Whitepaper

The New Strategic Imperative for Business

Contents

Introduction

Welcome to part 1 of a three-part series exploring why a secure and resilient business is more important than ever.

Over the next few weeks we will be releasing two further reports that together build a comprehensive story highlighting how small and medium-sized businesses can better protect their workplaces, increase operational resilience, and ensure that their customer-facing apps are more engaging, secure, and frictionless.

In part 1, we explore why it's imperative that small and medium-sized businesses build proactive, identity-enabled resilience into their customer apps and workplace authentication models.

Whether you're driving IT or security strategy for your business or you're leading the charge in product development, this series will provide a comprehensive guide to how frictionless, adaptable authentication and Identity and Access Management (IAM) can drive business resilience, innovation, greater productivity, collaboration, and customer satisfaction.

From managing risks to building resilience

Today's business depends on digital transactions, workflows, and resilience. Global banking networks process trillions each year. Linked to those networks are the hand-held, wireless point-of-sale devices restaurants now use to charge diners for their meals. From farm to fork, technology assists all along the way.

The modern world has apps for just about everything. They span every industry — in both public and private sectors — from energy to manufacturing and logistics to stocking store shelves. Healthcare. Financial services. Education. Entertainment. They enrich people's lives by helping them stay informed and connected. But only if they work.

Ensuring trust

No matter the app, where it's hosted, or how it's accessed, users must be able to trust its availability, performance, and safeguards for their authentication credentials. They don't want any of their apps exposing them to risk, much less having to manage those risks. That's where resilience comes into play, enabled by robust digital Identity capabilities.

Identity, the entry point to today's digital world

To get cyber safeguards right, identity must be done right. When identity is managed correctly, resilience follows.

- To protect customers using their products, developers incorporate **Customer Identity and Access Management** (CIAM) capabilities. CIAM can enable users to seamlessly and conveniently access all of a company's products from a single login. It can also control their data and usage.
- In the workplace, **Identity and Access Management** (IAM) encompasses policies and technologies that ensure that only authorized individuals can access specific resources at the right time.

For digital internal and external applications, IAM and CIAM functionalities enable efficient lifecycle management of user identities. With seamless, friction-free authentications, users can enjoy secure, personalized experiences from login to logout.

For software, resilience means that an app keeps functioning despite component faults or failures. For businesses, this enables companies to resume operations quickly if a disruption occurs, such as a data breach.

Businesses must protect their users — both customers and employees — with end-to-end, adaptive digital Identity capabilities. Easy authentication and access are essential design points. User personalization can be a big plus, elevating customer engagement and delivering a competitive advantage.

What is software resilience?

Software resilience refers to an app's capacity to maintain its functionality and performance, even if the operation of a certain component or components start to degrade or even fail altogether. CIAM solutions can enhance resilience in several ways:

- **Centralized Identity management** reduces the complexity and potential vulnerabilities associated with managing identities in disparate systems.
- **Scalability and redundancy** enables the handling of large volumes of user requests across a distributed infrastructure, even during high traffic periods.
- **Adaptive authentication** monitors user behavior and context throughout a session and can detect and respond to suspicious activities in real-time, enhancing an application's overall credentials, protection, and resilience.
- **Developer-friendly integration** offers robust APIs and SDKs that make it easier to integrate CIAM into applications. This reduces the time and effort needed to build safe, resilient applications. Learn more.

Supporting innovation

Whether their products are destined for business-to-consumer (B2C) or business-to-business (B2B), developers need easy ways to provide these functions in their products — and easily maintain them throughout each product's lifecycle.

While most developers and product managers know the importance of robust CIAM and IAM capabilities in their products, they're not necessarily skilled at architecting and coding them. They'd rather use their talents to drive innovations, delighting customers with new features and functions that keep them coming back.

In turn, their team leaders want to improve efficiency and productivity, compress development cycles, and launch products and upgrades much faster. And product managers want those products fully tested, well differentiated, and ready to drive significant revenue and growth.

Maximizing resources

Too often, businesses lack the needed resources to handle the increasingly complex challenges of safeguarding digital identities of users confidently and at scale. Skills, tools, and budgets can be scarce. This is especially true for companies providing software as a service (SaaS), web-based apps, or digital content. Whether they're targeting B2C or B2B markets, their offering must be resilient in its performance — and help business customers be resilient in their operations.

After all, protecting Identity today is far more than protecting authentication logins. Every click must be kept safe. From login through logout, user experiences must not only be easy and personalized but also adaptive to their various devices, geolocations, connectivity channels, language and currency preferences, and more.

What is business resilience?

Business resilience refers to a company's ability to recover quickly from operational disruption, such as what a breach can cause. Here are some of the ways digital Identity using IAM tools can help:

- **Centralized identity management** reduces the complexity and potential vulnerabilities of managing multiple identity systems. It also ensures consistent policy enforcement and easier management.
- **Adaptive MFA** adjusts authentication challenges based on real-time risk signals, such as the user's location, device, network, and behavior. This provides stronger protection against account compromise while ensuring legitimate users experience minimal disruptions.
- **High availability and disaster recovery** ensure that services stay operational even during regional outages. This reduces failover times and maintains access to critical applications.
- **Continuous threat monitoring** assesses risks using native identity signals that can interoperate with third-party providers for enhanced, proactive threat detection. This provides a more resilient operational posture.
- **Improved user accessibility** to necessary tools and resources, seamlessly and securely, enables employees to work efficiently from anywhere. This flexibility can support business continuity and disaster recovery, both keys to operational resilience. Learn more.

Risks beyond cyberthreats — and why resilience is important

In the past, risk containment typically involved providing customers with fast and secure access to digital products or keeping threats out of the workplace. Today, however, it must do more. It must proactively deliver resilience that can protect app customers as well as a company's assets and employees from many other vulnerabilities.

Among those are regulatory violations, reputational damage, weakened market and competitive positioning, and potential litigation. Any of these alone or in combination can cost dearly and undermine, or even destroy, a company's future prospects. News about breaches can make it hard to attract and retain talent. Breaches can also send long-time customers fleeing to competitors.

Building loyalty

For customers, resilience in their digital apps and services can define the quality of their experiences. Authentication credentials must be safeguarded without affecting app performance or impeding login sequences. Apps must also be able to resist or recover quickly from faults or load spikes and stay fully functional without unusual latencies or unexpected behaviors.

App resilience can set companies apart from their competitors, too. Should customers have a bad experience, they may quickly seek alternative providers for their services. Even worse, they may disparage the original provider to family and friends. Many will share their poor interactions via social media as well.

Not just keeping threats out but knowing who is in

In the workplace, businesses, especially small and medium-sized ones, are finding it's no longer enough to focus solely on cyber defense. They must be on the offensive against threats across their core and extended digital domains. These can include on-premises infrastructure, the edge, data centers, the cloud, and the mobile devices of users on the go.

Companies must also protect their entire workforce — employees, contractors, and partners — from threats that are ever-increasing in their frequency and sophistication. Artificial intelligence (AI) has added new levels of complexity to those threats. It can also be used to counter them.

Here, too, resilience plays a critical role. The different risks facing organizations and their workforces require a holistic strategy via a layered, defense-in-depth, Zero Trust architecture. While guarding against traditional and emerging threats, this approach must also ensure that a business can anticipate, respond, and recover from attacks.

Identity: The key to enabling Zero Trust architecture

Zero Trust is a proactive protective framework based on the belief that every user, device, and IP address accessing a resource is a threat until proven otherwise. Identity is its key.

Under the concept of "never trust, always verify," it requires that IT and security teams implement strict access controls and verify anything that tries to connect to an enterprise's network.

Zero Trust has since gained ground as an effective strategy to prevent cyber attacks. It complements and strengthens defense-in-depth architectures long used worldwide.

New imperative

For today's businesses, enhancing cyber safeguards with a focus on resilience is a strategic imperative. Comprehensive but friction-free identity and access privileges can facilitate workflows, information access, and multiparty collaborations. This can enhance organizational efficiency, productivity, and innovation. It can make companies more agile and competitive in their markets. It can also lower costs and increase profits.

Resilience makes traditionally reactive countermeasures against workplace cyberthreats much more proactive, even anticipatory. To be effective, it requires the following:

- Proper governance with executive support
- Continual monitoring of all safeguards, policies, and protocols
- Training employees and keeping them vigilant
- Delivering great user authentication experiences in all digital offerings

IT and security teams need to know exactly who's inside their digital perimeters. Businesses must be able to enforce their governance policies consistently across all users. While these are typically employees and contractors, more and more are vendors and partners who make up the company's business ecosystem.

Authorized individuals should only have access to the information or services they need, when and where those are required. But managing the dynamics across all user types can be a tall order. Users come and go physically and virtually all the time. Without seamless, friction-free authentications, workforces can suffer losses in their:

- Efficiency and productivity
- Communication and collaboration
- Job satisfaction

Staying ahead in a rapidly evolving landscape

Addressing business cyberthreats is increasingly complex and evolving rapidly. For the developers of large-scale SaaS services, web-based apps, and digital content, it can be daunting to provide seamless, easy user authentications.

Single sign-on and social login functionalities with multi-factor authentication (MFA) have become the norm. Soon these will be complemented by hardware-based MFA, such as YubiKeys, and by passkeys, biometrics, and other tools.

In addition, threat actors are adopting more sophisticated tactics, supported by powerful AI-enabled tools. With these, hackers can launch more accurate and effective attacks at greater frequencies and lower costs. Machine learning algorithms can analyze vast amounts of data to identify new vulnerabilities and automate their attack strategies. The good news is that AI can also be used in CIAM and IAM tools to counter those attacks using anomaly and bot detection, among other intelligent capabilities.

Expanding attack surfaces

Another issue is the rise of work-anywhere scenarios — remote, hybrid, and mobile — which have vastly expanded companies' attack surfaces. Traditional offices are no longer the sole points of entry for hackers. Now, every remote laptop, mobile phone, and external connection represents a potential vulnerability to exploit.

Add to that how companies are increasingly using cloud services and third-party web connections. These can complicate their threat detection and mitigation challenges even more. This evolution makes small and medium-sized businesses particularly vulnerable because they may not have the resources to effectively secure such a breadth of potential entry points.

92%

92% of small and medium-sized business breaches involved system intrusion, social engineering, and basic web application attacks.

98%

98% of small and medium-sized business breaches were financially motivated.

Safeguarding employees

Today's organizations face increasing numbers of threats targeting employees. Identity-based attacks, such as phishing and credential theft, are rising. They exploit human vulnerabilities via social engineering.

Consider the following statistics regarding small and medium-sized business breaches from the 2023 Verizon Data Breach Investigations Report:

- 92% involved system intrusion, social engineering, and basic web application attacks.
- 94% were perpetrated by external threat actors.
- 98% were financially motivated.
- 54% involved compromised credentials.

These figures highlight the growing need to proactively prevent their occurrence. This is why workplaces must use strong Identity and Access Management tools and processes. At the same time, employees must watch out for deceptive emails.

If a breach happens, resilient Zero Trust architectures with strong IAM capabilities can help a business contain the intrusion, minimize disruption, and recover much faster.

80%

80% of customers consider a company's user experience as important as its products and services.

80%

80% of customers think their experiences should be better, given all the data companies collect.

Protecting customers

Businesses must efficiently authenticate their customers so they can log in to their apps or services safely and securely from anywhere, using any device, at any time.

Once authenticated, customers want convenient, consistent, and personalized experiences. Recent research of 14,300 customers worldwide revealed that:

- 80% consider the company's user experience as important as its products and services.
- 80% think their experiences should be better, given all the data companies collect.
- 79% are increasingly protective of their data.
- 65% expect service providers to adapt to their changing needs and preferences.

These responses suggest that companies must ensure their customers' digital experiences are the best they can be, no matter how they're accessed. And despite high-profile, massive data breaches in recent years, customers trust providers to protect their data, especially given that they're sharing more data than ever.

Many nations mandate strict data privacy laws, such as the US Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule shielding all individually identifiable health information and the EU General Data Protection Regulation (GDPR), which governs the confidentiality of nearly all an individual's privacy and personal data.

Noncompliance with the GDPR can be extremely costly. For example, since the GDPR was enacted in 2018, Meta has paid many billions in fines for violations by its different businesses.

Can legacy safeguards address modern threats?

As cyberthreats evolve, legacy safeguards can struggle to keep up, opening vulnerability gaps. Outdated defenses can be inadequate for protecting against modern threats.

Edge and cloud connections, for example, require their own defenses to prevent unauthorized access and data breaches. The “shadow IT” phenomenon, where employees use unauthorized applications or devices, complicates the threat landscape further.

Even with upgrades to protect against cyber attacks, advanced IAM tools are needed. They can help ensure only authorized individuals have access to sensitive information. This will reduce risks of data exfiltration, intellectual property theft, and other disruptive breaches.

Why resilience is critical: Business impacts of a breach can be massive

The costs of breaches are higher than ever. Companies can suffer big monetary losses, legal and regulatory impacts, and reputational damages. These make prevention and resilience critical.

High-profile data breaches are reported frequently — mostly via social engineering, especially phishing. For small and medium-sized businesses, these impacts can be painful:

- **CafePress.** Attackers exploited a vulnerability in this online retailer's website, where users can create and sell custom products. They stole the personal data of 23 million users. The firm paid huge sums to notify customers, provide credit monitoring, and enhance safeguards. Customer trust vanished.
- **Medical Oncology Hematology Consultants.** A phishing email resulted in a ransomware attack that encrypted the patient data of this well-known specialty practice. Costs included data recovery, system restoration, and enhanced IT upgrades to detect and contain threats better and faster. The disruptions and loss of patient trust were substantial.
- **The Heritage Company.** No longer in business, The Heritage Company, a 61-year-old Arkansas telemarketing firm, was shut down by a ransomware attack. The financial strain, including recovery costs, forced nearly 300 employee layoffs and then led to its closing.

Key challenges in modernizing protections and building resilience

Businesses must balance innovation with protecting sensitive data. In the workplace, resilience against threats is needed with automated Identity and Access Management. This can thwart attacks, especially phishing and credential hacking, and help a business rebound quickly if an incident disrupts operations.

Single sign-on, passwordless authentication, and biometrics can boost employee productivity and collaboration by modernizing outdated identity and access methods. Plus, automated, real-time onboarding and offboarding of employee credentials can save HR and IT valuable time. It can also prevent malevolent, post-termination intrusions.

Streamlining development

In producing and updating digital products, developers must implement secure authentication workflows while providing seamless, frictionless experiences for employees and customers. As product features and user bases increase, more points of failure and new vulnerabilities can emerge, reducing resilience and increasing performance and risks of compromise.

Containing these risks can be difficult, especially at scale across different devices and user scenarios. Doing so in dynamic DevOps models can be even harder. That’s why developers are advised to inject Identity authentication capabilities as early as possible into their automation pipelines to minimize the exposure of sensitive accounts and credentials.

This way, they can remove static credentials from code and replace them with just-in-time (JIT) credentials that help reduce the threat surface and enterprise-wide risk. Doing so can save developers time and effort while accelerating time to market and new feature releases.

From a reactive to a resilient, proactive threat protection

Proactive workplace threat protections provide resilience that builds on layered, defense-in-depth models. It can not only detect and react to threats but also anticipate and mitigate the risks of evolving threats before they escalate.

Further enhancing this approach is the concept of Zero Trust architectures that use sophisticated and automated IAM. Legacy security frameworks typically have trusted individuals and devices already within an organization's network. In contrast, a Zero Trust approach requires verified identities of all access attempts by both people and devices internal and external to company networks.

By incorporating advanced IAM capabilities into a Zero Trust architecture, businesses will always know who their users are. This applies across both workplaces and customer bases. Everyone's data includes their access privileges, what devices they're using, and when and where they went during their user session.

Developers can also derive insights from other authentication and session data that can help them improve the performance and resilience of apps and services. This data can assist in personalizing user interactions with digital apps, services, and content. By making their products more engaging, they can differentiate them in the marketplace and gain competitive advantages.

Developers must similarly streamline the authentication process of confirming customers' identities when accessing their apps and products to enhance the experience without compromising data privacy or inadvertently adding new vulnerabilities.

Ideally, advanced IAM capabilities can also automate the lifecycle management of who's who and their specific privileges in real-time. This can help companies deal with the constantly changing dynamics involved in authenticating their customers. It can also assist in user Identity and Access Management across all their diverse technology domains.

To achieve this, digital Identity mechanisms must be able to adapt access to individual user situations on the fly, depending on their context and risk. By doing so, developers can reduce or eliminate authentication roadblocks and friction.

Start now to build resilience across workplaces and customer bases

Today, it's imperative that small and medium-sized businesses build proactive, identity-enabled resilience into their customer apps and workplace authentication models. Seamless, friction-free digital Identity capabilities can be a competitive differentiator.

Internally, easy IAM capabilities can improve employees' productivity, collaboration, and overall job satisfaction, aiding in their retention and the recruiting of new talent.

This is especially true for a company's developer team that is in charge of product innovation. It's certainly easier to plug in a fully tested, turnkey authentication solution that's easily branded instead of coding one. And time to market can be accelerated by weeks, if not months.

At the same time, a proven authentication solution can provide users with consistently great experiences from login to logout. This will keep customers coming back and new ones joining their ranks. Developers and product managers can also analyze user authentication data to refine, de-risk, and accelerate reaching key milestones on their feature innovation roadmaps.

Advanced digital Identity capabilities can help businesses shift from solely managing threat risks to building resilience into the workplace, its extended domains, and digital products. Doing so can improve company performance, user satisfaction, and market positioning.

But these competitive advantages won't remain forever. Other companies will begin to implement them, too. In short, today's differentiators will be tomorrow's table stakes. Forward-looking businesses need to get started implementing them now.

Are you ready to learn more?

We hope that you found part 1 of the series interesting and challenging. Parts 2 and 3 will now automatically be delivered to your inbox over the next few weeks. Here's what to expect:

Part 2

For IT strategists and security leaders, we will explore:

- Knowing who's where, when, and for what purpose across the company's digital landscape
- Keeping employees productive and empowered, not impeded
- Optimizing the potential of remote and hybrid work without increasing risk
- Offering easy logins while improving cybersecurity, governance, risk, and compliance initiatives

For development and product leaders, we will explore:

- Streamlining access with multi-factor authentication and passkeys
- Easy customer identity lifecycle management
- Simplified regulatory compliance and auditing
- Seamless integration with cloud solutions
- Driving development efficiency

Part 3

How Okta's Workforce Identity Cloud can:

- Accelerate times to innovation, market, and cash
- Reinforce operational resilience
- Create better work experiences and job satisfaction
- Build stronger trust among suppliers, partners, and customers

How Okta's Customer Identity Cloud can:

- Provide superior user experiences across all their devices and channels
- Enhance product performance, strengthen security resilience, and help you scale easily and quickly
- Save developers time so they can focus more on innovation
- Boost revenue with improved acquisition and retention

If you would like to read more about Okta in the meantime - visit our website