Cyolo

SECURE DIGITAL TRANSFORMATION REQUIRES IDENTITY-BASED ACCESS CONTROL

INTRODUCTION

Digital transformation is an all-encompassing term that refers to a wide swath of activities designed to modernize and streamline a company's business operations. But these initiatives are challenging, as many organizations struggle to fully implement the solutions needed to achieve their goals.

Still, the benefits far outweigh the difficult implementation. A recent Deloitte digital transformation report found that organizations with higher digital transformation maturity ratings reported **45% revenue growth**. Successful digital transformation provides organizations with the tools to become modern, agile, and digital-first businesses. But while change can be a force for progress, it must be performed well, weaving a robust identity strategy into the process from its start. The race to digitize is ongoing, with **55% of businesses under pressure to complete the process**, believing that they will otherwise lose market share.

The problem that many companies encounter during digitization is that digital boundaries are fuzzy, making security more challenging. This ambiguity supplies numerous opportunities for accidental data leaks and cybercriminal exploitation involving human operators. The resulting gap in security is due to the dynamic nature of new modes of work driven by cloud computing, work from home, and an expanding security landscape.

The key to digital transformation success lies in controlling these fuzzy borders using adaptive, intelligent, and identity-based access control. An identity-based zero-trust approach can accelerate your journey to successful digital transformation.

THE WHO, WHAT AND WHY OF DIGITAL TRANSFORMATION

Innovating new ways of working or new models of production are critical shifts that drive businesses forward and come in many forms. Gartner has named the top three business trends: growth, digitization, and efficiency with digitization being the pivot for the other two trends. Digitization adds value and efficiency to a company and its processes, and the market for digital transformation is predicted to grow to $2.4 trillion by 2024. This trend is one of the most disruptive to business as usual in recent years.

THE DRIVERS AND ENABLERS OF DIGITAL TRANSFORMATION

As with any momentous organizational change, there are drivers and enablers pushing projects forward. While the specifics of each organization will differ, the generalities of this transformation broadly apply. It is entirely up to each organization to choose how they respond to these circumstances.

> ***Digital has radically shifted where threats come from and how quickly they emerge... cybersecurity is now a top board agenda item.”***
> McKinsey

DRIVERS OF DIGITAL TRANSFORMATION

- **Customers:** Technology used well promises to create fantastic customer experiences. The “total experience” (TX) combines customer (CX), user (UX), and employee (EX) experience. Gartner highlights TX as a competitive edge, saying that “organizations providing a total experience (TX) will outperform competitors by 25% in satisfaction metrics.”
- **Efficiency and automation:** Automation is parallel to digital transformation, providing the rails to drive efficiency, reduce human error, and unlock new value for a business.
- **Competitive edge and revenue generation:** Digital tools empower digital marketing and firms with a mature digital strategy had a 23% increase in growth.
- **New working practices:** A remote-first culture has emerged over the past few years with a need to accommodate always-on, anywhere, and secure access.
- **Mobile and eCommerce buying:** Customers are making more digital-first purchases which has changed consumer interactions and metrics.
- **Access to innovative productivity tools:** Digitally transformed processes are built upon a wealth of intelligent technology now accessible to companies of all sizes.

ENABLERS OF DIGITAL TRANSFORMATION

- **Cloud computing and cloud-native tools:** Software as a Service (SaaS) is the lever of digital transformation. Without the accessibility and capability of the cloud, digital-first could not happen.
- **APIs and open data:** Application programming interfaces (APIs) connect disparate parts of the digital landscape, and data drives the engines generated by API-enabled apps. Data is now enabled to flow freely to deliver digital services.
- **Everything as a Services (XaaS):** These flexible models supply the commercial mechanisms to deliver the digital transformation of services to organizations.
- **Big data and the data fabric:** Data provides the foundation for digital tools to generate insights and take prescriptive action.
- **Zero-trust security and identity-centric access:** A robust and flexible security model for a digital-first approach that lowers the risk of a cyber-attack and data exposure.
- **Identity and zero-trust are intrinsically linked.** This model of securing and authorizing access is a fundamental framework needed to add the security layer to digital transformation projects.
- **Artificial Intelligence (AI):** By handling the massive amount of data generated by apps and devices, AI can augment many services and supply new opportunities for an organization.
- **5G:** At around 10X the speed of 4G, this next-gen cellular connectivity provides the capacity and latency enhancements needed to ensure that connected devices and automation work reliably.
- **Hyper-Automation: Digital transformation uses a range of automation technologies**, which is the integration of various technologies, including Robotic Process Automation (RPA), AI, and data analytics.

DIGITIZATION:
ANYWHERE, ANYTIME – BUT ALWAYS SECURE

Companies across the world are adopting cloud infrastructures and digitizing their business processes. The benefits of performing this shift are clear: improved efficiency, business agility, productivity, and a great TX. According to **McKinsey**, the positive nature of digital transformation has reached the desk of the CEO and the board. At this level, the sign-off requires careful consideration of the key drivers and enablers to ensure that any digital transformation project is successful.

And yet, digital transformation is not an easy exercise. Research by the **Boston Consulting Group** (BCG) found that only 30% of digital transformation projects were successful. However, BCG also finds ways that a company can take a project to a successful conclusion with one of the key requisites being the deployment of a "modern technology architecture driven by business needs to enable secure, scalable performance, rapid change deployment, and seamless ecosystem integration."

A critical factor in successful digital transformation is removing the increased risk of connecting people, data, and devices. Companies today cannot afford to compromise on security; therefore, digital-first must fully embrace security-first.

WHY SECURITY IS VITAL FOR SUCCESSFUL DIGITAL TRANSFORMATION

In 2021, an **enterprise's average number of SaaS applications was 110**. In addition to these modern applications, there are numerous legacy, thick client, and on-premises applications that significantly expand organizations' attack surface.xi

These applications generate an astounding amount of data that is used across the cloud and between devices and people. The result can be overwhelming for IT and security departments, who must continuously put out security fires.

DATA SECURITY STATISTICS REVEAL THE EXTENT OF THIS CHALLENGE:

- **22 billion data records** were exposed in 2021.
- **82% of data breaches** involve a human being.
- Cybercriminals can breach a perimeter and access local networks at **93% of companies**.
- In 100% of companies, domain privileges allow access to other key systems,
- Cyber-attack attempts increased by **50% in 2021**.
- In 81% of FTSE 100 companies, at least one credential was compromised and exposed on the dark web; **42% have more than 500 compromised credentials** exposed on the dark web.

Where the digital and human dovetail, a weak spot occurs - identity. When identity fails, cybercriminals deploy tactics, techniques, and procedures to exploit this weak point.

Dynamic and adaptable methods of authenticating and continuously authorizing access to resources based on user identity are key to fixing this weakness. In addition, as digital transformation opens the way for stakeholders to access applications outside the network perimeter, keeping enterprise IT infrastructures secure is a task for identity-based access.

Digital business demands modern authentication and identity-based access is needed now more than ever.

THE WEAKEST LINK: HOW IMPLICIT TRUST LETS ENTERPRISES DOWN

User identity is a weak link in security, with hybrid and remote working increasing the risk of employees being targeted by cybercriminals. It is the human factor that leads to insecurities, and implicit trust simply does not work within an IT infrastructure that is inherently open and massively connected.

The digital enterprise expands the attack surface as it adds new endpoints. Mobile devices, remote work, BYOD, IoT, and so on are all part of a widely spread tech fabric that depends on massive data sets. This increases the risk of a data breach, and poorly controlled access and authentication deliver vulnerabilities into the hands of cybercriminals.

The good news here is that the weakest link, user identity, can be augmented and secured by deploying identity-based access and connectivity strategy solution during the digital transformation process. A security strategy that encapsulates digital transformation should have a coordinated approach across IT, OT, and IS, as the threats from bad actors exploiting weaknesses in old authentication infrastructure are increasing.

> ***Increased trust is needed for employee identity verification.***
>
> World Economic Forum

AREAS AN IDENTITY STRATEGY SHOULD FOCUS ON:

Poorly controlled authentication and authorization: When there's little or no control over access to critical apps and data, cybercriminals have an open door to wreak havoc. Authentication and authorization should not be viewed as an on-off switch. Rather, dynamic control over access to sensitive data should form the core of any digital transformation program. Organizations need a modern authentication solution that covers the entire risk spectrum inherent in connecting users to applications. Simultaneously, they must ensure the accessibility and usability of every resource and asset without compromising security.

Social engineering: Social engineering attacks, in which bad actors manipulate users into divulging their credentials or other sensitive data, **increased by 270% in 2021**. Employees are in the maelstrom of these attempts, which often result in the theft of large sums of money. Having control over employee identity and enforcing robust access and authorization provides a solid backbone for hardening a company against social engineering attempts.

Phishing: Phishing is often associated with social engineering, used to trick users into performing a behavior that helps a fraudster. A 2021 Cisco report placed phishing as one of the top two threats to business, with **86% of employees clicking on phishing links**. One-click is all it takes to steal login credentials. A "2022 Annual Identity Exposure Report" found that **1.7 billion credentials were exploited by cybercriminals in 2021**.

Insider threats: Accidental insiders can be as destructive as external hackers. Credential exposure can be caused by careless employees and malicious attempts at unauthorized access or misuse of privilege. A 2022 study by the Ponemon Institute into the cost of insider threats found that **56% of cyber-attacks were due to employee negligence**. The study also found the cost of **credential theft has increased by 65%**, from $2.79 million in 2020 to $4.6 million at present.

Identity theft: In 2021, **15 million Americans had their identity stolen**, according to a 2022 study from Javelin. A stolen, or synthetic identity is like a forged key; it can open digital doors. Therefore, digital transformation programs need to be hardened against fraudulent identities.

Poor password hygiene / Credentials sharing + generic accounts: Insecure passwords continue to plague the security of digitally transformed enterprises. Shockingly, **60% of users** reuse passwords, and **52% reuse passwords across multiple accounts**. In addition, **42% of employees share passwords** with co-workers.

WHAT ABOUT REGULATIONS AND STANDARDS?

The digitization of services and processes places companies at risk of non-compliance with data protection laws. But security and compliance are intrinsically linked. By creating a secured environment during a digital transformation project, maintaining regulatory compliance will naturally follow.

Globally, the data protection landscape is fluid and evolving; by addressing the areas of weakness in an organization, namely the human factor and identity and access control, organizations can more easily meet the stringent requirements of data protection and privacy laws. Areas such as identity-centric access control and zero-trust provide the backbone for robust security measures. Using these methods provides a natural fit with many data protection regulations and laws focus on identity and access control and zero-trust.

Some examples include:

- EU - **NIS 2 Directive** (Network and Information Security (NIS) Directive)
- UK - **DSPT** (Data Security and Protection Toolkit) standard 20-21
- U.S. - **HIPAA** (Health Insurance Portability and Accountability Act)
- U.S. - **White House Executive Order on Cybersecurity**
- U.S. - **CISA documents on Zero Trust**

VERIFIED IDENTITY ENABLES DIGITAL TRANSFORMATION

As we have seen, cybersecurity attacks are increasingly linked to human factors, with credential theft and poor credential hygiene being at the core of many security incidents. This finding maps to **a recent report on digital transformation** and the cloud that surveyed 500 institutions for insights into what is needed for an effective plan. The study placed cybersecurity as a top priority and enabler of digital transformation.

This industry research plays a crucial part in supplying key insights and supporting businesses in creating and implementing a digital transformation plan that prioritizes identity and access control alongside the wider zero-trust security framework.

There is an alignment of planets that includes the increase in cloud technology use, compliance requirements, remote work, and total experience (TX) expectations, making a robust approach to controlling cybersecurity attacks that are human-centric imperative.

Cyolo

ABOUT CYOLO

Too many critical assets and systems remain exposed because traditional secure access solutions are not able to protect the high-risk access scenarios and legacy applications that keep modern business operations running.

Cyolo provides the only trustless zero-trust access solution, giving organizations visibility and access control over the users who leave them most exposed to risk, including third-party workers, remote OT operators, and post-M&A employees and applications.

cyolo.io