
 USE CASE BRIEF

Maintaining Cybersecurity During Mergers And Acquisitions (M&A)

M&A is a Cybersecurity Event, Not Just a Financial One

Mergers and acquisitions run on tight, fixed timelines, and cybersecurity has traditionally been squeezed into that timeline as a tick-the-box exercise. That approach no longer holds: cybersecurity is now a primary driver of deal valuations and, increasingly, a deal-killer.

AI is a major reason why. AI-powered attacks can find and chain together vulnerabilities far faster than any human team, and that speed is most dangerous exactly when two companies' networks, identities, and systems are being pulled together, the moment reachability spikes and visibility is lowest. Against attacks that move this fast, resilience matters more than prevention: being breach ready means planning as though a breach is inevitable and building the ability to contain it before it spreads.

Every M&A transaction needs to be breach ready before the two companies are interconnected. That makes reachability, not patch percentage, the real question: which critical systems, at the data center, on the factory floor, in the cloud, or with remote users and suppliers, are reachable from every point of access, or from an AI tool that's already inside?

Plan a merger around what's likely true, not what you hope is true. Somewhere in the combined environment, assume: unpatched zero-days and compromised credentials already exist; some assets, endpoints, or service accounts fall short of baseline or carry excess privilege; legacy systems won't modernize on the deal timeline; and an attacker may already be present, with lateral-movement paths nobody can yet see.

Patch management alone can't close that gap on a merger timeline. The practical starting point is foundational microsegmentation that spans data centers, offices, remote users, and cloud instances, and integrates with the tools already in place, so that even before every vulnerability is found and fixed, a compromise stays compromise-sized instead of becoming a breach of the entire combined enterprise.

THE CORE CHALLENGES

Cybersecurity Friction Points in M&A

Every merger creates the same handful of cybersecurity problems, regardless of industry or deal size:



The attack surface expands overnight, before anyone can see it. Users, identities, endpoints, applications, cloud environments, and networks get folded into one ecosystem on the deal's timeline, not on security's. A previously isolated, compromised endpoint can suddenly reach corporate identity services, shared file systems, privileged administration systems, and production environments, all at once.



The acquiring company inherits trust it never mapped. VPN connections, service accounts, legacy applications, cloud identities, and AI agents that were fine in isolation can become tunnels, footholds, and lateral movement paths the moment two networks touch. Nobody finds out until it's tested by an attacker.



Layoffs create a narrow window for insider risk. Mergers routinely trigger workforce reductions, and departing employees often retain access for days or weeks after their roles end. Some of that access was never fully inventoried in the first place, making it hard to know who still has a way in, and harder still to revoke it everywhere at once.



Tooling gets cluttered instead of consolidated. Under deal pressure, due diligence often becomes a checklist exercise: inventorying each side's tools and policies rather than architecting how they'll actually work together. The result is a duplicated, inconsistent stack and no clear answer when the board asks if the risk is covered.



The two companies don't agree on what "secure" means. What one organization treats as a baseline control, the other may never have considered, and that mismatch doesn't surface until systems are already interconnected.



The deal clock doesn't wait for security to catch up. Full asset discovery, risk assessment, and remediation take time that a sign-to-close timeline rarely allows, leaving leadership to choose between slowing the deal or accepting unknown risk.

During a merger, Xshield is built to answer exactly the kind of pressure a deal creates

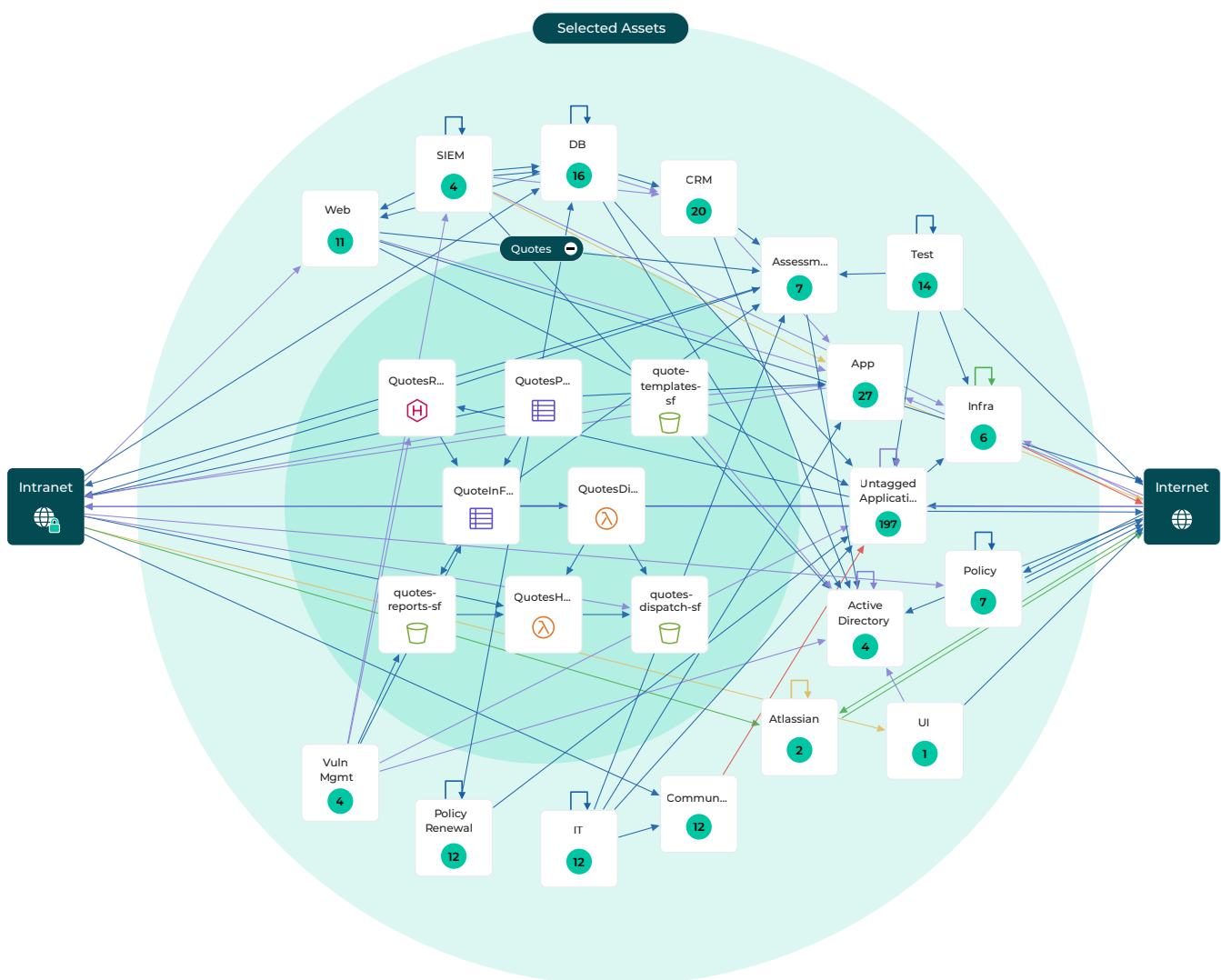
Xshield lets you connect two environments quickly, without connecting their risks. It gives you real-time visibility into what's actually talking to what, enforces access by identity rather than inherited network trust, and applies one consistent policy standard across IT, cloud, containers, and OT/IoT, regardless of which company's environment it came from. Because it deploys through multiple enforcement methods, including its own lightweight agent, EDR agents already in place, or fully agentless modes, it can be stood up without new hardware or a lengthy re-architecture project. Its AI-assisted policy generation means segmentation can happen in days, not months, buying time to patch without waiting for patching to finish first. It also lets teams query the environment in plain English, with live situational awareness of MITRE ATT&CK techniques and CISA Known Exploited Vulnerabilities, replacing another dashboard to learn with a direct answer to "are we exposed, and where."

Patching faster, auditing more thoroughly, adding another point tool, or leaning on contractual protections won't solve these problems. None of them stop lateral movement or revoke a stolen credential once an attacker is inside. What solves them is architecture: a way to see and control what's connected to what, regardless of whose environment it came from.

THE COLORTOKENS APPROACH

Security Starts with Visibility

ColorTokens Xshield Enterprise Microsegmentation Platform™ gives security teams **visibility and control** over how systems, identities, and workloads communicate across the enterprise, and enforces zero Trust policy at every point of connection.



— USE CASE DEEP DIVES

Scenario A - Sell-Side: Divesting a Business Unit

Selling a business unit means proving to a buyer that what they're inheriting is clean, with evidence, not assurances. The unit has to separate cleanly from the parent company's identities, data, and network paths, all while staying operational and sellable.



Buyer-ready evidence, not verbal assurance. Xshield generates a documented map of every workload, identity, and connection tied to the unit being divested; evidence you can hand directly to a buyer's diligence team or auditors, instead of asking them to take isolation on faith.



A measurable isolation report. Xshield shows you concrete numbers: what percentage of the unit's workloads carry enforced communication policies, how many paths back into the parent network have been closed, turning "it's isolated" into something the buyer can verify line by line.



Identities and data separated, not just networks. Xshield extends segregation beyond network paths to the accounts, credentials, and data tied to the divested unit, so nothing that belongs to the sale still reaches back into what the parent retains.



Departing employees lose access everywhere, immediately. When roles are eliminated as part of the separation, Xshield revokes that identity's access across every system it touched in one action, closing the insider-risk window instead of relying on each team to manually track down every account.



Separation without a network overhaul. Because Xshield enforces through agent, agentless, and native modes, you get clean isolation without new hardware or a redesign project, on whatever mix of systems the unit runs.



No disruption to the business you're selling. Xshield secures the unit while it keeps running normally throughout. The sale process itself never becomes the thing that interrupts operations.

The result: a faster, more confident close, backed by documentation that holds up under the buyer's own scrutiny, not just the seller's word, with AI-assisted policy generation compressing the separation timeline itself, not just the paperwork behind it.

USE CASE DEEP DIVES

Scenario B - Buy-Side: Integrating an Acquired Business

Acquiring a company means inheriting a network you don't yet know. The instinct is to connect everything on day one so people can be productive immediately, but a fully open network is exactly how a contained problem becomes an enterprise-wide one.



Access that expands as trust is proven. Xshield lets you broaden connectivity for the newly acquired environment incrementally, based on verified behavior, rather than granting full network reach on close.



Protection using what's already there. Xshield enforces Zero Trust policy through its own agent, existing EDR tools, or agentless modes, with unified visualization and policy management across IT, IoT, containers, and multi-cloud. This means day-one protection across whatever infrastructure the acquired company brings, without new software or re-architecting the acquired company's infrastructure.



One security standard, applied immediately. Whatever stack the acquired company was running, Xshield extends your policy standard across it from day one, closing the gap where the two companies never agreed on what "secure" means.



AI agents don't get a pass. Newly acquired AI agents and automated workflows are governed by the same least-privilege policy as human users, closing off a lateral-movement path most integration plans don't even check.



Containment built in. If something in the newly acquired environment is compromised, it stays confined to its microsegment instead of reaching your critical systems.

The result: an acquired environment that's productive fast, without becoming the entry point that puts the parent company's most critical systems at risk.

The Payoff - Deal Confidence, Not Just a Checkbox

AI-driven attacks are reshaping the threat landscape faster than most integration timelines can adapt to. Every day a merger runs on unmapped trust and unresolved visibility is a day an attacker, human or automated, has more surface to work with and needs less time to exploit it. What matters isn't whether a deal will attract that kind of attention; it's whether the combined business can absorb a compromise without the deal, the brand, or the board's confidence taking the hit.

Clean segmentation and documented isolation turn that uncertainty into evidence: audit-ready proof for diligence and reps-and-warranties conversations, reduced risk exposure on both sides of the table, and one less reason a deal slips past its target close date. Microsegmentation has become the go-to approach for exactly this kind of deal-time assurance, and ColorTokens has been independently recognized by Forrester as a Leader in the category, one of the best in the business at delivering it.

Deal timelines rarely leave room to wait for a perfect security posture. The organizations that plan for breach readiness before two networks connect are the ones that carry deal confidence into every stage of the transaction, and beyond it.

About ColorTokens:

ColorTokens is a leading provider of enterprise microsegmentation solutions that operationalize breach readiness across hybrid, cloud, and OT environments. By proactively minimizing lateral movement risk and reducing attack surface, ColorTokens enables organizations to operate in a continuous state of breach readiness — before, during, and after an incident. The Xshield™ platform visualizes traffic between workloads, OT/IoT/IoMT devices, and users, enforcing adaptive micro-perimeters that dynamically limit blast radius and accelerate response. Recognized as a Leader in The Forrester Wave™: Microsegmentation Solutions (Q3 2024) and the GigaOm Radar for Microsegmentation v3 (March 2026), ColorTokens helps enterprises strengthen operational resilience and maintain security posture as threats evolve. For more information, visit www.colortokens.com.