Five ways Identity accelerates post-merger IT integration

okta

Five ways Identity accelerates post-merger IT integration

Large organisations often carry out mergers and acquisitions (M&A) to increase their value – but completing the purchase is only the beginning. The real problems start when you ask questions like: how do you get two totally separate companies working together? How do your teams collaborate to drive new revenue? How do your leaders access the data they need from another organisation? Or how do you send an instant message?

On the one hand, business synergy, collaboration, employee performance, and network security can all suffer when the right IT integration strategy isn't set in place. On the other, the challenges of manually consolidating disparate IT systems and onboarding newly acquired IT teams can drive-up cost and place huge strain on IT resources that are already overstretched. That's the reason why many acquired and merged IT systems often don't integrate at all, they run standalone. No synergies or 1 + 1 = 3, just 1 + 1 = 2, or, if handled badly and with strong employee churn, a more value destructive 1 + 1 = 1 format.

Perhaps that's why reports have claimed between 70 and 90% of all mergers and acquisitions fail to deliver shareholder value[1] – but it doesn't have to be that way. In this eBook, we look at five ways an Identity-first approach can help simplify and accelerate IT integration during M&A to ensure your business continues to thrive.

[1] The Big Idea: The New M&A Playbook, Harvard Business Review

1. It creates a single source of truth for identities

Controlling Identity sprawl, or the rapid growth of the many accounts a user creates to access online services as a result of having both companies' architectures adding complexity, is a key challenge during any M&A process. And, what happens if your acquisition has in turn done an acquisition that they've not addressed properly? To ease IT pains and protect networks against surging cyberthreats that prey on M&A vulnerabilities, many IT teams will want to bring all their user identities together through a domain consolidation project – yet getting there is far from simple.

Manually combining domains is highly time-consuming and complex, and usually requires external help, long project durations and high costs to complete. Yet, choosing a robust Identity platform like Okta, for example, can solve each of these challenges by automatically importing users from an unlimited number of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) directories and using data transformation capabilities to convert all profiles and attributes into a common schema.

As a result, organisations can quickly establish a single source of truth for all employee identities, easily manage AD groups, and grant people access to the appropriate applications from a single central admin console – allowing organisations to effortlessly connect all directories and applications of the acquired company and its subsidiaries to enable greater flexibility and agility.

Case study

Like many giant enterprises, ENGIE experiences constant M&A activity – buying companies, spinning off companies, and doing their best to keep everyone happy and productive through it all. Okta Universal Directory makes it easy for IT to synchronise data from various directories across the company, greatly simplifying what had been an extremely complex and time-consuming process.

- 120,000 employees using Okta to access applications from anywhere
- 100+ Active Directory domains consolidated to create one Global Address List for Office 365

Read the full case study

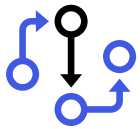
2. It provides employees with access to critical applications on day-one

After creating a single source of truth, the next way Identity can help accelerate IT integration and achieve quick wins for employees during an M&A transition is to turn on day-one access to all the applications – from both companies – that are critical to productivity.

At the acquiring side, modern Identity will automate onboarding processes to remove provisioning burdens for IT teams – allowing them to bring the acquired company's systems and employees into the fold swiftly with minimal disruption to workflows. At the seller-side, having immediate access to the intranet, IT helpdesk, and other parts of the buy-side technology stack improves productivity, creates a sense of belonging and demonstrates the broader organisation's commitment to connectivity and communications. Considering this, wouldn't it be valuable if both companies' sales teams could see each other's client lists and know where the new opportunities were to drive revenue?

All in all, an Identity solution that offers pre-built provisioning integrations for all the cloud, mobile, and web apps in either technology stack facilitates a best-of-breed IT strategy, since it gives IT teams the ability to bring the acquired company's systems into their secure environment from day one. It will also allow IT leaders to gradually sunset outdated tools as they upgrade the combined IT stack – delivering a digital workplace that users will love, and cost savings that business leaders will celebrate.

3. It secures and automates access during times of high turnover



It is an unfortunate reality that when a company is acquired, people do often leave at a higher rate than normal. As organisations move through their M&A transition, different parts of their combined organisation will often require different levels of access and in-app entitlements – and it's crucial to remember that leaving even a single account of one terminated employee active for too long creates a dangerous security loophole. Perhaps that's why a recent survey found that 76% of IT leaders cite offboarding as a significant security threat[2] that paves the way for bad actors to infiltrate IT networks during M&A transitions.

To avoid unnecessary data loss and protect the valuable IP of the acquired organisation, IT teams must be prepared to manage group access policies – as well as advanced onboarding and offboarding workflows – at scale. By linking a modern Identity solution with both the acquirer's HR system, and the acquired organisation's HR system, organisations can set prescriptive lifecycle orchestration policies that ensure seamless and timely account provisioning and deprovisioning for all employees - and how would you prove you've done this well to your auditors? Okta's governance solution automates this critical step.

Okta can also be configured so that any termination in the HR platform triggers the immediate deactivation of all accounts for that user, including those across multiple HR systems and downstream apps. IT teams can also customise this process to only take effect for involuntary terminations, to rollover access for key data to managers, or to allow grace periods for certain systems that a user still needs after they leave (e.g. payroll) while removing access to all apps containing personally identifiable information.

[2] Offboarding Security for a Remote Workforce, Torii

Case study

S&P Global

“Okta gives us freedom to enable our developers provide seamless access and better user experience.”

Ravi Chinni

Head of Identity and Access Management
S&P Global

See the full case study

4. It streamlines complex compliance processes

Merging two (or more) organisations together can create a complex regulatory environment that requires compliance with multiple legal, regulatory, and contractual obligations. Alongside the dire legal and financial consequences, failure to meet these requirements can severely damage the reputation of the acquiring business and forever compromise employee, partner, and customer trust.

While managing compliance manually is an option that many organisations will likely consider during their transition, doing so can often bring M&A activities to a standstill and create countless problems further down the line. By centralising access management with Identity, however, IT teams can effortlessly streamline the process of merging their user accounts and access rights from different organisations to ensure compliance is maintained throughout.

As well as enabling IT, security, and compliance leaders to better enforce governance and compliance policies, the right Identity solution will also automate processes such as access certification, access requests, and access reviews to ease the burden on IT and eliminate the risk of non-compliance through human error.

5. It standardises security to accelerate Zero Trust initiatives

In addition to carefully managing employee offboarding, there are several other critical aspects of IT security to prioritise when risk exposure is high. In fact, the overall M&A change management exercise can present acquiring businesses with the perfect opportunity to bolster their security posture with new Zero Trust practices.

As soon as an acquisition is on the horizon, it's crucial that IT and security teams start building out both interim and long-term plans to create common security policies, technologies, governance, and architecture across the combined business. To achieve this, they should be ready to set up new security policies for the newly acquired organisation immediately upon the acquisition closing and treat that entity as an external network with restrictive controls until its security posture is reviewed, validated, and probably upgraded.

By adopting an Identity-first approach, organisations can quickly roll out adaptive Multi-Factor Authentication (MFA) with step-up authorisation for sensitive apps to evenly secure every login attempt. Over time, Identity will help IT and security teams strengthen their Zero Trust security strategy even further by applying context or risk-based access policies, improving integration between Identity and security information and event management (SIEM) platforms, securing developer access to servers and APIs, and providing frictionless passwordless access for every user.

Case study

Envision HEALTHCARE

“When we think about cloud, we think about security first, and what data is being put there as employees ebb and flow between the company as we merge and acquire companies... Going with Okta was the best decision since we were positive that we had the right access controls in place to ensure that whoever was accessing that data was authenticated and appropriate within our organisation.”

Mark Hagan

Chief Information Officer
Envision Healthcare

Read the full case study

Summing up

By immediately creating a single source of truth for all user identities, avoiding multi year consolidation projects, automating provisioning processes, simplifying compliance management, and bolstering IT security with Zero Trust practices, the right Identity solution can help accelerate post-merger IT integration across the board.

As an agile Identity platform that was built from the ground up in the cloud, Okta can support all these use cases with a flexible architecture. That's how we've helped customers reduce the time it takes to begin collaborating with newly acquired domains by over 70%[3] and accelerated M&A activity by synchronising and consolidating domains with immediate effect.

Find out more

About Okta
Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology – anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customisable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you.
Learn more at okta.com/uk

[3] French energy giant connects 24 global business units in a flash