FUTURE OF PHYSICAL SECURITY

Extending converged digital capabilities across logical & physical environments

Microsoft

accenturestrategy

Table of contents

SECTION 1:

Physical Security: Long Overdue for Digital Transformation

NEW APPROACHES FOR A CHANGING THREAT LANDSCAPE

The threat landscape is changing. The digital revolution has transformed the world in a multitude of positive ways—but it has inadvertently created new threats. Social media and messaging platforms are unintentionally providing new ways to plan and orchestrate mass-casualty incidents. Over half of these active threat incidents occur in the workplace. Coupled with the escalation of catastrophic climate events such as hurricanes, security teams are facing mounting challenges.

Combating these threats requires intelligent applications that can rapidly sift through overwhelming amounts of data that cannot be processed at the human level. Recent developments in artificial intelligence and signals processing can help security catch up. As tools become more sophisticated and readily available, security organizations must adopt new practices and capabilities. Failure to transform will increase the likelihood of becoming a target.

In 2018, Microsoft and Accenture conducted a "Future of Physical Security" survey. 200 senior physical security leaders across multiple industries participated. We found that although security leaders see the opportunity to enhance risk management with digital capabilities, the industry is at various levels of maturity, and at worst is a decade behind. Respondents identified "reactive threat management" and "intuition-led decision-making based on subjectivity" as the two leading challenges facing physical security operations today. These challenges—operating reactively and improving decision-making—make it difficult to be proactive. This puts your people, brand and reputation at risk.

> **"Cloud computing, artificial intelligence and machine learning with edge IoT are blurring the lines between logical and physical environments. Traditional security risk management and threat detection are quickly becoming obsolete. Security leaders who do not embrace a digital mindset risk becoming business irrelevant."**
>
> **– Michael Foynes, Senior Director, Microsoft Global Physical Security Operations**

The security industry is facing a huge digital disruption, and to be successful, it needs to embrace digital transformation. Maintaining the status quo will only increase this gap and prevent companies from capitalizing on a valuable opportunity. By challenging conventional thinking and reimagining how business is done, physical security can provide next-level insights, improving life safety and creating value across the organization beyond traditional risk management.

THE DISRUPTIVE FORCE OF DIGITAL TRANSFORMATION

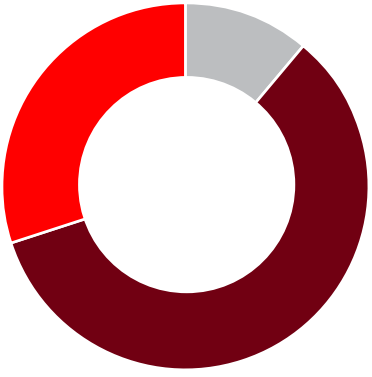
Organizations are complex ecosystems. When people, processes and technologies are connected and working together across an organization, it improves business performance.

Sometimes, to improve efficiencies and break down silos, change is necessary. In the Microsoft-Accenture Survey, 89% of Security leaders stated that digital transformation was important (see Figure 1).

However, only 30% deemed it urgent. This is in stark contrast to a key finding from a Harvard Business Review: 47% of business leaders across industries believe their business model will be obsolete in the next two years. This makes digital transformation a matter of survival.

Digital transformation of physical security is still in its infancy compared to other industries. This threatens organizations' high-value assets—both employee life safety and intellectual property—and can result in missed opportunities to significantly raise the organization's bottom line.

Figure 1: Level of Priority for Digital Transformation
Security leaders understand and recognize the importance of digital transformation.



30%
Important and urgent

59%
Important but not urgent

11%
Not important

35%
Percent of C-level executives indicating digital transformation is important and urgent

30%
Percent of non C-level executives indicating digital transformation is important and urgent

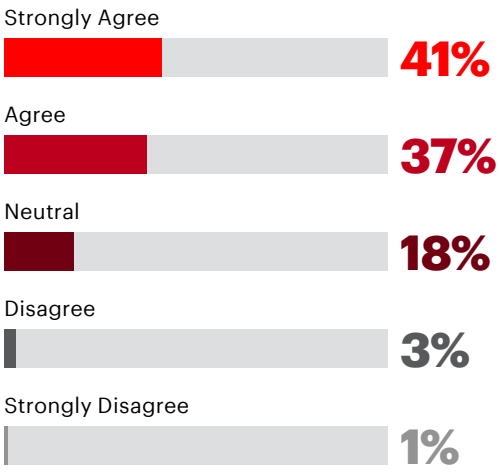
Source: 2018 Accenture-Microsoft Security Survey

RETURN ON INVESTMENT

Traditional measures of investment success, such as return on investment (ROI), highlight the direct benefits of digital transformation. Beyond improved responsiveness to threats and more effective risk management, new physical security models deliver faster response times at a lower cost, better security asset utilization, and improved lifecycle management. Additionally, more than 80% of security leaders believe that digital transformation will deliver significant non-financial benefits such as an enhanced employee experience; converged cyber and physical intelligence; and environments that are not only smart but aware.

Figure 2: Return On Investment

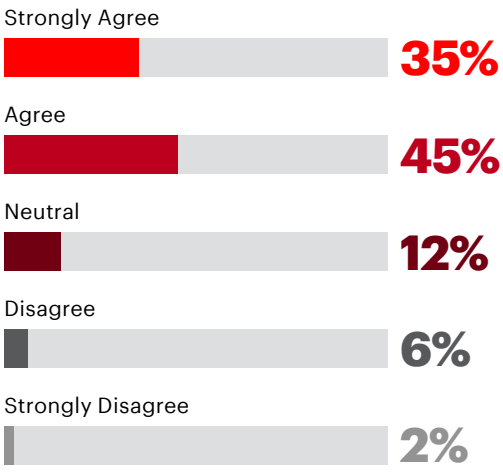
More than half of the respondents believe digital transformation of physical security will generate a meaningful return on investment (ROI).



Source: 2018 Accenture-Microsoft Security Survey

Figure 3: Non-financial Benefits

A majority of respondents believe that digital transformation delivers non-financial benefits that are worthwhile investments to the organization, regardless of ROI.



Source: 2018 Accenture-Microsoft Security Survey

By leveraging technology to generate greater intelligence, physical security will also be able to do more with less, improving operating efficiency and reducing operating and capital expenses by up to 30-50% (depending on rollout and the size of the organization). To generate further value, organizations could take their solutions to market in a "security-as-a-service" model to help the industry as a whole achieve widespread transformation—unlocking significant business opportunities.

The value proposition of digital transformation goes beyond the traditional ROI metrics. A combined view of returns should also measure Return on Data (ROD), or the value created from data by solutions such as advanced analytics, artificial intelligence and machine learning. Security leaders can leverage these systems to create compelling insights that can be shared across the organization to not only identify potential security vulnerabilities but to drive efficiencies, increase cost savings and elevate customer trust by preserving privacy and security.

> **Digital transformation is a new opportunity to provide clarity and solutions to problems in security.**
>
> **– Jeff Spivey, President of Security Risk Management**

No matter which metric the organization prioritizes, a data strategy will be required to optimize the outcome. An effective strategy will enable physical security to become the core intelligence platform of the organization, transforming from a cost center into a value hub.

SECTION 2:

Innovative Risk Management

Digital transformation reimagines risk management. Within security there are three elements that were either not possible before or are greatly enhanced by digital transformation: Dynamic Identity Management, Robust Threat Detection and Investigation, and Unification of Physical and Cyber Security.

DYNAMIC IDENTITY MANAGEMENT

Dynamic identity management authenticates identity—not just credentials—and eliminates the reliance on access tokens like badges and cards.

It's important to clear up the difference between authenticating credentials and authenticating identity. Many security organizations assume they manage two identities: a logical identity for the network (user profiles, passwords) and a physical identity for access to physical environments (badges, cards).

However, this is credential authentication, not actual identity authentication. To enable a single digital identity that is authenticated across logical and physical environments, security organizations need a combination of digital capabilities including facial recognition, video analytics and IoT sensors. In effect, these digital representations of physical environments combine to make logical and physical environments one and the same. Now the same tools that are used for cyber threat detection can be extended into the physical space without any customization or reconfiguration.

Dynamic identity management provides identity authentication, determines access privileges in real-time and enables identities to be tracked throughout digital and physical environments. Imagine that a datacenter technician enters a data facility and is immediately identified through facial recognition, automatically granting access to authorized areas. As the technician moves through the environment, IoT sensors and devices collect additional intelligence in real time, tracking movement and activity.

Using this data, the dynamic identity management system learns the technician's normal patterns for accessing server rooms and associated service requests and builds a behavior profile.

One day, the technician attempts to enter the main server room and the system recognizes that there are no corresponding service requests. The same learning engines that are used to pinpoint a suspicious activity—like an unauthorized user attempting to access a network—detects an unauthorized entry attempt. As this anomaly is detected, quick action by a digital officer or smart bot mitigates the threat by removing the technician's access.

Digitizing an individual's physical identity allows security organizations to leverage cyber skills and capabilities in the physical environment. By viewing the physical world as a network with a single identity, security organizations are better equipped to handle dynamic access management.

DEFINITION: DIGITAL OFFICER

A security officer digitally enabled with data insights in real-time to respond to incidents

SCENARIO: DATA CENTER TECHNICIAN

01 Data center technician arrives at data facility for work, facial recognition clears them for entry to the environment based on their dynamic risk-profile

02 IoT sensors and devices monitor locations and converges physical and cyber security to facilitate and control access

03 IoT sensors and devices record individual's interactions with an environment (e.g., location, time, etc.)

04 IoT sensors establish a baseline behavior of a profile user and detects and recognizes uncorrelated users

05 Employee attempts to enter unauthorized area of data center

06 The combination of logical and physical identity pinpoints the suspicious activity, guiding the digital officer to remove the technician from the environment

A BENEFIT FOR CUSTOMERS

Customers also receive a better experience when dynamic identity management is deployed. London's Heathrow Airport and the UK Border agency teamed with Accenture to create an interconnected system of data streams, biometrics and facial recognition tools to match identity and passport data with incoming travelers. The system monitors activity and ensures that travelers stay on the right path and verifies that identities match documents. For both security and travelers, the experience is simple, efficient and effective.

ROBUST THREAT DETECTION AND INVESTIGATION

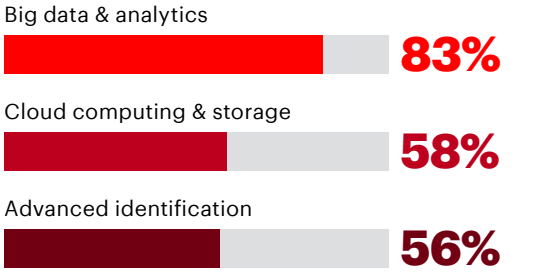
Ideally, every security professional would have the tools to proactively assess and manage risk. However, the complexity of managing current threats often gets in the way, leaving less time to focus on proactive threat management. Digital transformation empowers these operators with systems that contextualize data to identify threats before they occur, mitigate risks and better ensure life safety.

Today's model relies heavily on manual processes, which often results in missed signals. It is nearly impossible—not to mention costly—for humans to monitor all security content without digitally powered analytics. That's why it is commonly estimated among security professionals that more than 90% of security video footage goes unseen and is typically watched only for reactive investigation.

Physical security leaders know this model needs to change, and that data and analytics is the answer: over 80% of surveyed participants identified big data and analytics as a top three investment for the next 3-5 years.

Figure 4: Top Investments

Over the next 3-5 years, security leaders selected the following as their top three areas of investment.



Source: 2018 Accenture-Microsoft Security Survey

As physical security organizations transform to harness the power of data, they must also make data protection and privacy a priority. Currently, the General Data Protection Regulation (GDPR) requirements provide a clear guide to compliance, but data management systems should be flexible as regulations continue to evolve in the future.

Monitoring and analyzing data is only half of the equation: intelligence must be connected with people who can act on it.

That's where Digital Officers play a crucial role. Digital Officers respond to emergency and routine incidents on site, report data for incident activities to improve machine learning, and receive remote data to prioritize risk.

Of course, physical security is only as good as the intelligence it holds. By providing Digital Officers with a platform that collects, contextualizes and presents the right data at the right time, they will not only improve security, but also impact other functions ranging from maintenance to real estate services.

Figure 5: Digital Officer
The Digital Officer will interact and engage within digital enabled environments by integrating the front-end experience and back-end data systems for a proactive security model.

Facilitate.

I interact with employees, customers and partners to ensure life safety measures are current and persistent at all times.

Respond.

I am representative of a risk model within smart and aware environments. I am present to respond to data-informed emergency and routine incidents.

Report.

I provide incident activity data to improve machine learning and I receive remote data to prioritize risks.

UNIFICATION OF PHYSICAL AND CYBER SECURITY

The growth of Internet of Things (IoT) devices and sensors has increased the potential surface area for attacks, posing increased risks and vulnerabilities to physical and cyber worlds. These threats are very real. A nuclear power plant in Germany was found infected by computer viruses perpetrated via a cyberattack, risking physical control of the plant and sensitive information to hackers.

Today's threats often keep one foot on each side of the physical and digital divide. These blended threats require connecting data, building new capabilities and gaining new insights to allow security teams to better defend against attacks. 75% of physical security leaders are aligned to this vision, indicating that the convergence of physical and cyber security will reduce threats and vulnerabilities in the physical environment. In addition, over 60% of physical security leaders believe that this convergence will come in the form of data and new or emerging capabilities.

Unifying cyber and physical unlocks powerful new scenarios. For instance, cyber teams faced with intruders can quickly connect the cyber footprint to a physical location. By mapping cyber and physical presence against one another,

it's possible to understand where the threats originate. If an intrusive device is planted within an environment, the cyber teams can now track its presence to its origin and identify those responsible for bringing it in. This provides a better view of the threat and more tools to protect valuable assets. Converging physical and cyber identity is an example of how organizations can better prepare for security threats through digitizing physical spaces and allowing digital security tools to extend to the physical space.

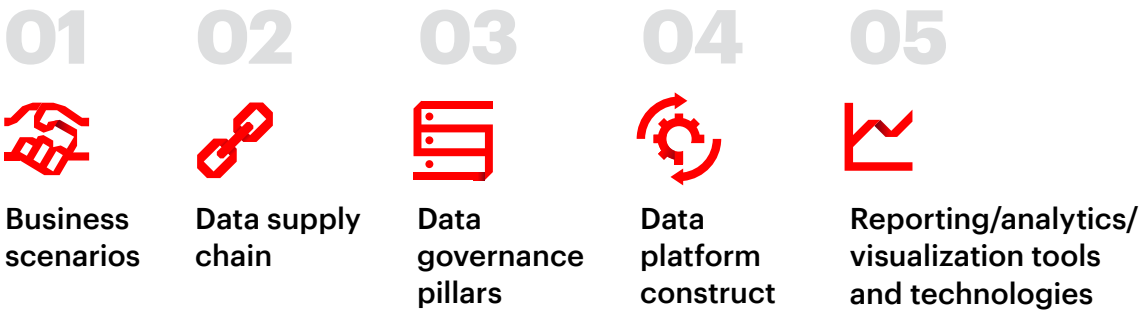
Once matured, the security platform can also be connected with teams beyond cyber. Real estate teams, for example, can leverage portions of the data to better understand space usage and design better workplaces.

Note: The use of the data by non-security teams would need to be done in a privacy compliant manner.

To combine physical security with digital solutions such as artificial intelligence and machine learning, organizations need a well-formed data and analytics strategy, as well a sophisticated data and analytics platform.

The data and analytics strategy is comprised of five sections, shown in the figure below.

Figure 6: Areas to Cover with Your Data and Analytics Strategy



All of these components come together in the data platform, typically built on a cloud-based solution, where data is ingested, processed, analyzed and then distributed to the teams.

> **Thought diversity is very important—we need to tear down the walls between physical and cyber security.**
>
> **– Vice President of Global Security, Global Television Network**

We find ourselves at a crossroads. The convergence of physical and cyber, of people and things... all intersect at the Digital Transformation. Will you seize the opportunity to lead and disrupt, or lag and be disrupted?

– Philip Halpin, Senior Vice President Global Security, Brown Brothers Harriman & Co.

Many will perceive unification as a threat to physical security. Instead, it's an evolution that brings together complementary skillsets and enables a more effective physical security model. Leading companies are already creating "Fusion Centers" that bring together all areas of security—including physical and cyber—to accomplish more together.

CASE STUDY

THE FUTURE IS TODAY: SINGAPORE'S "SAFE CITY"

These three themes aren't purely hypothetical ideas meant for the distant future—they are currently being implemented by others today. In partnership with Accenture, Singapore's "Safe City" initiative sought to better understand, mitigate and predict future security threats.

SOLUTION

Video and sensor analytics were utilized to enable the Singaporean Government to share data among agencies easily and deliver actionable insights for users in accordance with a wide range of requirements

Singapore's "Safe City" initiative incorporated many of the three themes to better understand, predict and mitigate future threats.

RESULTS

- 85% accuracy in crowd activity detection
- Predictive crowd model using surveillance & GPS
- Anomaly detection on social media
- Real-time decision-making
- Better collaboration and sharing of data

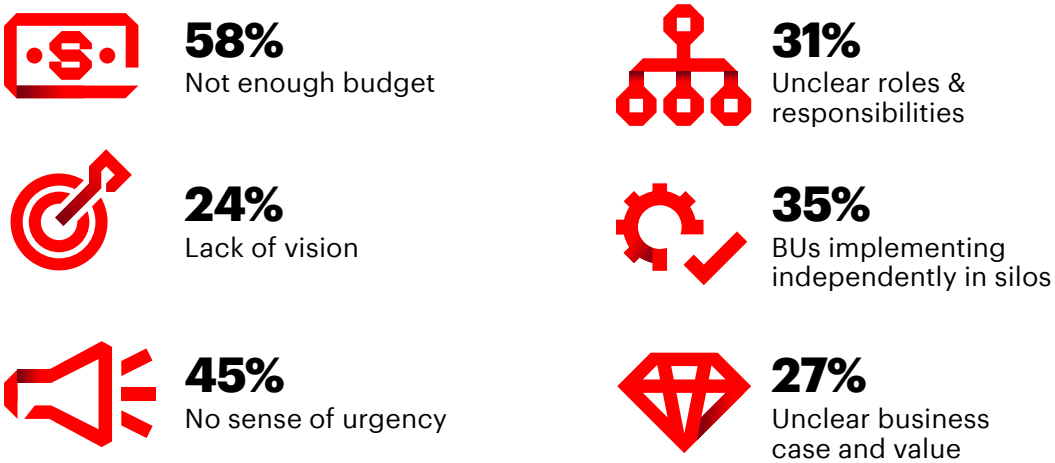
SECTION 3:

Keys to Successful Transformation

A successful digital transformation requires three elements: digital thought leadership, unified strategy and persistent innovation.

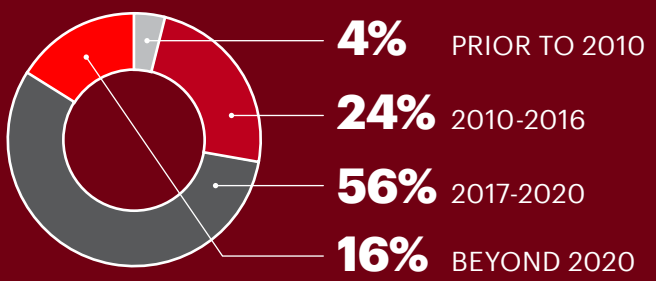
While physical security leaders agree on the importance and value of digital transformation, 45% of physical security leaders indicate that "no sense of urgency" is among their top three challenges preventing successful digital transformation. Furthermore, there appears to be a disconnect between the urgency felt by business leaders and security leads. In a 2017 Harvard Business Review study, 84% of respondents said their industry had already passed, or would pass, the disruption inflection point by 2020. This contrasts sharply with responses from the security survey. How can we drive transformation in an industry where pre-digital processes are entrenched?

Figure 7: Top challenges for implementing digital transformation
Security leaders selected the following as their top three challenges.



DIGITAL INFLECTION POINT IS IMMINENT

Percentages indicating their industry has already reached its point of disruption or will within the next three years.



Source: Harvard Business Review Analytic Services Survey, December 2016

DIGITAL THOUGHT LEADERSHIP

Successful digital transformation starts at the top. It is incumbent upon leadership to drive change and create a digital culture that is value-driven, outcomes-focused and based on continuous improvement. Creating this culture requires putting the right building blocks in place:

01

Put the customer first
Balance risk with delighting the customer. Security should be a seamless part of the process that supports, not hinders, the customer (and employee) experience.

02

Change your mindset
Foster an agile, innovative mindset that encourages constant innovation and builds up your risk tolerance. Only then will security stay ahead of threats.

03

Think collaboration
Build deep cross-functional partnerships which will enable the sharing of data, insights and knowledge. Improving risk management and life safety is priority number one, but once systems are in place, insights can be leveraged across the organization.

04

Cultivate a next-gen, diverse workforce
Ensure the right skills are in place to support the new digital services enabled by digital transformation. Upskilling and retooling staff is vital, specifically in the area of technology, data and analytics and business acumen.

05

Build a digital culture
Create a culture of digital pioneers empowered with the right learning opportunities to work in the operating model of tomorrow and prepare the people for massive transformation.

UNIFIED STRATEGY: VISION TO EXECUTION

> **In digital transformation, strategy must come before technology.**
>
> **– Don Erickson, CEO, Security Industry Association**

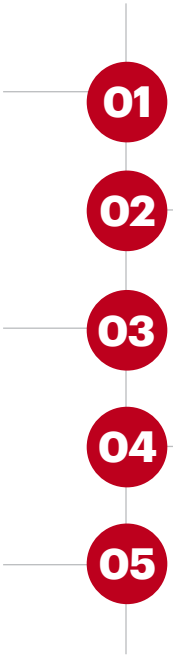
Before considering new technologies, leaders must develop a unified transformation strategy. This begins with a strong and compelling vision that can help develop a sense of ownership for security team members.

Microsoft Global Security partnered with Accenture to implement a human-centric approach to digital transformation, done in five steps:

VISION
Unite the organization around a single, unified vision that captures your aspirational goals and the value and benefits received.

ENABLING CAPABILITIES
Identify and organize the capabilities required across people, process and technology to support the created future state scenarios.

EXECUTION
Coordinate efforts and timing for the Digital Transformation with a multi-tiered, prioritized program roadmap and clearly defined governance structure.



PERSONAS & SCENARIOS
Define the new future with a human-centric approach, using personas and hero scenarios to translate the broad visions into real experiences for real people.

INITIATIVES & ROADMAP
Uncover new opportunities for value by rationalizing in-flight projects with digital transformation projects to identify overlaps, gaps and dependencies.

This approach enables physical security to bring the collective organization together, pave the way for a successful execution and design for continuous improvement and future needs.

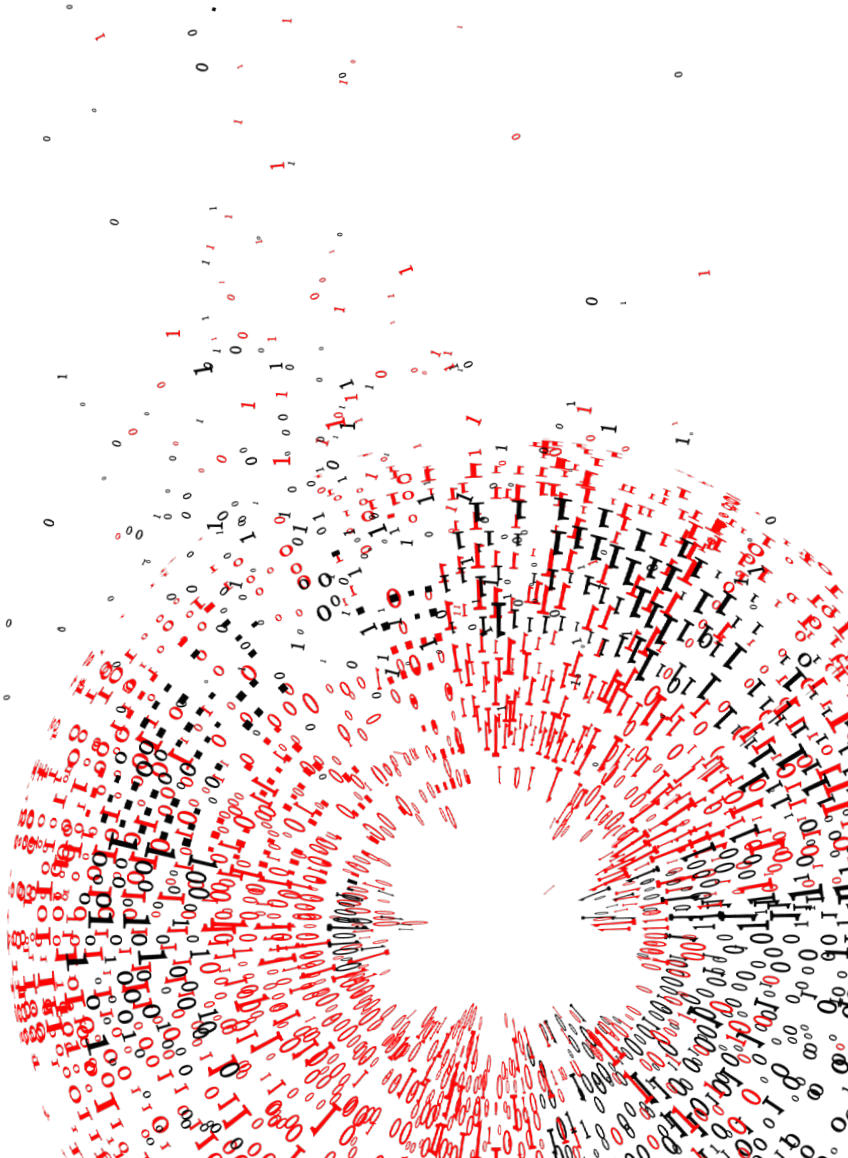
THE FUTURE OF PHYSICAL SECURITY

If digital transformation has not already shifted how security organizations operate—from reactive to proactive, from manual to intelligent—it will. 89% of physical security leaders surveyed agree that physical security needs to become predictive and are investing in technologies to deliver these capabilities.

Physical security leaders indicated that their top investments over the next 3-5 years are big data and analytics, cloud computing and storage, and the Internet of Things (IoT).

The future of physical security with digital transformation will be drastically different than physical security today. Teams will be able to predict and mitigate threats before they occur, freeing up resources to focus on strategic action and decisions. Every step forward in transformation is a step closer to realizing this vision.

> **We're just scratching the surface. The holy grail is being able to predict incidents before they occur and prevent them.**
>
> **– Michael Gips, Chief Global Knowledge and Learning Officer, ASIS**



SECTION 4:

Starting a Digital Transformation

Digital transformation is not a destination—it is a journey. Every digital transformation should start with a clear vision that is communicated by leadership. This vision should also prepare team members to expect disruption as part of the process; incremental growth will take too long and preserve too many legacy systems. A team that understands this reality and meets every challenge with a solution-oriented mindset will succeed.

The transformation team should be empowered to look internally and externally for solutions. Many of the tools that will move physical security into the New, such as facial recognition, AI signal processing or video analytics, have to be customized or even built in-house. These choices must be balanced to deliver business outcomes within defined budgets.

No matter the challenge, digital transformation is possible if it is prioritized and if businesses make the right partnerships. Microsoft approached these challenges head on and is in the midst of creating a new solution based on a mix of internal and third-party components.

Microsoft's Digital Transformation Journey

Microsoft has identified four pillars as key elements for enterprise-level digital transformation: engaging customers, empowering employees, optimizing operations and transforming products.

Microsoft began the journey by reimagining the customer experience to deliver hyper-personalized experiences. After shifting to a customer-obsessed mindset and data-driven culture, Microsoft is able to deliver transformative products and services to customers.

Engage customers

Microsoft's engagement strategy ties together customer insights across all channels. That builds deeper more contextual relationships across all segments for customers.

Empower employees

Microsoft is helping employees achieve more by creating a modern workplace that's intelligent, flexible and secure.

Optimize operations

By building state-of-the-art digital services on flexible and scalable platforms, Microsoft is creating operational and process efficiencies that reduce cost.

Transform products

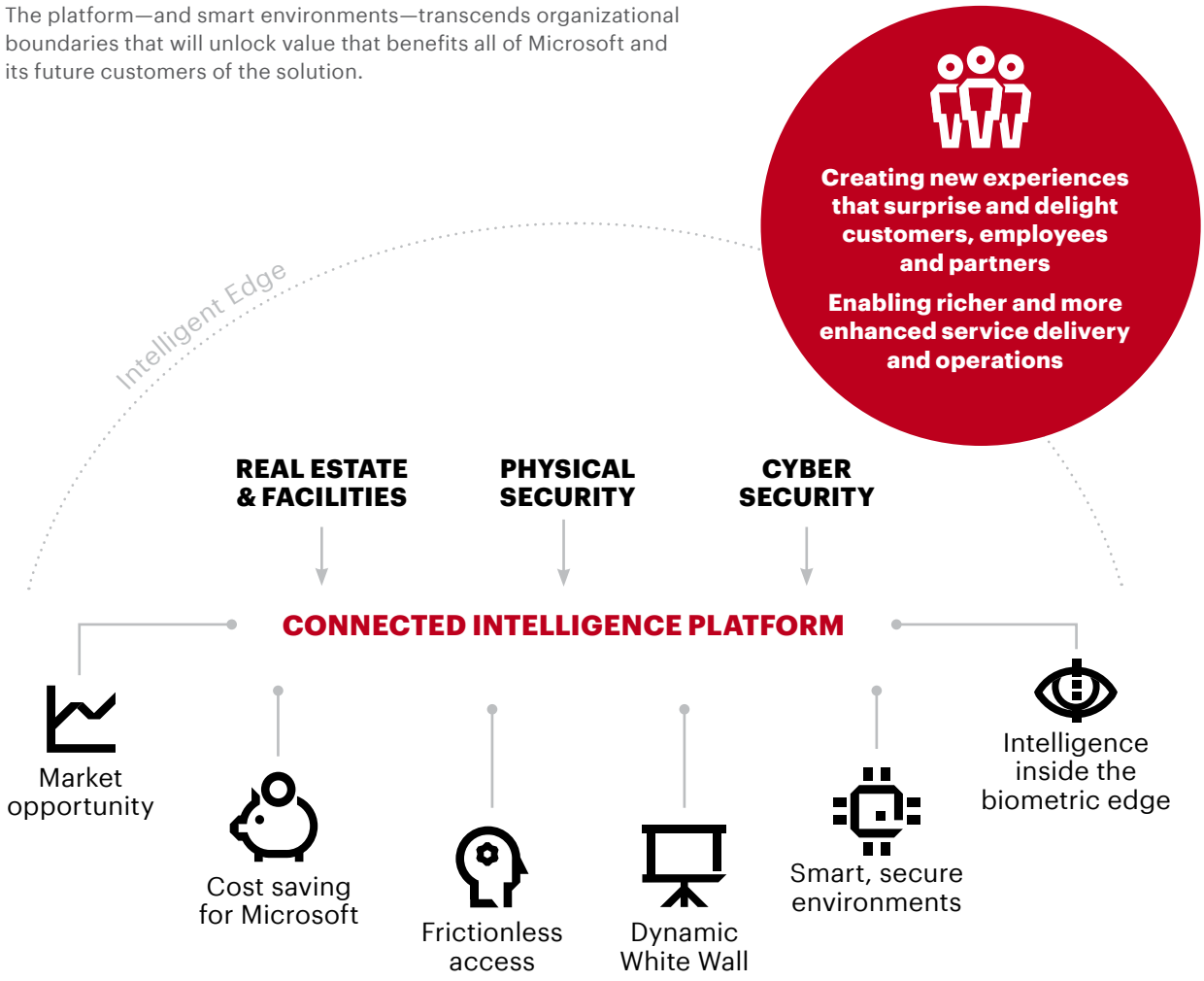
Microsoft uses data to reinvent business functions and unlock the power of intelligent technology to transform products, services and business models.

MICROSOFT GLOBAL SECURITY

Microsoft Global Security has several initiatives underway to digitally transform physical security into a more efficient, effective and intelligent model. These initiatives, codenamed Project Falcon, will create an intelligent platform that leverages data and insights to reimagine the employee experience and security delivery. Microsoft will potentially have significant cost savings through TCO reduction over the next 10 years. At the same time, digital transformation will strengthen global risk management, elevate employee and customer experiences, and unify groups within Microsoft to achieve more together.

Figure 8: Connected Intelligence Platform

The platform—and smart environments—transcends organizational boundaries that will unlock value that benefits all of Microsoft and its future customers of the solution.



The technology for this transformation did not exist when Microsoft started its journey. To create the solution, Microsoft engaged multiple internal and external partners to craft the vision and strategy, build technology, and transform organizations and processes.

One component of this solution is a data-enabled visualization platform, known as the Dynamic White Wall. Fed by a variety of data sources, the platform synthesizes data into a single, comprehensive view of a security event and allows security operations and partners to view the same information at the same time, no matter where they are in the world.

This data-enabled platform serves as a catalyst for new, disruptive way of working. By leveraging edge computing, artificial intelligence and advanced machine learning to automate repetitive processes, it allows decision-makers to focus on complex activities that require human judgement and expertise.

Note: Combining multiple data sources would need to be done in a privacy compliant manner.

As Microsoft has shown, digital transformation is more than implementing new technology. It is a disruptive shift that changes the way security operates and engages with the entire business in a meaningful way. At Microsoft, Project Falcon will create a culture of digital pioneers, empowered with the right learning opportunities to work in the operating model of tomorrow.

THE JOURNEY HAS ALREADY BEGUN

Physical security faces a host of challenges. Inbound threats continue to evolve in complexity and variety, requiring new response strategies. The fundamental rules of business are shifting, changing the definition of success. Partners in security products operate in a mode where they dictate to a market that looks for incremental change instead of generational leaps.

However, as digital transformation sweeps the industry, traditional threat detection and risk management will become obsolete. Physical security has a real opportunity to take a leadership role in transforming the organization and creating an intelligent platform which can extend throughout the enterprise. Digital transformation is about continuously evolving to meet the needs of tomorrow, through the application of digital technologies. It's about disrupting business as we know it. It's about serving as the catalyst for change. And it's about transitioning from a cost center to a value creator.

Digital security leaders have an incredible opportunity to lead this transformation. This is the decade of opportunity for the right leaders.

Take a moment to examine your organization and ask yourself the following questions:

01 Do you understand your company's digital transformation strategy?

02 Do you have a strategy and if so, how does your strategy align to that of the company?

03 What would you change in your organization if there were no limits?

04 How will digital transformation help you implement all the changes you need to deliver increased business value?

05 What business groups will you need to partner with to successfully transform?

Authors

Michael Foynes
Senior Director
Global Security
michael.foynes@microsoft.com

Mercedes Fuller
Managing Director
Accenture Strategy
mercedes.fuller@accenture.com

Accenture Strategy

https://twitter.com/AccentureStrat

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 449,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

About Accenture Strategy

Accenture Strategy operates at the intersection of business and technology. We bring together our capabilities in business, technology, operations and function strategy to help our clients envision and execute industry-specific strategies that support enterprise-wide transformation. Our focus on issues related to digital disruption, competitiveness, global operating models, talent and leadership helps drive both efficiencies and growth.

For more information, follow @AccentureStrat or visit www.accenture.com/strategy.

About Microsoft

Microsoft (Nasdaq "MSFT" @microsoft) is the leading platform and productivity company for the mobile-first, cloud-first world and its mission is to empower every person and every organization on the planet to achieve more.