TANIUM

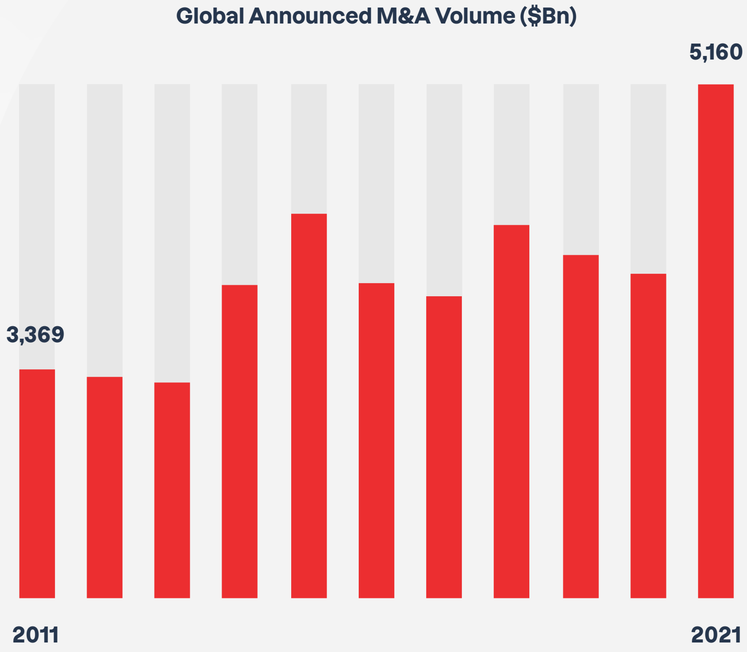
Managing M&A risk

How endpoint visibility can deliver critical advantages

Insight into IT risk can be overlooked — though it shouldn't be — when making acquisitions. That's why to manage cyber risk acquiring organizations need a rapid, accurate way to map all the endpoint assets in a target company.

In 2021, merger and acquisition (M&A) activity hit a record high of more than $5 trillion in global volume. While the market has certainly cooled in 2022, it remains on par with pre-pandemic levels — quite a feat at a time of business uncertainty and inflation. But when it comes to corporate deal-making, risk lurks around every corner. The potential for overpaying, miscalculating synergies and missing potentially serious deficiencies in a target company is high.

With so much at stake, accurate information is essential. But while plenty of focus is centered on gathering financials, reviewing contracts, picking through insurance details and more, gaining insight into IT risk may be put on the back burner. Acquiring organizations need a rapid, accurate way to assess and map all the endpoint assets in a target company, and then work quickly post-completion to assess and manage cyber risk.



The need for visibility

M&A deal volume may have fallen 12% year-on-year in early 2022, but the market remains bullish, driven according to McKinsey by cash-rich private equity firms sitting on trillions of dollars. Still, security and IT operations are a growing concern for those with money to spend. It's extremely rare for both sides of a deal to have similar standards for cybersecurity, asset management and key IT policies.

That disconnect can cause major problems down the road. Due diligence is a critical step — enabling acquiring firms to spot potential opportunities for cost savings and synergies, while also understanding how risky a company purchase may be.

> **If an acquirer cannot gain assurances around risk levels, it could theoretically call a deal off, or lower the acquisition price offer.**

Cyber risk transparency benefits both sides

If an acquirer cannot gain assurances around risk levels, it could theoretically call a deal off, or lower the acquisition price offer. If it presses on regardless, the organization may experience significant unforeseen problems trying to merge IT systems. Or it might unwittingly take on risk that erodes deal value over time — such as an undiscovered security breach that leads to customer class action suits, regulatory fines, and reputational damage.

These concerns are far from theoretical. In 2017, after the discovery of historic data breaches at Yahoo, Verizon lowered its offer price for the internet pioneer by $350M, or around 7% of deal size. Marriott International was not so lucky when it bought hotel giant Starwood. It wasn't until September 2018, two years after the acquisition and four years after the initial security breach, that an unauthorized intrusion was finally discovered. The breach turned out to be one of the biggest to date, impacting more than 380 million customers, and led to an £18.4m ($21M) fine from the UK's data protection regulator.

Getting due diligence right

In an ideal world, CIOs would be involved in M&A activity from the get-go, asking the right questions and providing counsel to the CEO and senior leadership team on whether to proceed with a target. Nevertheless, this isn't always the case. Such is the secrecy of deal-making that negotiations are usually limited to a handful of executives, leaving some bosses on the outside.

The best way CIOs can rectify this is to proactively educate senior executives about the importance of information security due diligence during M&A. If they succeed in embedding a security-by-design culture at the very top of the organization, those executives should be able to ask the right questions of targeted companies and judge their level of risk exposure early on. They may even be inclined to invite the CIO in to help.

> The best way CIOs can rectify this is to proactively educate senior executives about the importance of information security due diligence during M&A.

But for most organizations, however, the first critical point at which due diligence can be applied is after an acquisition has been announced. This is where the acquiring company must gather as much information as possible to better understand risk levels and opportunities for cost reduction and efficiencies. SOC 2 compliance would make things run more smoothly, providing useful insight into the level of security maturity at an acquired firm.

But more likely, the acquiring company's CIO will need to rely on its own processes. And they need accurate, current data on every endpoint in the corporate environment, plus granular detail on what software is running on each asset and where there are unpatched vulnerabilities and misconfigurations.

But that's much easier said than done. Most current tools on the market struggle to provide answers to these questions across the virtual machines, containers, cloud servers, home working laptops and office-based equipment that run the modern enterprise. Even if these tools can provide full coverage, they may take days or weeks to deliver results, by which time the information is out of date.

SOC 2 is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data. The standard is based on the following Trust Services Criteria: security, availability, processing integrity, confidentiality, privacy.

Managing post-deal risk

The second opportunity for the CIO is once contracts are signed. Now it's time to use a unified endpoint management platform to deliver a fast, accurate risk assessment of the acquired company's IT environment. By inventorying all hardware and software assets, they can develop a machine and license consolidation strategy, eliminating redundant or duplicate software. The same tools should also enable CIOs to distribute new applications to the acquired company, scan for unmanaged endpoints, find and remediate any problems, and enhance IT hygiene across the board.

Manage risk and increase business value during M&A with Tanium

M&A is a high-risk, high-pressure world. By prioritizing endpoint visibility and control at every stage of a deal, organizations stand the best chance of preserving business value, reducing cyber risk, and optimizing ROI. As we've already pointed out, acquiring companies face a long list of risks that must be assessed and carefully accounted for during due diligence: financial, litigation, intellectual property, and regulatory matters all represent potential inherited impact on a business.

When you buy a company, you buy its data

Today, disparate security and IT operations practices among companies represent a growing concern for acquiring corporations.

It's rare for both companies to have the same standards for cybersecurity, asset management, and IT policies, such as BYOD. In fact, unknown threats might already have infected an acquired company's endpoints — leaving companies exposed to future data compromise, fines, and loss of trust with customers.

Aligning IT operations and security functions of two companies is a massive task. The goals are generally universal: find synergies that drive cost reduction, while understanding and containing the acquired company's threat matrix.

> **Acquiring companies face a long list of risks that must be assessed and carefully accounted for during due diligence**

How Tanium can help

Tanium can help accelerate the due diligence process and reduce risk by rapidly deploying 10,000 endpoints per day on average. Tanium customers can ask simple or complex questions about the current or historical state of their networks, get fast responses from all their endpoints, and take action to secure and manage all their endpoints.

Organizations can use Tanium to:

Identify synergies and rationalize assets at the target company

Inventory hardware and software assets to drive machine and license consolidation strategy

Consolidate servers and ensure full server utilization

Distribute new software and required applications

Eliminate redundant point solutions and streamline infrastructure

Assess risk and contain threats

Proactively identify rogue machines and malicious actors, and bring all assets undermanagement

Reduce risk by scanning endpoints to ensure that vulnerabilities don't already exist on acquired endpoints

Investigate and remediate exposures

Standardize data center management tools and ensure all VMs are under proper management

Ensure strong security hygiene of the acquired company's endpoints

Frasers Group secures growth and improves cyber hygiene with Tanium

Frasers Group is all about growth. The UK-based retailer started in 1982 as a modest one-store operation and has grown into a global, multi-brand powerhouse. Today, Frasers operates hundreds of stores, employs more than 25,000 people, and runs brick-and-mortar and online businesses in 25 countries. In Frasers' fiscal 2021, sales topped £3.6 billion (approx. 4.7 billion USD).

Much of Frasers' growth has come via acquisitions, often of troubled companies. It's a strategy that continues. In early 2022, Frasers Group acquired bankrupt online specialist Studio Retail, adding it to a brand portfolio that now includes Sports Direct and GAME and Sofa.com.

All that M&A activity also means merging IT systems, a complex task that includes applying cybersecurity practices. Frasers must decide whether a newly acquired unit should be permitted to follow its own cybersecurity rules or be required to follow those of the corporate parent.

There's no doubt integrating IT systems is critical to M&A success. When two companies join, or one

Photo credit: Simeon87, Wikipedia

acquires another, the resulting entity often ends up with two of everything. CRMs, ERPs, finance and accounting apps, supply chain and human capital management platforms, etc. How companies navigate that environment is critical.

Getting bogged down in a morass of duplicate systems is a real momentum killer. The deal's initial excitement based on the promise of expanded opportunities can quickly fade. Ideally, the new company hits the ground running on Day 1.

To oversee these challenges, Frasers created a global group for information security and privacy. And it hired Matthew Wilmot, formerly an IT consultant, as the group's head. Wilmot now works closely with Richard Marlow, who joined two years ago as part of an acquisition and is now Frasers' manager of vulnerability testing.

Working together, they created Frasers' long list of cybersecurity must-haves. These included new capabilities for penetration testing, vulnerability scanning, and greater endpoint visibility.

“We were struggling to get a hold on our overall environment,” explains Wilmot. “The tooling we had really didn't tell us much about our assets.”

Fortunately, Wilmot was already familiar with Tanium. In a previous consulting role, he had used Tanium while helping a client respond to a cyberbreach. Now at Frasers, Wilmot felt his new employer could use Tanium to dramatically improve cyber hygiene, gain visibility into vulnerabilities and keep its systems secure.

Initially, Tanium was deployed only in Frasers' Game unit, a gaming specialist that operates more than 250 stores in the UK plus an expansive website. Because Game operates as a standalone business, Wilmot reasoned, it could function as his test lab for Tanium. The first test was limited to just 10 stores because the timing coincided with the company's busiest time — the weeks in December leading up to Christmas.

“If we took down either the website or the stores,” Wilmot recalls, “that would have been massively frowned upon.”

Fortunately, the test was a success. Frasers then rolled out Tanium to an additional 200 stores, again with a smooth delivery.

“Now we're in a position where everyone is comfortable with Tanium,” Wilmot adds. “They know it's not going to take anything down. And that lets us accelerate the rollout.”

During the Christmas season, as many other retailers were scrambling to mitigate the Log4j vulnerability, Wilmot, Marlow, and their teams were celebrating the holiday. That's because Tanium helped the company identify where Log4j existed in their environment and resolved the vulnerabilities quickly.

Now, Frasers is so confident in the Tanium platform, it's requiring every newly acquired unit to use it. Tanium will be fully implemented at Studio Retail, its most recent acquisition, and Sports Direct, its largest unit by far, accounting for roughly 70% of total group sales.

Tanium has also helped Wilmot sharpen his reporting to Frasers' board. "The boards not necessarily interested in the detailed data," he notes. "They just want to know what vulnerabilities we have and what we've done to mitigate them. With Tanium, I can be clear and concise." Adds Marlow, "Tanium is invaluable for the level of insight it's able to give us."

Learn more about how Tanium can help manage risk and increase business value during mergers and acquisitions.

LEARN MORE