netskope

SOLUTION BRIEF

Smoothing Out M&A

How Netskope solutions such as Next Gen SWG and ZTNA can strengthen, and streamline, security processes on both sides during the deal process.

EXECUTIVE SUMMARY

Mergers and acquisitions are high-stakes transactions. To optimize the chance of success, companies have begun to rely on their cybersecurity teams to protect both companies' applications and data, 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 SECURITY CHALLENGE IN M&A

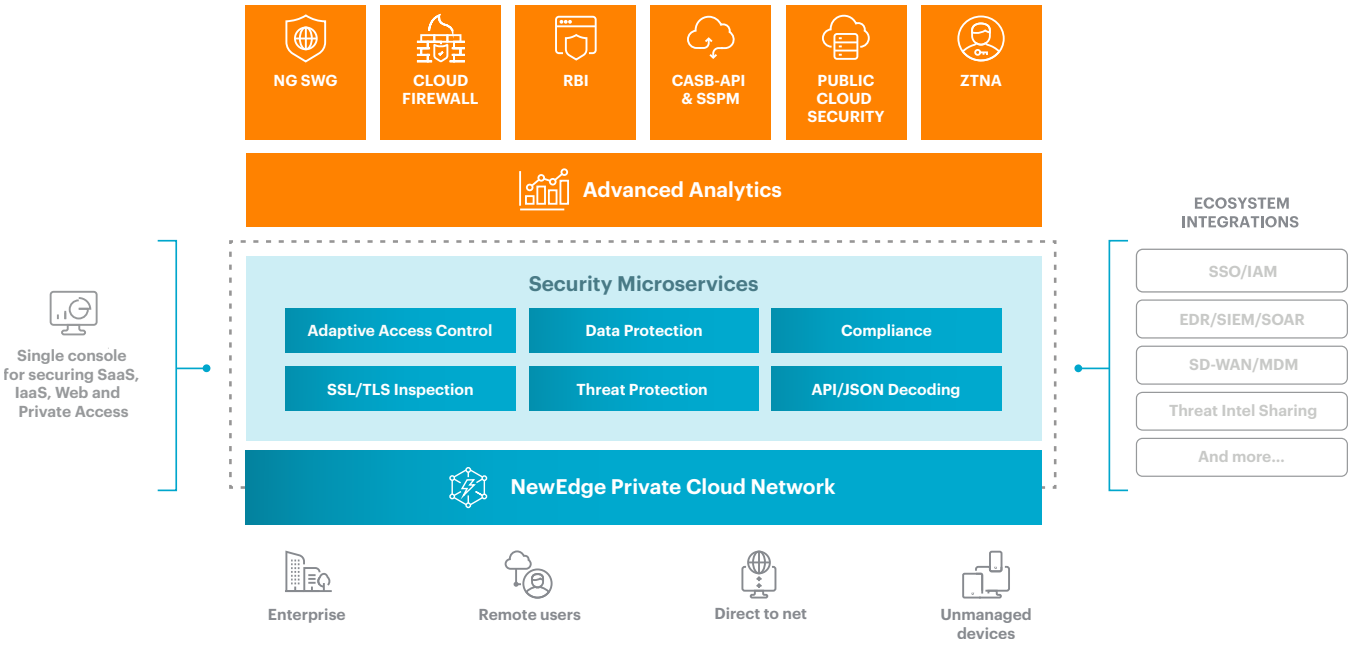
When business executives enter into a merger or acquisition, they need the IT team to provide each company with selective and secure access to the other business's key systems. They also expect security staff to keep data and applications secure at a time when both organizations' technology environments are changing rapidly.

The acquiring company's security team needs to integrate the target's diverse applications, data, and users into the acquirer's internal infrastructure and policies. They need visibility into the target companies' full IT estate, including unmanaged SaaS applications (also known as shadow IT). They need to understand the vulnerabilities of the target organization and determine the degree to which the impending deal might increase their own company's cybersecurity risk.

As the deal progresses, they need to minimize the friction that technology issues may create as the organizations combine. They also must ensure that employees on both sides of the transaction—who might be concerned about the future of their jobs—refrain from actions that might put sensitive data at risk.

These responsibilities may seem overwhelming for security teams that are stretched thin just managing their usual day-to-day duties. On top of that, the security team's approach to merger and acquisition (M&A) security must be dynamic. Rather than a set-and-forget proposition, security activities must evolve through each phase of the transaction, including if the transaction ends up not closing.

Netskope solutions, which are captured as an architecture in the graphic on page 2, can help ease the burden of M&A security management in many key ways, starting with the due diligence process.



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. They need to develop visibility into all 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 are buying and the risks they will be assuming before they close the deal.

Netskope technologies enhance this process in several ways. Netskope Risk Insights is purpose-built to identify all the Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and web use within an organization. Its discovery capability performs in-line asset and user inventories, then displays high-level results in a comprehensive risk dashboard. The solution also offers granular visibility into users' online activities and enables security teams to run ad hoc queries looking for specific behaviors. An acquiring company's security team should take advantage of these capabilities to inventory the target's applications and users.

The security team's approach to merger and acquisition (M&A) security must be dynamic. Rather than a set-and-forget proposition, security activities must evolve through each phase of the transaction, including if the transaction ends up not closing.

Another risk concern during M&A due diligence is that sensitive data might be compromised as it's accessed by one organization or the other. Business groups' evaluation of prospective merger or acquisition targets necessarily involves access to sensitive data, such as financial results and forecasts, customer lists, and employees' personal information. Executives need this information to assess the target and determine whether to move forward with the deal. But if this data is handled improperly, the due diligence process itself will present a serious security risk.

Netskope's Next Generation Secure Web Gateway (Next Gen SWG) detects threats to data in transit. Security teams engaged in M&A due diligence should use the solution to monitor data transfers between

acquirer and target, to lock down any detected threats, mitigate any vulnerabilities, and ensure that the companies are aware of attempted attacks.

Along the same lines, the acquirer should start keeping tabs on the target's security environment as soon as possible. The security team should leverage both Netskope Next Gen SWG and the user and entity behavior analytics (UEBA) feature within Netskope Threat Protection to monitor the target organization's cloud presence. These solutions can look for command-and-control actions arising within any solution used by the target company, as well as anomalous user or application behaviors. (Note that these uses also significantly enhance Phases 3 and 4.)

Early detection of an attack or breach could save the acquirer from unwittingly taking on a material liability that might be both expensive and accompanied by bad press. In one example from a few years ago, Verizon reduced its offer for Yahoo by $350 million after discovering two massive data breaches in Yahoo's recent past that had not been fully disclosed. There are many other examples, not often reported in the press.

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, it 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.

The acquirer's security team should review the target's threat-monitoring capabilities (if that wasn't part of the due diligence process). Netskope Next Gen SWG can provide visibility into the movement of data to or from the target's cloud solutions. It can also provide visibility into data at rest, via its API interface.

Netskope Cloud XD is another useful tool for security teams preparing for a merger or acquisition. The solution combines big data analytics with data loss prevention (DLP) capabilities to achieve real-time threat protection for cloud-based data and applications. Because it was built specifically to secure cloud solutions, Cloud XD is uniquely equipped to determine and execute the appropriate response to cloud threats based on the acquiring company's enforcement policies. This can improve both companies' security if threats increase in the lead-up to the deal close.

In addition to external threats, security teams need to pay attention to both organizations' employees. Staff will inevitably worry about what the impending transaction means for them. Some may begin moving sensitive information onto personal devices or private cloud storage. They may simply be looking for evidence of accomplishments should they seek a new job. But inappropriate data transfers make information more vulnerable to threat actors.

Security teams should use the Netskope Next Gen SWG to monitor internal users' behavior, and should use Netskope Threat Protection's UEBA feature to identify relevant changes in user behavior. These solutions can also monitor activity on online job boards, as well as search dark-web sites for both companies' brand names, to gauge specific employees' likelihood to pose a data security threat.

Security teams can also use Netskope Advanced Analytics to identify high-risk behaviors by employees of either organization. What are the differences between the two companies' cloud policies, and what needs to change to bring them into parity? Will operational integration require data to be moved

across national borders in a way that violates either country's regulations? The custom big-data analytics available in Netskope Advanced Analytics streamlines answering questions like these, and many more.

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. The security teams can leverage Netskope Next Gen SWG's granular controls (including CASB capability) to limit access to cloud services and applications. These controls are key during the period of initial integration, when data leaks are likely and known security gaps are closed only as overtaxed staff get to them, in order of priority. The UEBA feature within Netskope Threat Protection will again be important to monitor the overall cloud environment.

Integrating Netskope Next Gen SWG into the target organization's SD-WAN implementations can provide visibility and data protection for those connections. The security teams can also use Netskope Next Gen SWG to give the acquiring company's employees and managers secure access to the different instances of the target's various SaaS applications. And they can identify and manage third-party integrations using Netskope Risk Insights. Adding passive threat hunting services available through the Netskope Cloud Threat Exchange to the mix can further enhance an acquirer's ability to detect problematic activities by target-company users.

Meanwhile, Netskope SaaS Security Posture Management (SSPM) simplifies enforcement of SaaS security policies throughout the combined company and gives security teams insight into the configuration of SaaS applications. And Netskope Cloud Security Posture Management (CSPM) enables the security teams to implement continuous monitoring of IaaS implementations in public clouds including Google Cloud Platform (GCP), Amazon Web Services (AWS), and Microsoft Azure.

Finally—and crucially—throughout the integration, both teams should leverage cloud-delivered zero trust network access (ZTNA) capabilities to efficiently control users' access to sensitive data and private resources. Netskope Private Access provides ZTNA for any and all cloud-based resources. The solution grants users access to resources based both on their network location and on explicit but adaptive trust criteria that consider user identity, device identity, cyber hygiene, and other contextual data—all while avoiding the challenge of duplicate IP addresses that often occurs during the merger of two previously discrete networks. By granting users access to only those applications and data that they explicitly require, Netskope Private Access minimizes the risk of lateral movement should an attacker gain access to one part of the newly integrated network.

More than one in three executives say they have experienced data breaches that can be attributed to M&A activity during integration.

Nick Coleman, SecurityIntelligence

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. An early step in designing the combined infrastructure for the long-term should be to leverage Netskope Advanced Analytics to identify the cloud applications that each business group is currently using, the number of users accessing them, the sensitivity of the data, and the data movement that each system requires.

After compiling a comprehensive inventory, the security teams can analyze the total cost of ownership (TCO) of different options for securing applications and data across the combined company. Netskope offers a workshop to help customers understand the TCO of different cloud and network security controls. Companies can use the resulting TCO analysis to rationalize applications, eliminating redundancy and building efficiency into their infrastructure of the future.

At the same time, the security teams should continue to monitor both staff and contractors for behavior changes that might indicate an increased security risk. The insider threat is greater in a merger or acquisition that involves different geographic locations, cultures, security controls, and operating models. Netskope Private Access helps ensure, on an ongoing basis, that the only people accessing sensitive information are those who truly need access. The DLP capabilities in Netskope Next Gen SWG help prevent intellectual property and other valuable information from leaving the organization. And deploying Netskope CSPM on all the combined company's public cloud applications—including Google GCP, Amazon AWS, and Microsoft Azure—adds another layer of protection via routine checks and monitoring of the IaaS configurations.

INTEGRATED SOLUTION SUITE STREAMLINES EFFECTIVE M&A PROTECTION

Companies entering into a merger or acquisition need to keep all systems and data secure. Failing to do so could reduce, or even eliminate, the value of the M&A transaction. It's not uncommon for an acquirer to recognize a serious vulnerability or even a previous successful data breach only after the acquisition closes.

The acquiring company's cybersecurity team needs to be front and center throughout M&A due diligence, decision-making, and then integration. Managing these tasks efficiently requires a platform of integrated solutions that provide broad protection with efficient management.

Netskope's Security Cloud Platform is leading the way to safer M&A. **Contact Netskope to get started today.**