TRINITY CYBER

Mergers and Acquisition

Accelerating and Derisking M&A

DICEMBER 2025

240.654.1451
info@trinitycyber.com

Merger and acquisition (M&A) decision-makers must consider the cybersecurity risk that acquisitions and related data breaches pose to critical business assets and functions. The loss of intellectual property (IP), service operations, and valuable customer data could result in diminished revenues, profits, market value, market share, and brand reputation. M&A is a massive undertaking that often changes the shape of an organization and positions it for growth. Few organizations have enough time to adequately review a target company's security posture, and deals occasionally fall through because the security risk is too great. Addressing the cybersecurity risks and integrating the companies' security postures are essential to achieving positive, risk-reduced M&A results.

Some key security considerations when executing M&A include:

Device Security

Ensure that all devices are equipped with up-to-date security software and patches.

Security Policies and Procedures

Develop and communicate unified security policies and procedures for the newly merged organization.

Network Security

The acquired company's network must be considered completely untrusted until proven otherwise.

Compliance

Ensure compliance with relevant data protection laws and regulations.

Holdings

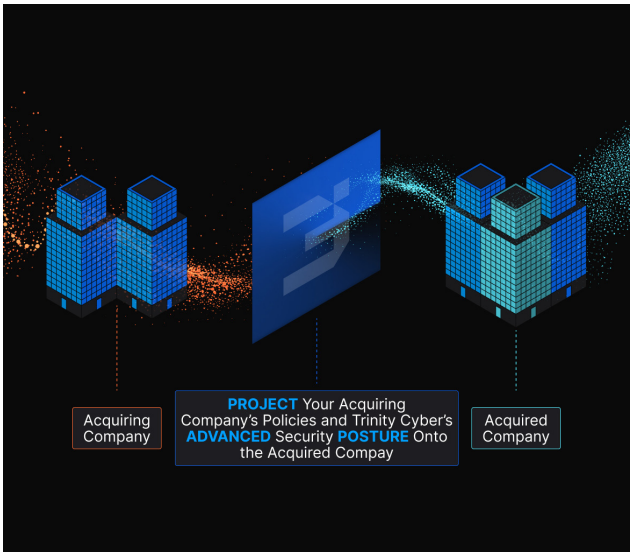
All files in all holdings must be checked for malware or compromise before any integration takes place.

Continuous Monitoring and Improvement

Implement continuous monitoring of the threat landscape and security controls to detect and respond to emerging insider and external threats.

Trinity Cyber helps rapidly addresses each of these considerations, reducing effort and risk while accelerating integration. Our Full Content Inspection (FCI) technology and expert Threat Analysis team actively protects your M&A assets (and your company from those assets) though an easy-to-employ subscription model.

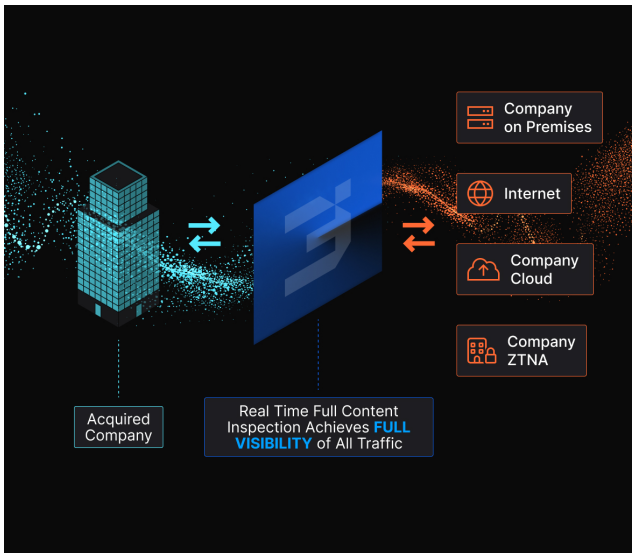
Often, the cyber risk associated with the acquired company's assets is poorly understood or the IT staff is behind on closing known vulnerabilities, leaving security gaps within the acquired company's enterprise. Their network and all the devices in it must be considered untrusted until proven otherwise. Trinity Cyber mitigates the vulnerabilities resulting from unpatched systems within minutes by applying rules within our inline security service. These rules proactively remove the ability for vulnerabilities to be exploited, providing critical time for patching. Systems are virtually patched with Trinity Cyber, allowing the M&A team to focus on integration activities.



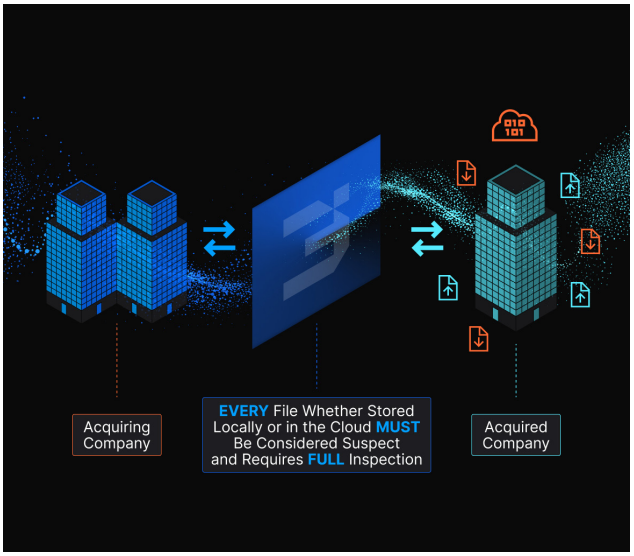
As companies combine, there are different security policies between them. With its flexible rule language, Trinity Cyber can "mimic" and project the security posture of the purchasing company and enforce that posture on the assets of the acquired company (through a variety of internet connection types). For customers who take advantage of Trinity Cyber's internet gateway feature, the company offers a Cloud Firewall service with standard L3 (source/destination IP) and L4 (stateful port and protocol inspection) functionality. Between Trinity Cyber's unique threat protection capabilities and traditional Cloud Firewall policies, Trinity Cyber provides a single policy enforcement point that harmonizes security policy enforcement between companies, the internet, and cloud services, simplifying security operations and administration while reducing cybersecurity risk.

Full visibility of the acquired company's network traffic is essential.

Trinity Cyber offers comprehensive packet capture (PCAP) of all network traffic, not just the published events of prevented threats. The acquiring digital forensics and incident response (DFIR) teams get SSL-decrypted PCAP at their fingertips to check for the presence of insider and external threats. Trinity Cyber's integrated PCAP solution enables the security team to use standard Berkeley Packet Filtering (BPF) syntax during a rolling 72-hour window, enabling search and retrieve SSL-decrypted packet captures to support analysis and investigations. The acquiring security team gets a complete picture, analyzing even the most subtle threats and anomalies. The IT team will also appreciate the ability to use SSL-decrypted PCAP to troubleshoot technology integration.



Finally, every file in the acquired company's holding must be considered suspect. Files downloaded from untrusted sources may include malware and may reside on company file systems. Trinity Cyber provides a powerful file inspection capability that accepts drag-and-drop files in its customer portal as well as bulk, batch uploading of an unlimited number of files through our API. WIth both methods, Trinity Cyber's Full Content Inspection (FCI) puts the power of advanced file analytics at your fingertips. FCI delivers an immediate maliciousness verdict while portraying a breakout of all file components and their content. Security teams can also use it to aid in threat intelligence and incident response. The context-rich visibility is critical in protecting the acquiring company's valuable assets while providing essential risk information to the M&A team.



Trinity Cyber's FCI capability is delivered as a service to provide simpler onboarding, on-demand scalability, easy subscription terms, and a comprehensive dashboard with contextual data and analytic tools at your fingertips. Trinity Cyber delivers unparalleled threat protection, provides full visibility into all network activity, and checks every file to achieve trust - all without performing lengthy security assessments and traditional security integrations.

M&A presents many challenges that can diminish revenues, profits, market value, market share, and brand reputation. Accelerating technology integration and reducing cyber security risk improves success. Trinity Cyber accelerates integration, reduces cybersecurity costs, and reduces risk so companies can move past the obstacles and focus on operating as a combined organization, delivering real financial results.

The Trinity Cyber Core Technology

Trinity Cyber's award-winning capability delivers unparalleled deep, content based, full session inspection and real-time active network defense – all operated for you and tuned to your M&A conditions by an expert team of seasoned professionals.

In an industry ecosystem overoptimized to support alert aggregation and incident response, Trinity Cyber's patented FCI technology empowers a wide spectrum of real-time corrective actions – each meticulously crafted to match a CVE, threat actor group, ransomware gang, and entire families of threats. No alerts to aggregate. Near zero false positives.

When the technology encounters a threat on your assets' network traffic - which it does more accurately and with a more enduring approach than competing solutions on the market - it mitigates that threat on the wire, seamlessly and in real-time while delivering a context-rich notification to your security team. With average inspection and remediation processing times of less than 1ms, neither your acquisition end users, nor the opposition, will even know the technology is there.

Trinity Cyber offers a wide range of connection options to cover any internet access, internet gateway, and ZTNA configuration. As soon as your acquisition is connected, you can project your security posture immediately. All internet content is actively inspected to protect against the ever-evolving threat landscape while conforming to your policies. The technology is backed by a suite of additional cybersecurity services like content-based threat hunting and emerging threat analysis – all made better through the patented technology. Trinity Cyber operates on your behalf, tunes its systems to address your security concerns, defends you against the latest threats, manages all the systems, and provides you with a context-rich, interactive customer portal where you can see and drill into each and every threat stopped by Trinity Cyber. Each event is fully triaged so that your security team can rest assured that you are protected. You can also depend upon notifications in the portal being legitimate, with more than 99.99% accuracy and a de-facto elimination of false positives to enable strong threat protection that does not impede real-time business operations.

About Trinity Cyber

Trinity Cyber's Full Content Inspection (FCI is a high-availability cybersecurity countermeasure capability that is delivered as a service. You get clean traffic and less noise. It radically reduces risk and false positives. Trinity Cyber catches threats others miss and replaces costly SWG, NGFW, and IPS licenses.

Contact us today at info@trinitycyber.com to learn more.