ecosystm

Improving Experiences Through Trust, Convenience And Speed

Empower your Customers & Employees
During Uncertain Times

REPORT AUTHOR
Claus Mortensen
Principal Analyst, Ecosystm

okta

September 2021

Executive Summary

The last year has seen organizations worldwide make drastic changes to their business processes and employee strategies.

The focus for organizations today is on how to improve the experience for their customers as well as employees in a fast and flexible way while maintaining high levels of data integrity and security. This challenge became especially obvious when the pandemic started, and it taught organizations the importance of implementing solutions at speed and with agility for future survival. In this world, companies that can adapt and innovate quickly stand a good chance of success – those that cannot, do not.

As businesses focus on improving customer and employee experiences, three core elements of success emerge – Trust, Ease of Use and Speed.

In this whitepaper we examine the significance of these core elements; the impact they have on cybersecurity measures; and the need for constant innovation.

The Future of Work and Commerce

Customer behavior and expectations have evolved during the pandemic.

As the physical interface between customers and sellers of goods and services reduced, consumers and B2B customers alike quickly came to expect more seamless online customer experiences. And although most are eager to go back to the physical shopping experience of the recent past, online and digital expectations will remain in a post-COVID world.

Similarly, employee expectations have also changed, and organisations have been forced to increase and alter their focus on employee experience (EX). In particular, they have been forced to re-evaluate what drives EX. COVID-19 brought with it a degree of fear and uncertainty in employees – fear for their job security and uncertainty on whether they could do their jobs outside their normal work environment. Whereas in the past, EX was thought to have been driven by "traditional" concepts such as salary, employee recognition and overall job satisfaction, COVID-19 has shown that factors such as flexibility, accessibility, social cohesion, effective communication and trusting relationships are almost as important for employee well-being and productivity.

The challenge to organizations is to make sure that the technology to support these objectives is available, usable, and secure – while being flexible at the same time. But they also need to learn their lessons from the past crisis and realize that the future is more uncertain than they had imagined. Ad-hoc and stop-gap solutions may have been necessary evils during the early stages of the pandemic; but looking forward, their technology choices will need to be flexible and robust enough to deal with rapid and drastic changes in the workplace.

The Nature of "Experience"

Customer Experience

Ecosystm research shows that the focus on digital technologies for enhanced customer experience (CX) has really taken off in 2021.

While in 2020, as an immediate impact of the pandemic, the focus was primarily on eCommerce and digital payments, there is now a huge demand for new platforms to be able to interact digitally with the customer, not just to be able to sell online (Figure 1). We expect this trend to continue into 2022.

FIGURE 1:
Organizations Will Consolidate Focus on Digital CX Technologies in 2021-22

29%
focused on digital CX technologies in 2020

46%
will increase use of digital CX technologies in 2021-22

64%
have CX and Customer Retention as their key business priority in 2021-22

40%
will increase use of digital technologies for product delivery in 2021-22

Source: Ecosystm Digital Priorities in the New Normal Study, 2021
N=1,770

Employee Experience

Similarly, in the workplace we have seen a huge push towards flexible access and employee empowerment, as remote working became mainstream because of COVID-19.

Organizations have been forced to invest in remote work technologies and have accelerated their VPN and access technology investments. Ecosystm research finds that more than 50% of organizations will continue to increase use of collaboration platforms even after the COVID crisis and 44% will increase their use of digital technologies for EX (Figure 2).

FIGURE 2:
Employees at the Core on Tech Investments in 2021-22

51%
will use more collaborative platforms and tools for employees

50%
will increase use of digital technologies for process automation

44%
will increase use of digital technologies for CX

44%
expect more employees to interact virtually

Source: Ecosystm Digital Priorities in the New Normal Study, 2021
N=1,312

Core Elements of Exceptional Experiences

CX and EX hinge on a few core elements: timing, availability, speed, ease, and trust.

The information, services, or goods that both customers or employees need or want must be readily and quickly available when required. It has to be relatively easy to access and/or procure and it has to be done in a manner and in an environment where the users feel comfortable and that all activities are securely managed by the organization.

The problem is that the three core elements – Trust, Ease of Use, and Speed – are often at odds with each other. For example, to many, speed and a high degree of ease of use imply trade-offs in terms of security and trust. After all, opening up the corporate network to users outside the company premises inherently results in increased vulnerabilities – but this is an unavoidable trade-off in today's world.

Trust

Traditional work environments, particularly in Asia Pacific, have historically been very controlled.

Most organizations have been – and mostly still are – very hierarchical with a predominantly top-down control over the workforce. The pandemic forced many, if not most, organizations to let go of this high level of control at least for employees who suddenly had to (and were able to) work from home. Employers were forced, to a certain extent, to simply trust that their employees were putting in the hours and the effort required.

As it turned out, the fears that many organizations had that remote employee would be distracted and unproductive were proved wrong. In most cases, the shift to the work-from-home model brought out the best in employees, and some organizations noted an increase in employee productivity.

Trust but Verify

Still, few organizations are understandably wary of completely letting go of the notion of employer control and many of them are now moving to combine the concepts of trust and control into a “trust but verify” approach where they allow employees a great deal of freedom with regards to location and working hours but monitor the work-from-home practices by closely measuring behavior and productivity.

This evolution of the role of trust has to some degree been mirrored when it comes to IT and network security. Corporate networks were traditionally very controlled environments, but soon had to adopt a “verify then trust” approach as they opened up to the Internet and needed to be accessible to mobile and remote workers. A key property of this perimeter approach is that threats were seen as predominantly coming from the outside and any user accessing the network from within the organization’s perimeter was inherently trusted.

Although this was initially regarded as a reasonably secure approach, it is no longer viable in today's environment. According to the Verizon Data Breach Investigations Report 2021, hacked or phished credentials are the primary method for breaches into an organization, and credentials with privileged access to organizational systems and networks are being especially targeted. Furthermore, API attacks are quickly becoming one of the most frequent targets for hackers. APIs are about granting access to and providing transparency for developers. Client-side developers usually need fine-grained access to services and data, and API documentation often provides immense transparency on how that can be done. This is great for developers but, unfortunately, also for hackers. This means that attacks now often originate from what appears to be trusted devices and individuals or from applications that reside inside the network. Also, with the increasing adoption of cloud-based systems, the notion of what is "inside the network" has become blurred.

Never Trust, Always Verify

The result is that no one really can be trusted – even the users and applications that have been authenticated – in a perimeter-based security set-up.

This is one of the driving forces behind the evolution of the concept of "Zero Trust" security. With a Zero Trust security approach the assumption of trust is removed from users and networks. Instead, the focus is on accessing resources in a secure manner regardless of network location, user, and device; by enforcing thorough access controls and inspecting, monitoring, and logging network traffic. It also involves evaluating access requests and network traffic behaviors in real-time over the duration of any access session while continually and consistently adjusting access to the organization's resources.

The key principle behind Zero Trust is thus never to trust anyone but to always verify all access and traffic on the network – i.e. "never trust, always verify" – and the distinction between users and endpoints within or outside the network is now non-existent.

Attacks now often originate from what appears to be trusted devices and individuals or from applications that reside inside the network.

An important consequence of this “trust no one” approach is that it puts all on an equal footing. No one is thus “more equal than others” and that in turn can be a powerful approach to create more trust and better engagement with both employees and customers. It also allows a more open approach to organizations that wish or need to offer employees the option of working remotely.

Trust, Identity and Access

Zero Trust encompasses several technologies and principles such as microsegmentation (dividing IT environments into controllable compartments), least-privilege access (granting the lowest level of access necessary to each user) and real-time monitoring of traffic and user-behavior. A core element is identity and access management and control.

Two main authentication methods used in identity and access management (IAM) are Multi-Factor Authentication (MFA) and Single Sign-On (SSO).

01 **MFA – also known as 2FA (Two-Factor Authentication), means that users need more than one authentication method (such as a password) for logging into a device or system. Typically, this means combining a password with a token, a mobile device authentication, biometric authentication and so on. The use of MFA can considerably reduce the threat of breaches on the network.**

02 **SSO in an authentication scheme that allows a user to log in with a single ID and password to any of several software systems. True single sign-on allows the user to log in once and access services without re-entering authentication factors.**

While many see MFA and SSO as competing IAM solutions, they are in fact complementary and could (in our opinion, should) be used together. MFA improves security with regards to each login to the network whereas SSO increases the ease of use especially for those who need access to several applications. Both are therefore critical features in a Zero Trust set-up.

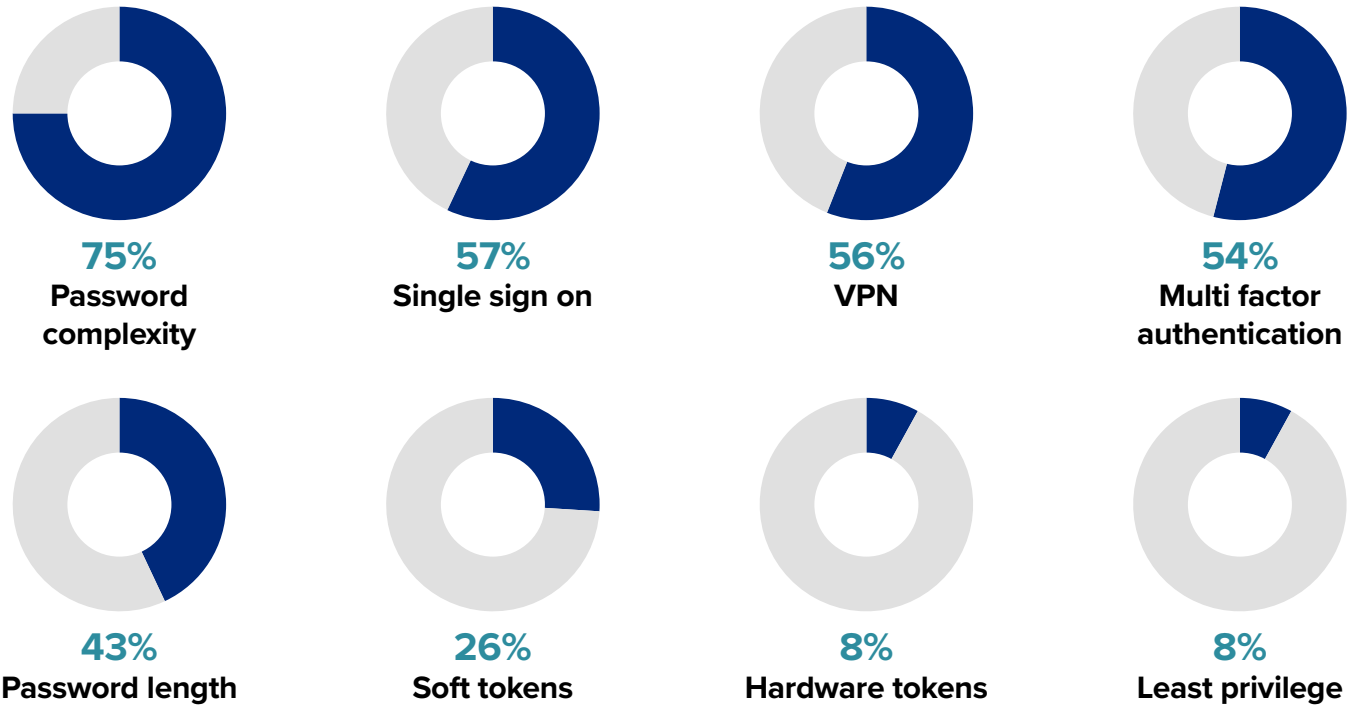
An extra level of security can be introduced through context-based authentication that introduces risk assessment capabilities into access decisions by analyzing a user’s behavior and context. Context-based authentication can include insights into devices, geographic location or network, users are logging in from and other behavioral attributes of the login, such as what types of data is accessed and whether this is common or normal behavior for the person logging in.

As long as users are behaving like they normally would when logging in, a user would not feel any impact from this added security protocol.

Context-based authentication, when implemented as part of a combined MFA and SSO setup, can thus further enhance the robustness of an organization's authentication regimen without intruding on the user experience.

Ecosystm research clearly indicates that organizations in Asia Pacific have started to see the need for prioritizing IAM solutions after the pandemic. More than a third of organizations indicate Identity and Access Management as a top tech focus. However, Ecosystm research also indicates that almost half of the organizations in the region still don't use MFA to manage access to sensitive data. The adoption of SSO is slightly higher at 57% (Figure 3). With the increased use of remote access across the workforce, these numbers are alarmingly low. Those organizations that have not adopted MFA should do so sooner rather than later.

FIGURE 3:
Controls to Manage Sensitive Data Access in Asia Pacific Organizations



Source: Ecosystm Digital Priorities in the New Normal Study, 2021
N=1,312

Ease of Use

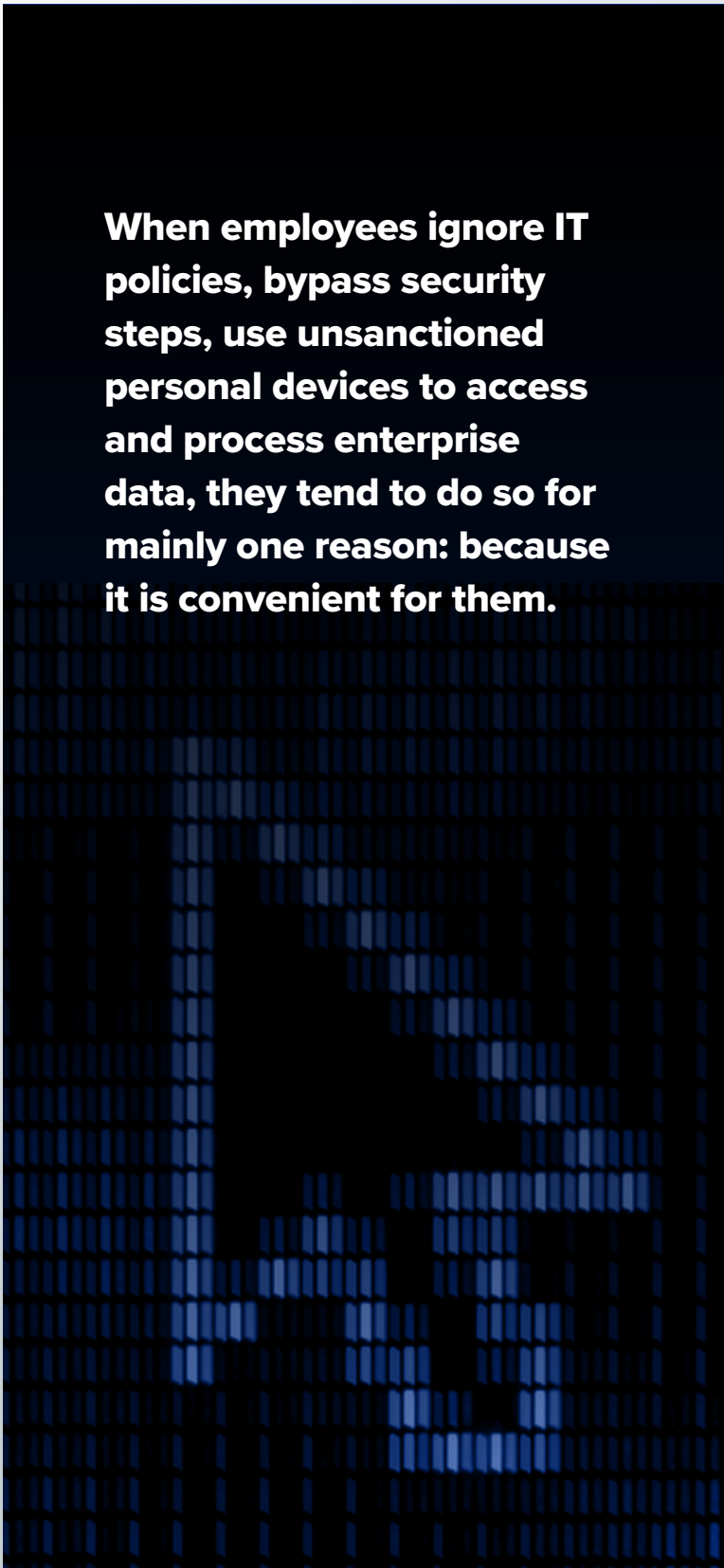
Ease of use is a crucial aspect in creating positive experience for both customers and employees.

However, it can often be at odds with security requirements – especially if it related to easy access to sensitive data. It is therefore often seen as a security risk by IT organizations.

However, we believe that it is the other way around and that ease of use and convenience should be regarded as a “security feature” – one that many IT organizations still tend to overlook. When employees ignore IT policies, bypass security steps, use unsanctioned personal devices to access and process enterprise data, they tend to do so for mainly one reason: because it is convenient for them. Employees just want to get the work done and following security protocols, making sure that devices have the right security software installed etc. is simply seen as too cumbersome or as slowing down the work process.

To counter this, ease of use and convenience need to an integral part of any security framework – especially when employees are no longer working in the office. IT managers in many organizations tend to have a narrow view of ease of use – for them it relates to their experience in implementing and running the systems. They have to expand their horizon and extend the ease to their users – the employees – as well.

When employees ignore IT policies, bypass security steps, use unsanctioned personal devices to access and process enterprise data, they tend to do so for mainly one reason: because it is convenient for them.



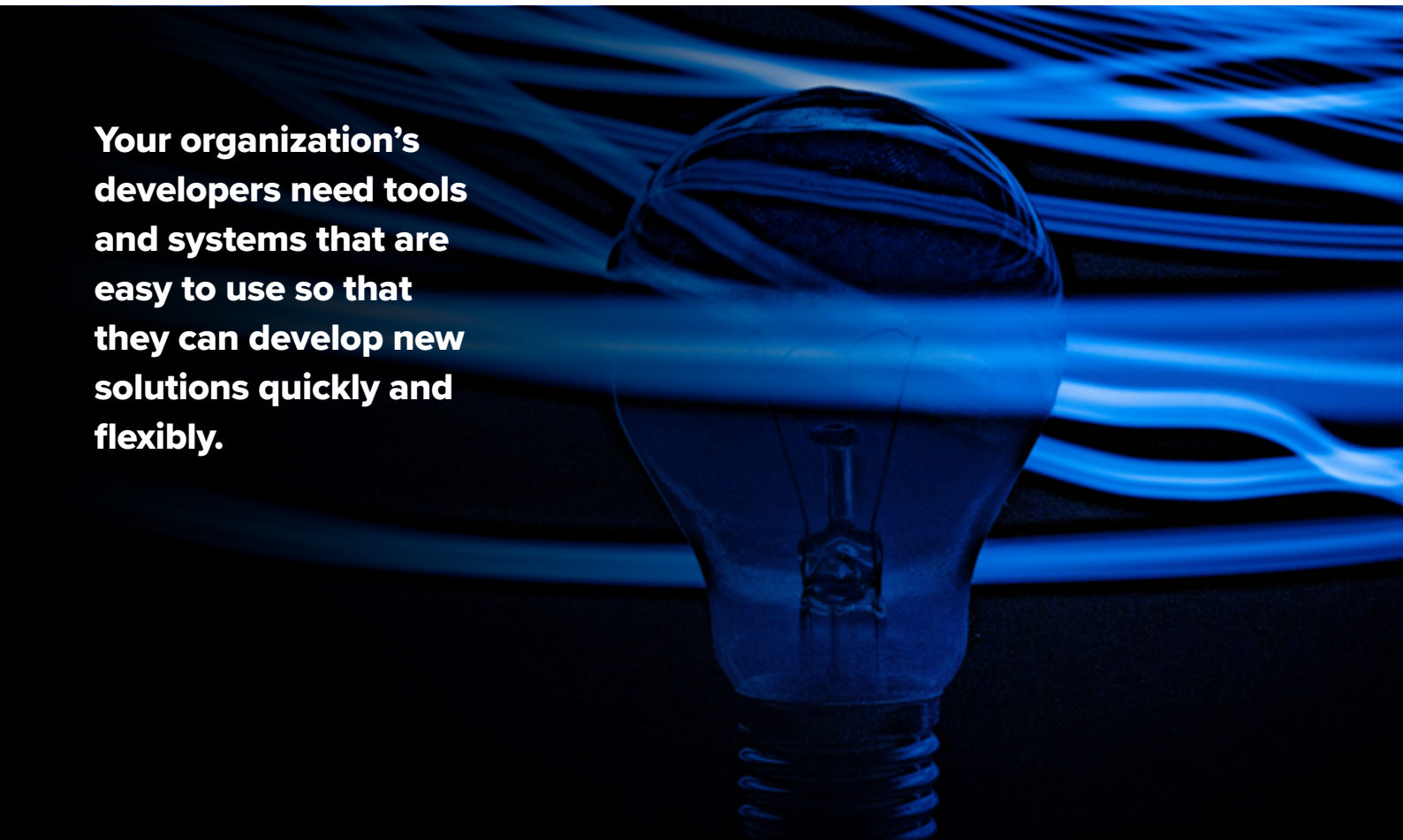
Speed and Innovation

The sudden change in work and consumption patterns has forced organizations to innovate at a pace and scale never seen before.

The few businesses that did not have an online presence became acutely aware that they need one – yesterday! It is our assessment that we have seen at least 4 years of digital growth squeezed into six months of 2020. And this is only the beginning.

This increased need and wish for new tools and applications has put a strain organizations' need for innovation. Over the last decade or so, an increased focus on innovation would have meant turning to external developers and suppliers for solutions, but more recently many businesses have started insourcing development to mitigate risk and cost – a trend that appears to have increased during the pandemic.

As in-house developers are already stretched in most organizations, the last thing they need is to have to re-architect legacy systems to work constrained identity management solutions or to have to develop stand-alone access solutions for these or other applications. Instead, they need the flexibility to develop and implement more seamlessly and quickly across the IT layers and stacks in the organization. They also need the ability to easily switch between solutions if a previous choice of technology turns out to be a poor fit for the organization.

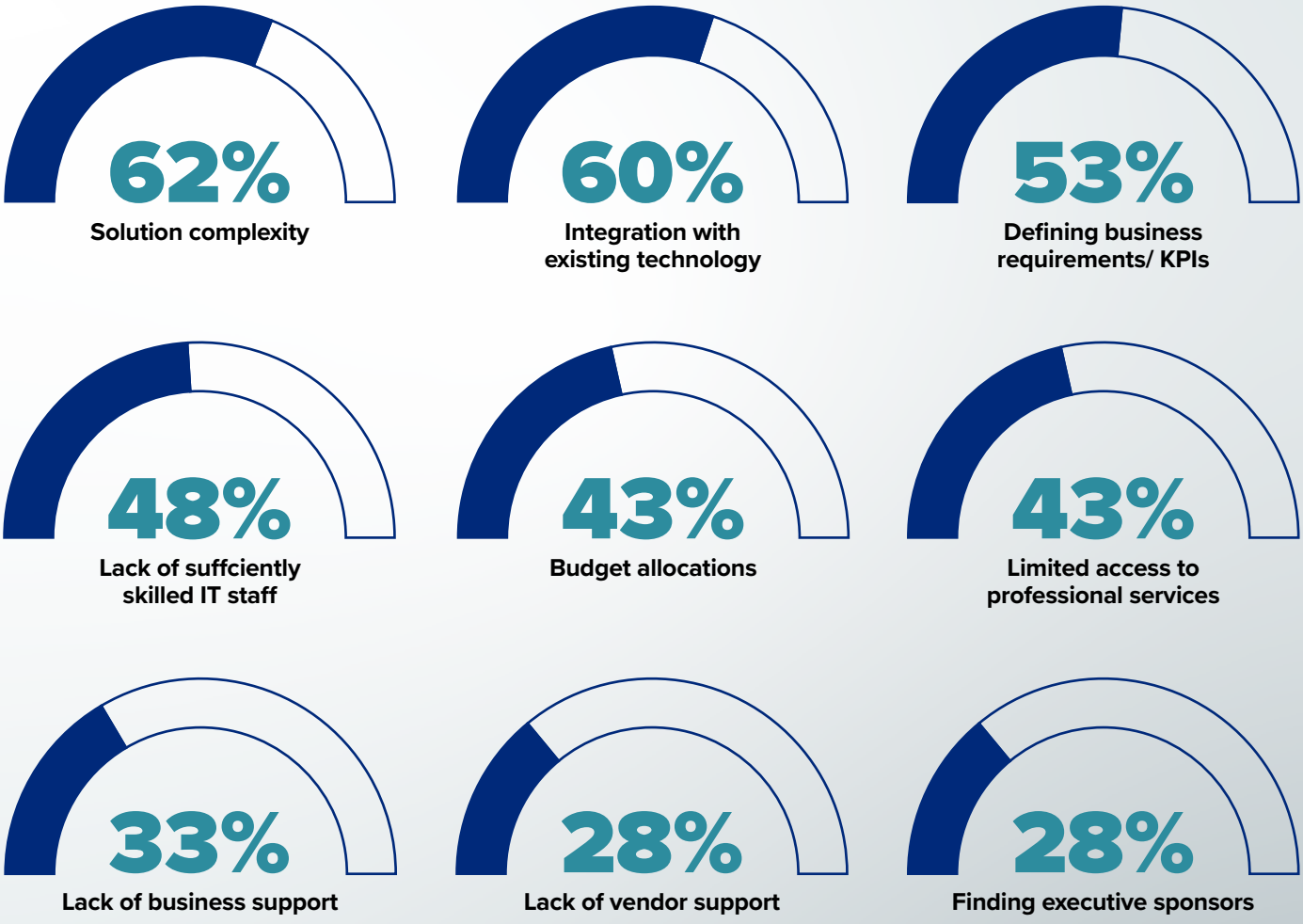


Your organization's developers need tools and systems that are easy to use so that they can develop new solutions quickly and flexibly.

The Ecosystm Cybersecurity Study finds that that more than 60% of organizations in Asia Pacific find the complexity of cybersecurity solutions and integrating these with existing technologies as major challenges (Figure 4).

In other words, your organization's developers need tools and systems that are easy to use so that they can develop new solutions quickly and flexibly.

FIGURE 4:
Challenges of Cybersecurity Solution Deployment in Asia Pacific



Source: Ecosystm Cybersecurity Study, 2021
N=1,564

A Holistic Approach to Zero Trust and Identity Management

As mentioned earlier, an important consequence of the "trust no one" approach is that it puts all on an equal footing where no one is "more equal than others".

While this is true in an ideal scenario, in the real world this is not always the case – something that many IT managers will acknowledge. Many vendors offer MFA and SSO solutions as an integrated add-on to their core solutions or platforms and while these may be very useful solutions for these apps and systems, they most often do not cover all relevant parts of the network – particularly legacy systems.

Legacy systems and many of the apps that have been adopted throughout an organization because of IT sprawl (i.e. apps and systems adopted by individual business units) are often excluded from the Zero Trust architecture and have identity and access management protocols which are incompatible with new integrated MFA and SSO solutions. IT departments then have to implement custom identity and access management solutions for these apps, which not only creates an inconsistent user experience for employees and customers but also consume more time and resources.

Consequently, a Zero Trust framework needs to embrace the entire IT system with a uniform approach to all applications and users wherever possible. So, the principles of "all things are equal" and "no one is more equal than others" also applies here.

While it may seem convenient to use an integrated or add-on solution from the same vendor who supplied an application, it often makes better sense to treat identity management and access control as a discrete, stand-alone solution

This not only offers a more consistent user experience across the entire network but also makes for a more frictionless solution for legacy and stand-alone applications. This should also result in more frictionless identity management for future applications in the organization as their compatibility and easy integration with existing MFA and SSO solutions can be examined before they are adopted.

Challenges to Zero Trust

Although Zero Trust security makes a lot of sense in most organizations, there are a number of challenges that can make adoption difficult:

01

Legacy applications, legacy networks and IT sprawl

Legacy systems are often very difficult and costly to re-architect and are therefore often excluded from the Zero Trust architecture. In the case of IT sprawl, they are often not fully visible to the cybersecurity team and risk being overlooked. Both legacy systems and sprawl applications can thus be a weak spot in even the best Zero Trust set-up.

02

Lack of skillsets

Being a fairly new approach to cybersecurity, many organizations simply don't have the knowhow or skillsets available to initiate the migration to a Zero Trust architecture. Many of these organizations may soon find themselves in a position where the need for more flexible and more cloud-based IT systems renders their present cybersecurity architectures less than adequate. They will need to educate themselves and update their skillsets so that they can better assess whether Zero Trust is a viable option for them in the near future.

03

Legacy mindsets

The Zero Trust concept is still too alien to many IT departments and even CISOs. Those who have worked with perimeter-based security set-ups for years may find it very difficult to accept a security architecture that differs significantly from what they are used to. Supporters of Zero Trust may find the biggest hurdle to adoption come from within the organization.

04

Out of date regulation

Many regulations – and regulators – have not yet adopted or approved of the Zero Trust concept. In some geographies and industries – especially where regulatory compliance and certification is a must – Zero Trust may not yet be a viable option as it could mean failing regulatory scrutiny and auditing requirements.

Key Takeaways

Never trust. Always verify.

Network security based on trusted devices or users is rapidly becoming unfeasible. Hacked or phished credentials are the primary method for breaches into an organization, and credentials with privileged access to organizational systems and networks are being especially targeted. Once a trusted device or identity is compromised, the damage to the network and data can be immense. A well implemented Zero Trust framework can help counter such threats.

Prioritize IAM with "bells and whistles".

Identity and access management is a key element of Zero Trust – especially when using the appropriate authentication measures. MFA and SSO are complementary and should be used together, but security and ease of use can be augmented by adopting context-based authentication.

Adapt @ speed.

COVID-19 has taught organizations the importance of implementing solutions at speed and with agility for future survival. Organizations that can adapt and innovate quickly stand a good chance of success – those that cannot, do not. Whenever possible, your security solutions should not obstruct your workforce's agility or your ability to innovate.

Don't underestimate the importance of ease of use.

Most security breaches involve some level of human error. If your access and identity management measures appear disruptive and cumbersome to your workforce, chances are that some of them will seek to bypass these measures whenever possible. Your security measures should therefore be as frictionless as possible, and access and connectivity should be provided without interfering with the user experience.

Your developers need ease of use too!

In-house developers are already stretched and the last thing they need is to have to re-architect legacy systems, to work with constrained identity management solutions or to have to develop stand-alone access solutions. Instead, they need the flexibility to develop and implement seamlessly and quickly across the IT layers and stacks in the organization; and they need tools and systems that are easy to use.

A holistic approach is essential.

Consider a discrete, stand-alone solution for identity management and access control. Discrete options are often better to achieve a consistent user experience across the entire network and can offer frictionless solution for legacy and stand-alone applications.

Case Study - FedEx's Journey Towards IDaaS and Zero Trust

The Challenge

Until recently, FedEx had spent 20 years developing best-of-breed IAM and was running a VPN along with on-premises MFA, on-premises federation, and on-premises web access management. This had resulted in a "Whack-A-Mole game" from a security perspective with each separate IAM solution posing a risk to the company as they could potentially get the configuration wrong. The resulting IAM infrastructure created complexity not only for the security team but also for the rest of FedEx's business units, as employees often needed multiple password entries to access the apps and information they needed to get their jobs done.

The Solution

To solve the company's IAM problems, the FedEx cybersecurity team opted for an identity as a service (IDaaS) solution and chose Okta as their service provider. FedEx's reasons for choosing Okta's solution came down to five key points:

- Ease of implementation
- API availability
- A wide range of MFA options
- Universal Directory and the ability to easily aggregate identities from multiple user stores
- Turnkey compatibility with key development applications

Moving to Zero Trust

While reviewing their IAM infrastructure, FedEx had also decided to adopt a Zero Trust security model for their overall network infrastructure and to move away from the previous reliance on passwords. That meant adopting a security framework that could verify users and devices, evaluate each login situation in context, and use the results to tailor the sign-in experience according to the level of trust assigned to it. FedEx found that adopting the Okta Identity Cloud with the identity-as-a-service model, using Okta Universal Directory and Okta Single Sign-On, was the solution that enabled these requirements.

Okta's support of modern authentication protocols, such as SAML 2.0 and OpenID Connect meant that they could support FedEx apps, whether SaaS, cloud-native, or legacy applications. Furthermore, Okta Adaptive Multi-Factor Authentication allowed FedEx to add contextual verification requirements for users.

The FedEx cybersecurity team can now manage conditional access across the company from a single access policy engine that covers every application in the network – meaning that they can tailor the sign-in experience – whether it is password only, no password at all, or password plus MFA.

Speed was key

As the pandemic began in February 2020, the FedEx team was still early in the process of integrating all their applications into Okta. Because of the increased work-at-home environment, the company had to accelerate some of the integration work and over a period of 36 hours, FedEx and Okta managed to move Workday, Office 365, Webex, ServiceNow, Salesforce, Checkpoint VPN, and Zoom to Okta.

The Outcomes

- The FedEx team is making progress in decommissioning legacy IAM solutions and integrating approximately 250 SaaS apps, 500+ on-prem apps, and 400+ cloud-native apps into their Okta solution.
- A particularly valuable outcome for FedEx has been the ability to flex the company's applications into consumption and hybrid situations like co-location or even public clouds to be able to handle volume surges, which can typically be a challenge for logistics companies.
- With the Okta model, FedEx's development teams now have just one token to worry about – they can do authentication and authorization in a consistent way no matter where they are deployed.
- The team is also in a position to aggregate identity stores into Okta Universal Directory, using a lightweight on-premises agent approach, when presented with M&A activity. That strategy helps them integrate new companies more quickly. With one cloud-native platform – covering SaaS apps, cloud-native apps, and legacy apps – and one unified directory – for the entire FedEx workforce – everyone can log in and get to work with less friction and fuss.

About the Author

Claus Mortensen
Principal Advisor

Claus has more than 17 years of experience in both strategic and tactical guidance for vendors and service providers in the IT and telecommunications space. Having worked as an analyst and a consultant in both Europe and Asia, Claus has supported clients with local, regional and global briefs to position their offerings and grow their businesses in their target markets. These have included Google, Microsoft, IBM, AT&T, Orange and SingTel.

Previously, Claus spent nine years at IDC Asia Pacific, where he climbed the ranks to launch and lead IDC's Emerging Technology practice. In Asia and Europe, Claus is also a renowned speaker and blogger, who continues to evaluate and forecast how disruptive technologies impact the marketplace and how digitization is transforming business models across all industries.

Claus is based in Copenhagen, Denmark, which also marks Ecosystm's extension and coverage in the EMEA region.

okta

Okta is the leading independent provider of identity for the enterprise, and the Okta Identity Cloud enables organizations to both secure and manage their extended enterprise, and transform their customers' experiences.

With over 5,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely adopt the technologies they need to fulfill their missions. Over 5,600 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to securely connect their people and technology.

ecosystm

Ecosystm is a private equity backed Digital Research and Advisory Platform with global headquarters in Singapore. As a global first, Ecosystm brings together tech buyers, tech vendors and analysts into one integrated platform to enable the best decision making in the evolving digital economy. The firm moves away from the highly inefficient business models of traditional research firms and instead focuses on research democratisation, with an emphasis on accessibility, transparency and autonomy.

Ecosystm's research originates from its custom designed "Peer-2-Peer" platform which allows Tech Buyers to benchmark their organisation in "real-time" against their industry or market. This bold new research paradigm enables Ecosystm to provide Tech Vendors access to ongoing and real time Market Insights in an affordable "as-a-Service" subscription model.

This white paper is sponsored by Okta. It is based on the analyst's subject matter expertise in the area of coverage in addition to specific research based on interactions with technology buyers from multiple industries and technology vendors, industry events, and secondary research.

The data findings mentioned in all Ecosystm reports are drawn from Ecosystm's live and on-going studies on the Ecosystm research platform. This document refers to data from the global Ecosystm Cybersecurity Study and the Ecosystm Digital Priorities in the New Normal Study; based on participant inputs that include decision-makers from IT and other Lines of Business, from small, medium, and large enterprises.

For more information about Ecosystm studies visit www.ecosystm360.com