Solution Brief

Netskope Security Cloud: Solutions for Secure M&A

Mergers and acquisitions are high-stakes transactions. To optimize the chance of success, companies have begun to rely on their cybersecurity teams to protect the applications and data of all companies involved, both before and after the deal closes. They also need to ensure that operational and technological integrations proceed smoothly. This is a challenge in the on-premises world, certainly. That challenge is exacerbated as companies move more and more crucial workloads to the cloud and must account for managed and unmanaged (also known as shadow) IT. The following matrix identifies key considerations for five phases of M&A and how to leverage the Netskope Security Cloud to strengthen and streamline security processes throughout the deal process.

PHASE	KEY CONSIDERATIONS / THREATS	NETSKOPE SOLUTIONS AND OFFERINGS
Due Diligence Phase: All teams should engage security early in the process of M&A. The security team's key responsibility during M&A due diligence is to evaluate the degree to which the merger or acquisition would impact the acquiring company's security posture and/or the probability they have already been compromised. They need to develop visibility into the target business's attack surfaces, both on-premises and in the cloud. Then, they need to perform a comprehensive risk assessment that identifies security gaps and quantifies the risk associated with each gap. The goal should be to ensure that business decision-makers are fully aware of what they're buying before they close the deal, as well as the risks they will be assuming.	• Can you ensure sensitive data is properly handled during the due diligence process? • Can you monitor data transfers between acquirer and target and detect threats, mitigate vulnerabilities, and ensure both companies are aware of attempted attacks?	• Netskope Risk Insights to provide inventory and risk of SaaS applications in use • Netskope CloudXD Inline controls CASB Instance Awareness • Netskope Advanced Analytics for specific user behaviors • Netskope SWG threat monitoring

PHASE	KEY CONSIDERATIONS / THREATS	NETSKOPE SOLUTIONS AND OFFERINGS
Integration Planning Phase and Public Announcements: Throughout the due diligence process, companies typically keep the prospective transaction under wraps. Once they publicly announce a deal, that announcement introduces a number of new security challenges. One is that attackers frequently target companies approaching an M&A transaction because they know that staffing, processes, and data management are in transition. They try to take advantage of the fluidity of the environment to phish the acquiring company, the target, or both. It's incumbent upon both security teams to intensify their monitoring of data movement throughout the companies' on-premises and cloud infrastructures, including all endpoints, email, and storage.	• Can you determine and execute the appropriate response to cloud threats based on the acquiring company's enforcement policies? • Can you effectively monitor internal user behavior and identify relevant changes in that behavior to avoid inappropriate data transfers? • Can you identify high-risk behavior by employees?	• Netskope DLP API for data at rest • Netskope Next Gen SWG for cloud threats • Netskope CloudXD CASB for policy enforcement • Netskope UEBA for high-risk user behavior monitoring • Netskope Advanced Analytics for risk management
Merger or Acquisition Close-Day 1: As soon as the deal has closed, on day one of the merger or acquisition, the IT team faces a new set of pressures. They need to integrate systems and open up access to applications and data so that people on both sides of the transaction can begin to operate as a unified entity. But providing access, via the internet, to core systems like financial or HR applications would create significant risk. The security teams must make sure all data remains protected, even as they support immediate integration. This is the time for doubling down on determining risk assessment.	• Can you limit access to cloud services and applications to avoid data leaks and close security gaps during the initial integration phase? • Can you provide visibility into and data protection for SD-WAN connections? • Can you make a comprehensive assessment of the target's threat monitoring capabilities, including granular movement of data to or from the target's cloud solutions? • Do you have visibility into data at rest? • Can you identify and manage third party integrations and detect problematic activities by target-company users? • Do you have full insight into SaaS application configurations? • Can you continuously monitor IaaS implementations in public clouds (AWS, Azure, GCP)? • Can you monitor the target organization's cloud presence? • Can you efficiently control users' access to sensitive data and private resources? • Can you provide seamless network integration to access to private applications for both parties?	• Netskope SaaS Security Posture Management for SaaS application configuration monitoring • Netskope Next Gen SWG Cloud Confidence Indicator for third-party risk • Netskope CSPM to manage public cloud implementations • Netskope Cloud XD CASB and DLP to manage access to sensitive data in-motion and at-rest • Netskope Private Access to handle duplicate IP addresses in networks • Netskope Private Access to provide zero trust to private applications

PHASE	KEY CONSIDERATIONS / THREATS	NETSKOPE SOLUTIONS AND OFFERINGS
Longer-Term Integration, including Insider Threat Mitigation: Once a merger or acquisition has survived day one and week one, the security teams need to plan and implement a secure and efficiently integrated architecture. They will undoubtedly find a great deal of duplication in technologies and teams, with many instances of the two businesses using different approaches to perform the same function. Instance awareness is a key feature needed to distinguish between the two companies' technology implementations (e.g. O365).	• Can you effectively analyze TCO of different options for secure applications and data across the newly combined company? • Can you effectively monitor staff and contractors for behavior changes that might indicate an increased security risk? • Can you continue to perform routine checks on all of the combined company's public cloud applications? • Can you determine where you have duplicate technologies implemented? • Can you provide real-time notice to users of a technology that is being sunset?	• Netskope UEBA to monitor changes in behavior of users • Netskope Advanced Analytics to identify and manage duplicate technologies • Netskope CloudXD for real time notification of sunset technology • Netskope CSPM to perform routine checks on public cloud implementations