Reach

Navigating the Unknowns in M&A Cybersecurity

When larger companies acquire smaller ones, they inherit not only their assets but also their cybersecurity infrastructures. This transfer often occurs with limited visibility into the actual security posture of the acquired company. Despite assurances, the acquirer frequently remains in the dark about both the external exposures and the efficacy of the security tooling the smaller company claims to have in place.

Common Challenges

Inadequate Visibility into Security Configurations

Acquiring companies often receive claims from the target company about their protective security products for the network, devices, identity and data. However, the acquirer has no immediate way to verify whether these tools are configured optimally or if they are effectively safeguarding the target company's digital assets. This is often the case in the pre-acquisition and even due diligence phases where Attack Surface Management and Vulnerability Management tools are used to assess risk.

Uncertainty and Risk in Security Inheritance

Post-acquisition, the acquiring company might work towards a limited integration because the acquired entity will continue standalone, or more commonly seek a tighter integration challenged by security measures previously described by the target company that are inadequate, outdated, or misconfigured, leaving sensitive data and systems vulnerable. This risk is compounded by the lack of transparency and the often superficial security assessments completed in the due diligence phase.

Resource-Intensive Security Audits

Although there is typically a budget allocated for auditing the cybersecurity posture of an acquisition target, the process is cumbersome and resource-intensive. It involves extensive consulting hours, manual interviews, documentation reviews, and more. This not only lengthens the timeline to close the deal but also increases the costs and complexity of the acquisition.

Solving the Challenge is within Reach

Reach transforms your security landscape by not only identifying gaps but also helping you effectively navigate the 'last mile' of cybersecurity. With a risk-based approach, Reach provides the context needed to optimize the M&A workflow to get the best security possible from the tools you already own. During the integration phase of an acquisition, Reach is particularly helpful in advising the team whether immediate integration is necessary or can be deferred. This guidance is based on a thorough understanding of the risks, threats facing the combined entity, and the capabilities licensed in their security tools.

Drive Outcomes with Reach

Drive Decisions with Data

Reach analyzes the security tooling and configurations of acquisition targets to provide comprehensive, data-driven reports to prioritize the level of effort, risk, and need associated with integrating an M&A. Reach is particularly helpful in advising the team whether immediate integration is necessary or can be deferred.

Reduce Acquisition Costs

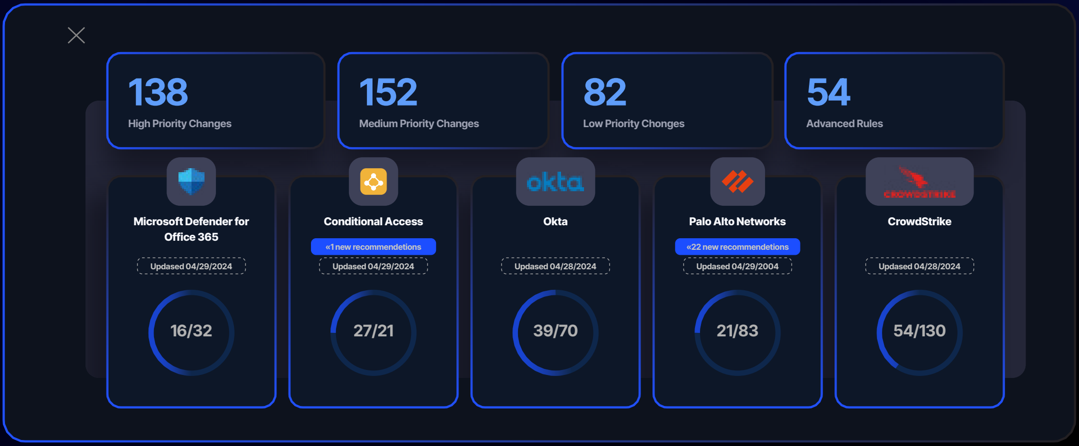
By automating and streamlining the security evaluation process, Reach reduces the need for expensive consultancy services and extensive manual labor, making the integration more cost-effective.

Unite Security Postures

Reach empowers the acquirer to manage and monitor the security postures of multiple acquisitions from a single platform, ensuring uniform security practices across all entities.

sales@reach.security
reach.security/connect

Tool Optimization Made Simple with Reach Security



Reach Capability	Description
Optimized Utilization of Licensed Capabilities	Reach conducts a thorough analysis of the cybersecurity infrastructure and tooling that an acquisition target has in place, offering actionable recommendations to optimize security integrations. This includes evaluating the configuration and effectiveness of existing security measures, regardless of their specific type, such network, devices, identity and data. Reach identifies the capabilities available with these tools and assesses their alignment with the acquirer's security standards, ensuring that investments in cybersecurity are fully capitalized and effectively safeguard both entities.
One-Click Automation and Deployment Guides	Reach simplifies the integration of security systems during mergers and acquisitions through one-click automation and provides comprehensive deployment guides and configurators. This capability allows security teams from both the acquiring and acquired companies to efficiently align and implement optimized security measures. It ensures that security enhancements are not only recommended but also promptly and precisely executed across the combined enterprise, fostering a seamless transition and strong security posture.

Proven Results: Amplifying Security with Reach

Reach Security is revolutionizing the cybersecurity landscape by empowering organizations to maximize the ROI of their existing security products. With a focus on optimizing what organizations already own rather than adding complexity with new tools, Reach Security is committed to simplifying cybersecurity, reducing operational costs, and enhancing protection against evolving threats. Founded by cybersecurity experts with venture-backing from leading investors and cybersecurity luminaries, Reach Security is setting a new standard for cybersecurity efficiency and effectiveness.

Get Started!

Automatically find and fix security blind spots. To learn more about Reach, visit:

reach.security/try-reach

sales@reach.security
reach.security/connect