illumio

SOLUTION BRIEF

ENSURING SECURE MERGERS AND ACQUISITIONS WITH ILLUMIO

OVERVIEW

Mergers and Acquisitions (M&A) represent opportunities for companies to expand, enter new markets, benefit from synergies, and exploit economies of scale. A key M&A success metric for a board of directors is the speed at which target companies can be integrated in order to ensure the value of the transaction is realized while maintaining a seamless experience for employees and customers. This creates challenges for the respective IT organizations as they are tasked with speedy integration but often lack an accurate understanding of how the information systems work and communicate. Properly managing this **IT integration risk** is a fundamental pillar of any M&A strategy.

Many acquiring CISOs/CSOs also have concerns about the security risk posture of the target. They fear that the target company's assets represent a target-rich environment for a post-closing cyberattack or, worse still, that they may have already been compromised and that any breach would propagate through the acquirer's organization when IT assets are merged. This **cybersecurity risk** must be mitigated to ensure the transaction is able to deliver on its promise of long-term strategic value for the company.

This sets up a very complex situation as organizations must weigh:

- **Projected value of transaction:** the compelling business needs that bring the two entities together.
- **Integration velocity:** board-level visibility on how the integration is progressing.
- **Integration risk:** the fear of breaking production applications as they migrate.
- **Cybersecurity risk:** the fear of acquiring IT assets that are already compromised.

Illumio is foundational to the M&A strategy of some of the most acquisitive organizations in the world. These organizations typically follow a four-step process to:

1. Map application dependencies within the target's environment.
2. Build segmentation policy around the target's critical IT infrastructure, leveraging the application dependency map.
3. Migrate the target company's applications into their own infrastructure.
4. Protect their own infrastructure from the target company's servers and applications.

Through this process, both businesses continue to run disruption-free, enabling a seamless integration.

CHALLENGES

IT teams of acquiring companies have little to no control over the applications inherited through an acquisition, yet they are tasked with efficient and secure migration and integration, usually with tight deadlines. Acquired environments can contain a variety of platforms including a mix of operating systems running on bare-metal, various hypervisors, or in different cloud environments. While migration of well-understood applications can be a challenge, a bigger challenge is migrating unknown applications without compromising security or impacting services.

The following factors are challenges for acquiring companies:

Lack of visibility can add delays in migrating acquired assets. Without understanding how applications and workloads are connected and communicating, acquiring companies risk breaking applications and disrupting service during migration or while securing acquired applications.

Ensuring consistent security that meets the standards of the acquiring company can be a major challenge since the acquiring company cannot completely change their network or infrastructure to accommodate the acquisition target.

Application migration without compromising on security is the essence of a successful outcome. A migration without unplanned disruption to an application is difficult since modern applications are interdependent and may be fragile. Deadlines to migrate applications can add to the pressure of the project and the need to get things right without disrupting production services.

ILLUMIO SOLUTION

The Adaptive Security Platform® (ASP) enables live visualization of your application environment across data centers and clouds before migrating any applications. Illumio policies created before migration can be adapted to the new environment to ensure consistent security across the project. Illumio ASP visibility and micro-segmentation enforcement adapt to changes in your application environment in real time – whether that is the movement of workloads, changes to security policies, or unauthorized communications among your applications.

How Illumio Addresses Key M&A Challenges

The Illumination® **application dependency map** provides real-time insights to help acquiring companies visualize acquired applications and their workloads across all environments before migration. With understanding of application dependencies, teams can ensure the migration is efficient and application behavior is not disrupted. Illumination is also a key component in the process of defining micro-segmentation policy.

Policy Generator **automates segmentation policy creation** with optimized micro-segmentation policy that saves time, accelerates security workflows, and reduces the risk of human errors. Policies can be modeled and tested with visual confirmation of the impact to the application environment to ensure enforced policies don't break application functionality.

Illumio micro-segmentation policy can be enforced on any compute and across any infrastructure for **uniform segmentation policy** across all environments. Illumio decouples security from the network and the hypervisor, for the freedom to work with any combination of platforms (e.g., bare-metal, virtualized platforms, or containerized workloads) and infrastructure (e.g., private data centers and public/private/hybrid clouds).

Illumio ASP **adaptive micro-segmentation policy** adjusts to changes in the application environment – as applications move, so does security. This allows applications to be secured before migration and policy to automatically adjust post migration, maintaining consistent and continuous protection during the migration process.

USE CASE

Customer Challenge

A large SaaS provider acquired a smaller company and was tasked with migrating the acquired applications to the main data center. Migrating the 3,200 workloads that comprised the acquired company's applications required investigation of their applications and dependencies to ensure service was not disrupted. The acquiring team was also working under a tight deadline of under 180 days to complete migration and integration of the acquired applications.

The team lacked visibility into application dependencies to perform the migration with confidence and integrate the acquired application without disrupting service. In addition, the security policies that were in place were static and would not automatically adapt to the new environment after migration of the workloads.

Another major concern was the risk of customer and company data being compromised as the workloads would potentially be exposed for the duration of the migration project.

Illumio Benefits

With Illumio, the acquiring team was able to meet the deadline to migrate and integrate the acquired applications in well under 180 days. Visibility in Illumination was an important component of the solution – allowing the team to see dependencies across the application environment. This was key in understanding application and workload relationships to ensure migration without disruption. Illumination also helped the team set up security before migration to minimize the risk of exposing customer and company data. Micro-segmentation policy was established and adapted to the new environment post migration to ensure consistent security enforcement throughout the process. The acquiring company was able to substantially minimize the attack surface of the acquired environment by reducing the flows by 15x – from 1.2 million to 80,000 – with micro-segmentation policy.

ABOUT ILLUMIO

Illumio, the leader in micro-segmentation, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information about Illumio, visit www.illumio.com/what-we-do or follow @Illumio.

- Engage with Illumio on Twitter
- Follow Illumio on LinkedIn
- Like Illumio on Facebook
- Subscribe to the Illumio YouTube Channel

CONTACT US

For more information about Illumio ASP and how it can be used to achieve visibility behind the firewall, email us at illuminate@illumio.com or call 855-426-3983 to speak to an Illumio representative.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 www.illumio.com