Automating the Security of Your Digital Identity: A “Super” Strategy

February 2024

Though there’s nothing fictional about the critical importance of securing digital identities, let’s imagine for a moment that we’re living in a superhero realm. After all, do references to Batman ever get old? Of course not.

Just as Batman must fight a rotating cast of villains focused on stealing, chaos, and destruction, today’s security teams inside organizations must also find and defeat dark actors working in the shadows before they breach an organization and destroy business functions, trust, and competitive advantage. These security teams may not wear capes, but they—and the technologies and tools they rely on—are the first line of defense in protecting a company’s sensitive data.

Defending Against Devasting Data Breaches

In a world without Batman, Gotham City would be under near-constant attack. Likewise, a world without secure, scalable solutions for securing digital identities—the gateway to a company’s systems, networks, and applications— would create space for free-for-all cyberattacks that result in costly data breaches, theft, and loss which would go unchallenged.

Consider these sobering statistics from a report sponsored and published by IBM's Security division and independently conducted by Ponemon Institute. The study surveyed 553 global organizations between March 2022 and March 2023 and found that the average cost of a data breach rose to USD 4.45 million—a 15% increase since 2020.

The study also revealed that:

- 82% of breaches involved data stored in the cloud—public, private, or multiple environments
- Only 1 in 3 security breaches were identified by an organization's own security team or tools—highlighting the need for better (and automated) threat detection
- 4 in 10 companies rely on manual inputs in their security operations
- 51% of organizations plan to increase security investments as a result of a breach

Fully securing your organization's digital identities, whether in government, healthcare, enterprise, or small business, is critically important. An organization's customers, partners, patients, employees each expect that their digital identities will remain secure. If or when that trust is broken through a security breach, organizations stand to lose business along with their reputation—not to mention the harm done to exposed individuals.

Unfortunately, organizations must also factor in insider threats from misuse of credentials, policies, and procedures. Likewise, outside threats in the form of phishing and other malicious cyber attempts remain an ongoing danger.

What to Consider When Choosing a 'Hero' Digital Identity Solution

Let's say Batman didn't have his Batmobile, super strength, or trusty sidekick, Robin, to help him fight villainous cybersecurity threats throughout Gotham. Let's say he wanted a SaaS-based solution that he could use in his organization to protect digital identities—his own, and those in his trusted circle. What should he keep in mind?

We recommend he consider a solution that:

- Ensures full security and privacy through encryption, strong authentication, and user consent mechanisms that will mitigate security and privacy risks
- Can automate complex, time-consuming tasks while minimizing the risk of human error
- Meets industry compliance and regulation requirements in order to avoid legal consequences, fines, and reputational damage
- Supports interoperability with existing systems and platforms
- Ensures business continuity by reducing disruptions caused by security incidents
- Is scalable and can grow with the organization

Fighting Cyber Crime Together

The ability to fully secure digital identities remains a top business priority for good reason. Think of it as a safety net in conducting business across the web.

Superhero talk aside, secure solutions for digital identities can optimize auditing and compliance processes, by keeping up with industry regulations, which truly is fundamental in helping companies avoid data breaches and the financial impact, legal consequences, and loss of business trust that can result.

Not only this, but employing the right solution for securing organizational digital identities can improve business strategy by improving connectivity and providing assurance for digital communications. Employing an automated solution for digital identities can also help to redistribute resources and reduce team workloads by removing manual security processes, as well as enhancing overall efficiency.

When it comes to digital identities, every business has different requirements for their security infrastructure, but choosing a solution does not need to be complex. Protect your digital identities with an automated solution.