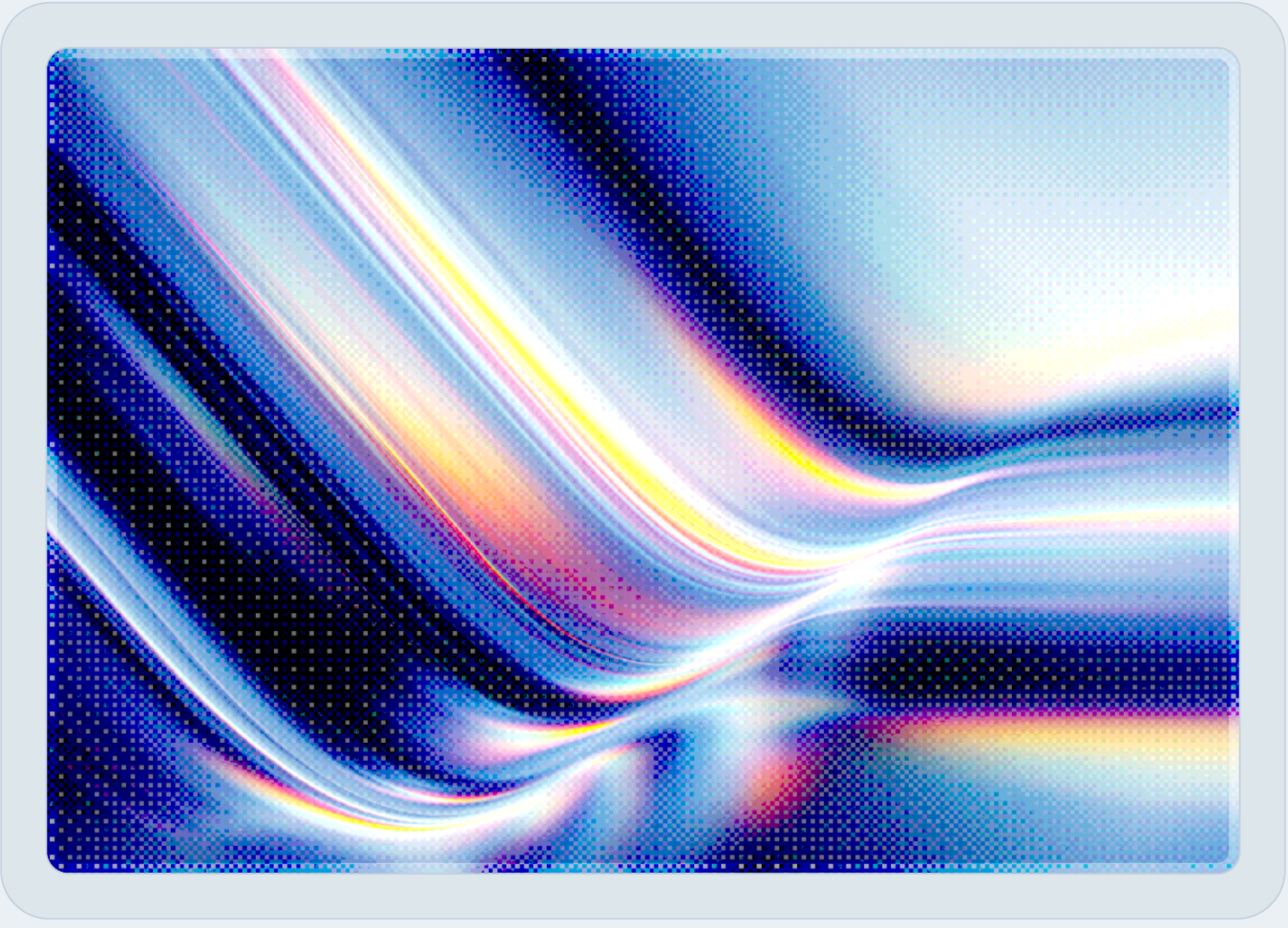
CSAI Foundation | Cloud Security Alliance

One Vendor, Two Control Planes: CrowdStrike–Zscaler Correlated-Failure Risk

Security Implications and Guidance for Consolidated Endpoint and Zero Trust Stacks

2026-11-26

AI-assisted Rapid Research



CSAI | CSA cloud security alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

On November 23, 2026, CrowdStrike announced a definitive agreement to acquire Zscaler in an all-stock transaction valued at approximately $43.9 billion. The deal is expected to close in the second half of CrowdStrike's fiscal year 2028, subject to Zscaler shareholder and regulatory approval [1][2]. CrowdStrike frames the combination as owning "the two most important control points": the Falcon sensor on every endpoint and the Zero Trust Exchange on every user, agent, and application connection. It describes the goal as "a single control plane" [1]. For customers that run both products, endpoint protection and network access enforcement would then sit with a single vendor's engineering, release, and administrative organization.

The central risk is correlated failure. Today these two layers are operated by separate companies with separate release pipelines and administrative planes, so they largely fail independently and each can partly compensate when the other is down, although existing posture-sharing integrations already couple them for some joint customers [3]. One owner, one data layer, and one release pipeline raise the chance that a single defective update, compromised administrative plane, or vendor-wide incident takes out both layers at the same time. The July 2024 Falcon content update incident, which took down an estimated 8.5 million Windows devices according to Microsoft, shows how far one vendor's defect can spread when its software runs with high privilege across a large installed base [4][5].

The companies will operate independently until closing [1]. Because CrowdStrike's fiscal 2028 begins in February 2027 [2], a second-half close implies roughly August 2027 to January 2028. Assuming the deal closes on the announced schedule, organizations have perhaps 9 to 14 months before operational integration can begin. That window is the time to map dependencies, document fail-open and fail-closed behavior, build break-glass access paths that do not depend on either vendor, and set contract terms.

Background

CrowdStrike's announcement describes the transaction as bringing "network security and Zero Trust to the Falcon platform." Each Zscaler share converts into 1.135 CrowdStrike shares, a premium of roughly 34% to Zscaler's closing price on November 20, 2026. After closing, existing CrowdStrike shareholders would own about 84.1% of the combined company [1][2]. The announcement projects more than $10 billion in combined annual recurring revenue at close and approximately $500 million in run-rate cost

synergies within 18 to 24 months. It also notes that the two companies already share more than 2,000 customers across 16 product integrations [1]. Zscaler founder Jay Chaudhry will continue to lead the Zscaler business and join CrowdStrike's board [1]. The Register called it the largest cybersecurity acquisition on record, surpassing Google's $32 billion purchase of Wiz [5].

The strategy is explicitly about convergence. Under the heading "One Platform, One Data Layer, One Flex Contract," the announcement says device and network telemetry will feed into Falcon Next-Gen SIEM as a single data set. That data set will also train CrowdStrike's security models, and Zscaler products will be sold through the Falcon Flex licensing contract [1]. CEO George Kurtz described the result as "cybersecurity's operating system: a single control plane to deploy AI, control AI" [1]. The announcement contains no specific commitment to merge the Falcon sensor with Zscaler Client Connector or to unify the two consoles. The roadmap language is still broad, and post-close architecture decisions have not been disclosed.

Reaction has focused mostly on price and lock-in. The Register quoted system administrators worried about cost increases and a "forced move to Falcon." It also observed that the July 2024 incident gave IT departments "a rather painful lesson in the risks of relying heavily on a single technology supplier" [5]. Coverage by the Associated Press and trade outlets centered on deal terms and the AI security rationale [2][3]. This note sets the commercial questions aside and examines the operational resilience question: what changes when the two most privileged enforcement points in an enterprise environment come under common ownership?

Security Analysis

The analysis below proceeds in three steps. It first describes how the two control points fail today, then sets out the mechanisms through which common ownership could correlate those failures, and finally places the transaction in the context of wider market consolidation and regulatory attention to concentration risk.

Two Control Points with Different Failure Modes

Endpoint detection and response and cloud-delivered security service edge (SSE) fail in different ways, and their independence is a large part of the defense-in-depth value of running both. The Falcon sensor runs on the host with kernel-level privilege. CrowdStrike's root cause analysis of the July 19, 2024 incident traced the crash to a Channel File 291 content update in which the new template type defined 21 input fields while the sensor code supplied only 20 [6][7]. CrowdStrike's preliminary post-incident review

further explained that a bug in the Content Validator allowed the problematic content to pass validation [8]. Because the sensor operates in kernel mode on Windows, the result was a system crash rather than a degraded security function, and many affected machines needed hands-on remediation.

Zscaler's Zero Trust Exchange fails differently. Client Connector steers traffic to a cloud enforcement point. If that cloud is unreachable or impaired, endpoints either lose connectivity, when configured to fail closed under strict enforcement, or lose inspection, when configured to fail open [9]. Zscaler's own continuity guidance acknowledges that even a service with a 99.999% uptime commitment "doesn't eliminate the need for a plan." It warns that "the instinct to route around security is dangerous," and promotes a per-customer Business Continuity Cloud with an isolated data plane and control plane as the fallback [10]. In both architectures, the vendor's operational behavior becomes part of the customer's availability profile.

The table below summarizes the two failure profiles and how integration under a single owner could couple them.

Dimension	Falcon endpoint sensor	Zscaler Zero Trust Exchange	Coupling risk after integration
Enforcement location	Host, kernel and user mode	Cloud proxy and broker, plus endpoint client	Shared endpoint footprint if agents converge
Dominant failure mode	Host crash or degraded protection from a defective content or sensor update [6]	Loss of connectivity (fail-closed) or loss of inspection (fail-open) during cloud impairment [9]	A single defect or compromise affects both detection and access
Update mechanism	Vendor-pushed sensor and Rapid Response Content [7]	Vendor-operated cloud policy and client releases	One release organization and possibly one content pipeline
Administrative plane	Falcon console	Zscaler admin portals	A "single control plane" concentrates privileged administrative access [1]

Dimension	Falcon endpoint sensor	Zscaler Zero Trust Exchange	Coupling risk after integration
Existing cross-dependency	Falcon device posture shared with Zscaler [3]	Zscaler access decisions consume posture signals [3]	Posture-signal failure can cascade into access denial or over-permissive access

How Common Ownership Correlates Failure

Common ownership does not by itself make either product less reliable. The risk comes from removing independence between the two layers. Four mechanisms deserve attention, and each is an inference about integration choices that have not yet been made.

The first is a shared release pipeline. The announcement's emphasis on one data layer and one roadmap suggests that detection content, AI-model output, and policy logic may eventually flow to both enforcement points through common tooling [1]. If one validation process gates content for both the sensor and the network policy engine, a single validation defect of the Channel File 291 kind could reach both surfaces in the same deployment window. The 2024 incident showed how fast a vendor-pushed update can propagate, and a coupled pipeline would turn an endpoint outage into an endpoint-and-access outage.

The second is a concentrated administrative plane. A "single control plane" that can change endpoint containment and network access policy is operationally convenient, but it is also a high-value target. A compromise of administrative credentials, an insider action, or a misconfiguration pushed from that plane could isolate hosts from the network and change access policy at once. Today the two administrative planes are separate systems with separate role models. An adversary would typically need access to both, unless both are reachable through a shared identity provider or administrator account, which is itself a concentration organizations should review.

The third is signal cascade, and it already exists in partnership form. Existing integrations let Falcon's device risk assessment trigger reassessment of Zscaler access [3]. This design is consistent with the zero trust practice of continuously evaluating device posture. It also means that an endpoint telemetry failure feeds directly into access decisions. If posture signals become unavailable, the policy engine must either deny access to every device it cannot score or grant access without a posture check. Organizations should verify and document which of the two outcomes their configuration produces.

The fourth is recovery dependency. Recovery from the July 2024 incident often required physical or remote console access and BitLocker recovery keys, and CrowdStrike published dedicated BitLocker recovery procedures for multiple management environments [11]. Where the remote access path that IT staff use to reach systems runs through the same SSE platform, as it can in Zscaler Private Access deployments, one vendor operates both the failed control and the access path needed to fix it. In that situation, recovery runbooks that look independent on paper may share a hidden single point of failure.

Why This Matters Beyond One Transaction

The CrowdStrike–Zscaler deal is the largest example of a wider pattern. The market is consolidating endpoint, network, identity, data, and AI security into a small number of platforms, absorbing pure-play capabilities and concentrating telemetry and policy into a larger blast radius. The pattern matters because security tools hold unusual privilege. They run in the kernel, sit inline on all traffic, and control access, so their failures behave differently from failures of ordinary business applications. CSA's recent research note on the November 12, 2026 Microsoft 365 outage examined a real case of this dynamic, in which a security control failed together with the platform it protects under a single vendor [12].

Regulators and platform owners have started responding to this class of risk. After the 2024 incident, Microsoft launched the Windows Resiliency Initiative and is building a Windows endpoint security platform that lets protection products run outside kernel mode [13][14]. Microsoft is working with endpoint vendors including CrowdStrike, and its Microsoft Virus Initiative 3.0 requires participating vendors to follow safe deployment practices [13][15]. In the European Union, the Digital Operational Resilience Act requires financial entities to manage ICT concentration risk. In November 2025 the European Supervisory Authorities published their first list of designated critical ICT third-party providers, selected partly on concentration of reliance and substitutability [16][17]. This note makes no claim about whether either company is or will be designated. However, financial entities with a combined CrowdStrike–Zscaler dependency may need to reflect a more concentrated group-level exposure in their registers of information, depending on how the combined entity is structured.

The trade-off should be stated fairly. Consolidation has real security benefits: fewer integration seams, correlated telemetry for detection, faster response when endpoint and network signals agree, and a smaller administrative workload. Those benefits are likely to be real. The point of this analysis is that they come with a correlated-failure cost, and organizations should make that trade deliberately rather than inherit it through license bundling.

Recommendations

The recommendations follow the deal timeline. Immediate actions establish what an organization actually depends on, pre-close mitigations use the negotiating window before integration commitments harden, and strategic considerations address vendor diversity as a long-term architecture decision.

Immediate Actions (Next 30–60 Days)

Organizations should start by finding out where they actually depend on both vendors. Inventory every place Falcon and Zscaler are deployed together. Record which business services depend on each layer, and identify any integration in which one product's signal drives the other's enforcement decision. For each such integration, document what happens when the upstream signal is missing: deny, allow, or degrade. Test that behavior in a controlled setting rather than assuming it.

Next, confirm that emergency access is truly independent. Break-glass administrative access, BitLocker or other disk-encryption recovery keys, and remote management paths for critical systems should not require a working Falcon sensor or a reachable Zscaler cloud. Where they do, establish an alternate path, such as an out-of-band management network, an alternate remote-access mechanism with tightly restricted scope, or offline key escrow. Verify the path with a live drill.

Finally, review the content-update controls that are already available. Following the 2024 incident, CrowdStrike committed to giving customers more control over how Rapid Response Content is deployed and to staged deployment rings [7]. Organizations should confirm these controls are configured, placing a canary population ahead of production and crown-jewel systems, and should apply comparable staging to Zscaler client releases.

Short-Term Mitigations (Before Deal Close)

The pre-close period is the best time to negotiate, because integration commitments have not yet hardened. When renewing or extending either contract, organizations should seek written commitments in the four areas summarized below.

Area	Commitment to seek
Release separation	Independent change-management and validation gates for endpoint content and network policy releases, so a defect in one pipeline cannot automatically reach the other

Area	Commitment to seek
Administrative separation	Separable administrative roles and credentials for endpoint and network functions, even within a unified console, with step-up approval for cross-domain actions such as mass host isolation combined with access-policy changes
Interoperability	Continued support for running Zscaler with a different endpoint vendor, or Falcon with a different SSE vendor, without commercial penalty
Exit and portability	Exit and data-portability terms, including telemetry export in open formats, negotiated before deeper platform integration

Security teams should also run a tabletop exercise built on a "both layers down" scenario, in which a defective vendor update crashes a share of endpoints while access-policy enforcement is impaired at the same time. The exercise should measure time to restore Minimum Viable Service Levels for critical business services and should show whether the recovery runbooks depend on the failed vendor. Organizations that rely heavily on Zscaler should consider whether an isolated continuity option such as Zscaler's Business Continuity Cloud is appropriate. Because that option is operated by the same vendor, it should be evaluated as protection against a cloud outage, not against a vendor-level defect or compromise [10].

Strategic Considerations

Over the longer term, organizations should treat security-vendor diversity as an explicit architecture decision rather than an accident of purchasing. For the highest-consequence environments, such as payment systems, operational technology gateways, and clinical systems, a heterogeneous design that pairs the endpoint layer with a network enforcement layer from another vendor may be worth its added integration and operating cost. For general enterprise environments, a single-vendor stack may be acceptable when it is combined with tested independent recovery paths and contractual separation of release pipelines.

Security policy should also be expressed in vendor-neutral terms, through control frameworks, open identity standards, and portable telemetry schemas, so that substitution stays feasible if the combined platform's reliability or pricing changes. Finally, boards and risk committees should get visibility into security-tool concentration as a category of third-party risk. Regulated financial entities should make sure their DORA registers of information and concentration-risk assessments reflect the combined dependency once the transaction closes [16].

CSA Resource Alignment

CSA's **Zero Trust Guidance for Achieving Operational Resilience** (April 2026) is the most directly relevant published artifact [18]. It addresses single points of failure and risk aggregation, describing aggregation as occurring "when too many dependencies, risks, or critical services are concentrated with one or a limited number of suppliers." It advises organizations to ask of each third party, "Can we operate without them?" The guidance also calls for systems that are "loosely coupled, fault tolerant, globally distributed, and provider-diverse," and for break-glass access that is "independent of primary identity providers where possible." The recommendations in this note apply those principles to a specific case: the concentration of zero trust enforcement and endpoint protection in a single provider. The guidance's Business Impact Analysis methodology and its concept of Minimum Viable Service Levels are well suited to the "both layers down" tabletop recommended above.

CSA's **AI Controls Matrix (AICM) v1.1** supplies the control vocabulary for putting these recommendations into practice [19]. The Business Continuity Management and Operational Resilience (BCR) domain covers continuity planning, testing, and resilience of critical services. The Supply Chain Management, Transparency, and Accountability (STA) domain covers third-party responsibilities, supplier assessment, and contractual safeguards. Because CrowdStrike explicitly positions the combined platform as a control plane for AI agents and AI safety [1], organizations deploying agentic AI should treat the platform as both a security provider and an AI supply chain dependency within AICM's shared-responsibility model.

CSA's **Zero Trust Program Management Guidance** (September 2026) is a complement [20]. It helps organizations govern a zero trust program as a strategy rather than a product, which is the posture needed to avoid treating any single vendor's platform as equivalent to zero trust itself. CSA's recent research notes on correlated failure, including **When the Assistant and the Alarm Go Dark Together** [12] and **Five Days, Four Platforms: Correlated Outages and AI Agent Concentration** [21], examine the same concentration dynamic through recent real-world outages. The recommendations here, including anchoring policy to frameworks, negotiating exit terms before deepening integration, and keeping telemetry portable, are consistent with that line of work.

References

[1] CrowdStrike. "CrowdStrike to Acquire Zscaler, Bringing Network Security and Zero Trust to the Falcon Platform." Exhibit 99.1, Form 8-K, U.S. Securities and Exchange Commission, November 23, 2026.

[2] Associated Press. "CrowdStrike to acquire Zscaler in $44B deal that would create a cybersecurity giant." ABC News, November 23, 2026.

[3] Guru Baran. "CrowdStrike to Acquire Zscaler in Massive $43.9 Billion Cybersecurity Deal." Cyber Security News, November 23, 2026.

[4] David Weston. "Helping our customers through the CrowdStrike outage." Microsoft Official Blog, July 20, 2024.

[5] Carly Page. "CrowdStrike splashes $44B on Zscaler, customers brace for the bill." The Register, November 24, 2026.

[6] CrowdStrike. "Channel File 291 Incident: Root Cause Analysis is Available." CrowdStrike Blog, August 6, 2024.

[7] CrowdStrike. "Executive Summary: Root Cause Analysis, Channel File 291." CrowdStrike, August 2024.

[8] CrowdStrike. "Falcon Content Update Preliminary Post Incident Report." CrowdStrike Blog, July 24, 2024.

[9] Zscaler. "Configuring Fail-Open Settings for Zscaler Client Connector." Zscaler Help Center, accessed November 26, 2026.

[10] Lidor Pergament and Stephanie Rullo. "Lessons from Recent Outages: How Smart Enterprises Stay Ready." Zscaler Blog, September 21, 2026.

[11] CrowdStrike. "Remediation and Guidance Hub: Channel File 291 Incident." CrowdStrike, July 2024.

[12] Cloud Security Alliance. "When the Assistant and the Alarm Go Dark Together." CSA Labs, November 14, 2026.

[13] Microsoft. "Windows Resiliency Initiative." Microsoft, accessed November 26, 2026.

[14] Help Net Security. "Microsoft plans to limit security products' access to Windows kernel mode." Help Net Security, November 19, 2024.

[15] Eduard Kovacs. "Microsoft to Preview New Windows Endpoint Security Platform After CrowdStrike Outage." SecurityWeek, June 27, 2025.

[16] European Securities and Markets Authority. "European Supervisory Authorities designate critical ICT third-party providers." ESMA, November 18, 2025.

[17] Morgan Lewis. "DORA: EU Regulators Announce List of Critical ICT Third-Party Providers." Sourcing@MorganLewis, November 18, 2025.

[18] Cloud Security Alliance. "Zero Trust Guidance for Achieving Operational Resilience." CSA, April 6, 2026.

[19] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." CSA, June 22, 2026.

[20] Cloud Security Alliance. "Zero Trust Program Management Guidance." CSA, September 8, 2026.

[21] Cloud Security Alliance. "Five Days, Four Platforms: Correlated Outages and AI Agent Concentration." CSA Labs, November 2026.