closing that gap requires more than better visibility. It requires access enforcement that responds to risk as it happens, without disrupting users or requiring manual intervention at every decision point.

The Solution

AppGate ZTNA delivers Zero Trust access control that responds to the actual security state of your environment—not the state it was in when a session began. Unlike traditional ZTNA platforms that make a binary allow/deny decision at login, AppGate ZTNA continuously evaluates and enforces policy throughout the session, dynamically adjusting entitlements as risk signals change, without disrupting legitimate users or triggering broad network shutdowns.

What makes this integration distinct is the signal quality driving those decisions. AppGate ZTNA natively ingests two complementary CrowdStrike Falcon® capabilities to power real-time policy enforcement:

- **AppGate Insights for Falcon** surfaces AppGate ZTNA's access telemetry, session context, and Zero Trust posture data directly inside the CrowdStrike console, giving security operations center (SOC) teams a unified view of identity, device, and access risk without leaving their existing workflow.
- **AppGate ZTA Score Integration** ingests CrowdStrike Falcon's continuously updated Zero Trust Assessment score, translating live endpoint telemetry into automated access decisions. When Falcon detects degraded device posture, AppGate ZTNA restricts access in real time. When the device recovers, access is restored—no tickets, no manual intervention, no delay.

CrowdStrike is the authoritative risk and detection signal. AppGate ZTNA is the enforcement layer that acts on it, extending the value of existing Falcon investments directly into access control.

Risk-Adaptive Access: Falcon ZTA + AppGate ZTNA

AppGate ZTNA ingests Falcon ZTA scores and evaluates them against policy thresholds configured for each application or resource group throughout active sessions, not only at login. High-risk conditions trigger immediate restriction of sensitive application access. Mid-range conditions can require step-up multi-factor authentication (MFA). Score recovery automatically restores access without manual intervention.

Unlike basic agent checks, AppGate ZTNA's risk engine validates both the authenticity of the Falcon agent and the device's actual security posture, preventing attackers from spoofing processes or exploiting misregistered tenants. A compromised device loses access to mission-critical applications within seconds of a ZTA score change, regardless of when the user originally authenticated.



BENEFITS

Improve security posture

Extend conditional access to compliant devices with continuously updated Falcon ZTA risk scores applied throughout each session.

Streamline incident response

Detection-driven enforcement triggers immediate access changes within the AppGate ZTNA platform, closing the gap between detection and containment.

Simplify administration

Automate high-confidence enforcement with Fusion SOAR playbooks while preserving full manual control for complex decisions.

Unified SOC visibility

The AppGate Insights for Falcon panel surfaces active sessions, entitlements and policy context inside the CrowdStrike Falcon console—no platform switching required.

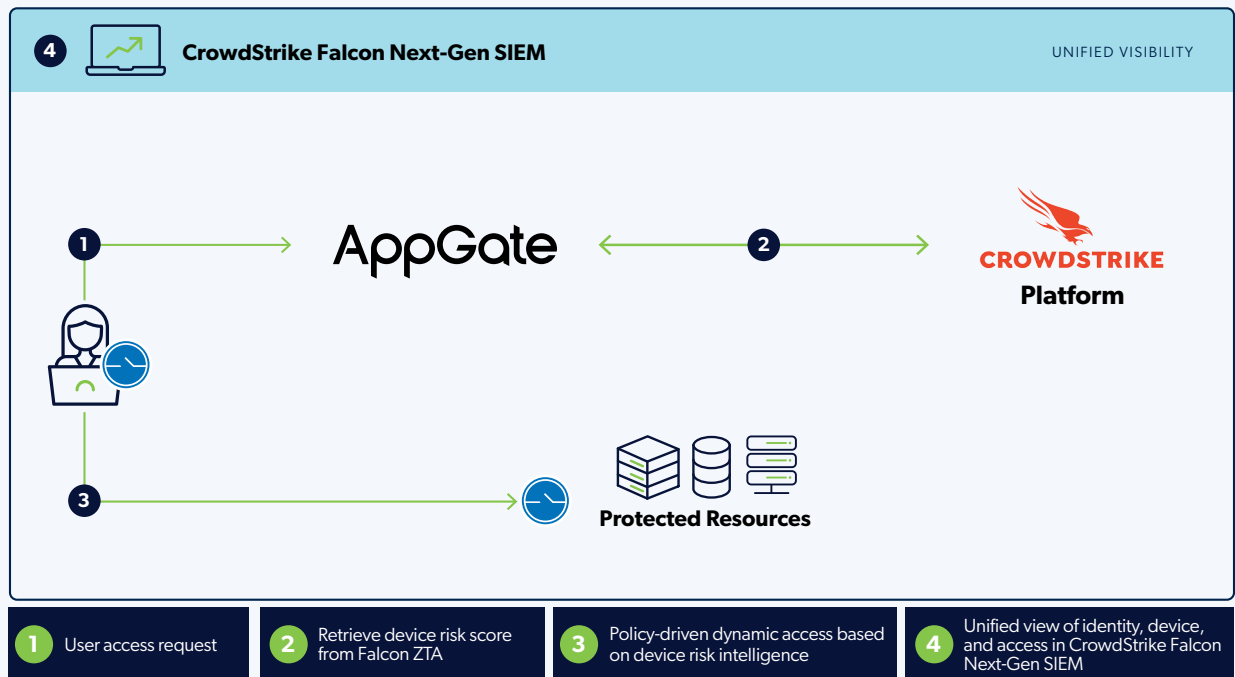
Granular enforcement

Block specific high-value applications, require step-up MFA for lower-risk resources, or grant temporary forensic access without broad network shutdowns.

Detection-Driven Enforcement: Falcon Next-Gen SIEM + AppGate ZTNA

The Falcon Next-Gen SIEM integration extends the joint solution in two meaningful ways: it connects detection events directly to access enforcement, and it surfaces AppGate ZTNA's full access context inside the CrowdStrike Falcon console, giving SOC analysts a unified view of identity, entitlements and policy without leaving the platform. Rather than waiting for a ZTA score threshold, a specific detection event or Fusion workflow can trigger an immediate access change in AppGate ZTNA, such as quarantining a user, removing entitlements, restricting access to high-value applications, or granting narrowly scoped forensic access. Foundry apps surface active sessions, entitlement profiles, policy impact and blast-radius analysis alongside Falcon telemetry in a single view, enabling more precise and confident response actions at machine speed.

AppGate also contributes rich context back into the security operations workflow via Foundry apps. Analysts see active sessions, entitlement profiles and policy impact alongside Falcon telemetry in a single view, without requiring a new platform. Blast-radius analysis for proposed policy changes and IP-to-access-path tracing reduce investigation time from hours to minutes, enabling more precise and confident response actions.



AppGate ZTNA and the CrowdStrike Falcon platform exchange real-time device risk intelligence to enforce dynamic, policy-driven access to protected resources — all monitored within the CrowdStrike Falcon Next-Gen SIEM.

The Bottom Line

Zero Trust only works if detection and enforcement operate as one system. AppGate and CrowdStrike make that operational, connecting Falcon's risk intelligence and detection capabilities directly to dynamic access enforcement, with full, built-in SOC visibility. The result is access that responds to risk in real time, response actions that are more precise, and a security posture that protects the business without getting in the way of it.

About CrowdStrike

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform delivers hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com.

About AppGate

AppGate secures an organization's most valuable assets with its Zero Trust Network Access (ZTNA) Platform. It's the leading ZTNA platform for enterprise IT, OT and AI protection. AppGate is the only direct-routed ZTNA solution built for peak performance, data sovereignty and seamless interoperability. AppGate safeguards enterprises and government agencies worldwide. Learn more at appgate.com.