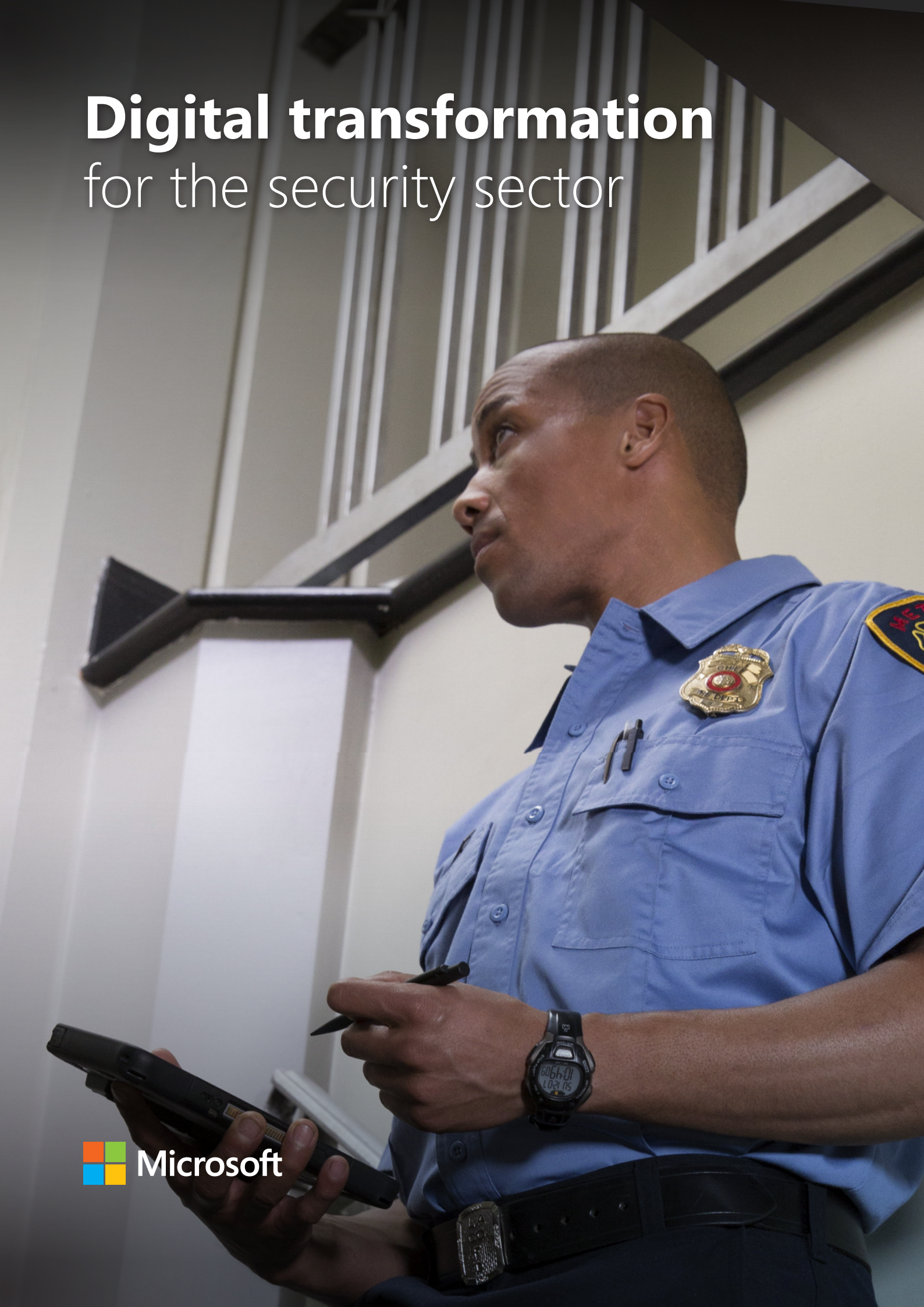
Digital transformation
for the security sector



Microsoft

Security in the era of IoT

Whole industries are being invented and reinvented by the rapid digital transformation fueled by the Internet of Things (IoT). IoT enables infinite connections between actively communicating devices from the smallest sensors to the largest industry platforms.

Devices operate silently at the edge of the network, generating, consuming, and aggregating valuable data. These devices need robust security features to prevent their identities and data from becoming compromised. While the number, type, and applications of these devices evolve continuously, security standards haven't kept pace.

Without a framework in place to ensure devices are built with security features "engineered in," every new device added to the ecosystem represents a potential new vulnerability. Deterring hostile attacks and data compromise requires a comprehensive, continuously evolving plan to assess every device, every component of the infrastructure, every member of the organization—even your customers.

A revolution of global cyber-threats is making it difficult to effectively address risks, even for organizations with enormous security budgets and elite security analysts. As tomorrow's devices are designed and marketed for mass adoption with the flattest learning curve, we will see progressively deeper integration into sensitive facets of our business and personal lives. Unfolding data security and personal privacy concerns make security a business imperative crucial for organizations capitalizing on the promise of IoT.

We have already seen this process take root for enterprise systems; demands for tight controls are driving design of large-scale systems with security features "built in." Risk awareness is already shaping buying decisions that clearly favor the most robust security capabilities.

Security and threat deterrence will drive device design and innovation, without compromise to interoperability, cost of integration, or sacrificing high-quality user experience.

Threat landscape—evolving reach and sophistication

In the early 2000s, low-impact "kiddie scripts" were mostly mischievous but didn't pose risk to operations, data integrity, or security of user identities. Organized crime syndicates soon realized the profit potential and rapidly adopted monetizing cyber-crime with sophisticated and targeted tactics like click fraud, identity theft, and ransomware. In the past three years, nation-states and terrorist groups have arrived on the scene, intent on disruption rather than just mass IP theft and profit.

The US Office of Personnel Management breach was no ordinary attack. The sensitivity of information stolen and the impact on national security of that event could make it history's most damaging assault upon the United States.

Hacking Team exploits put hundreds of millions of Flash users at risk

"An unknown group of hackers brought…surveillance firm Hacking Team to its knees when its entire network was breached—and subsequently published online."

– **Zack Whittaker**, ZDNet, January 13, 2016

"Hacking Team was in 2012 named as one of the 'corporate enemies of the internet' by Reporters Without Borders for its role in providing tools to oppressive nations."

- **Zack Whittaker,** ZDNet, July 6, 2015

Microsoft is taking a systematic approach to disrupting the attackers.

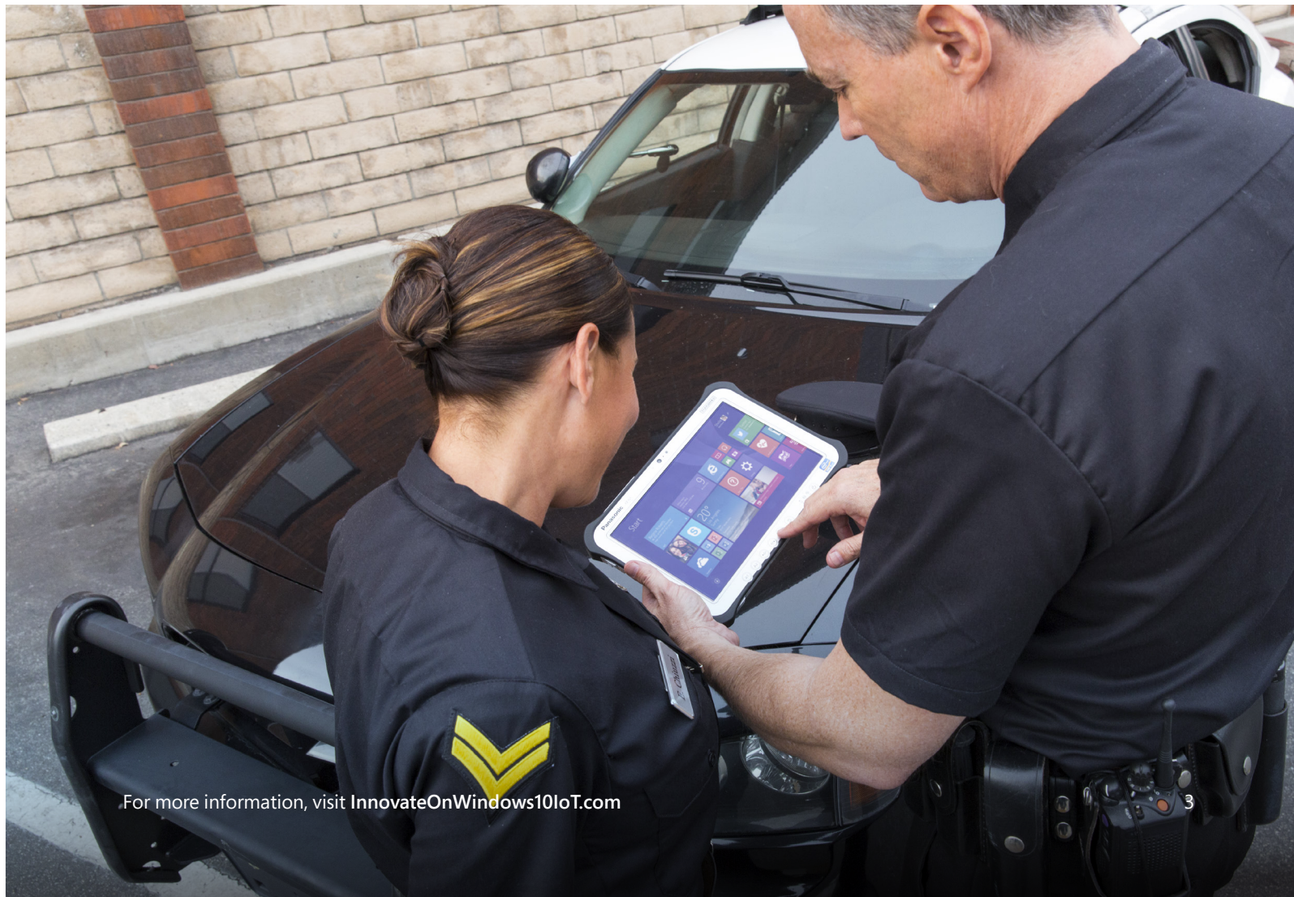
For those with profit motive, the goal is to ruin the economics of what they do. Each solution that Microsoft delivers will raise their costs substantially with the expectation of reducing the volume of bad actors in the ecosystem.

They need to break their playbook. Microsoft has telemetry data from more devices than anyone in the world and it provides great insights into what the attackers are doing and how. They tend to exploit the same underlying weakness in the platform that they've had for generations. Windows 10 eliminates these types of fundamental weaknesses by eliminating the vectors of attack themselves, implementing architectural changes—some of which use virtualization, containers, and other technologies.

The goal:
make the usual attacks obsolete, meaning the attack "*isn't just harder to do*" but instead "*it just can't be done anymore.*"

ADDRESSING THE THREATS REQUIRES A NEW APPROACH:

Security from the inside out—beyond bigger walls



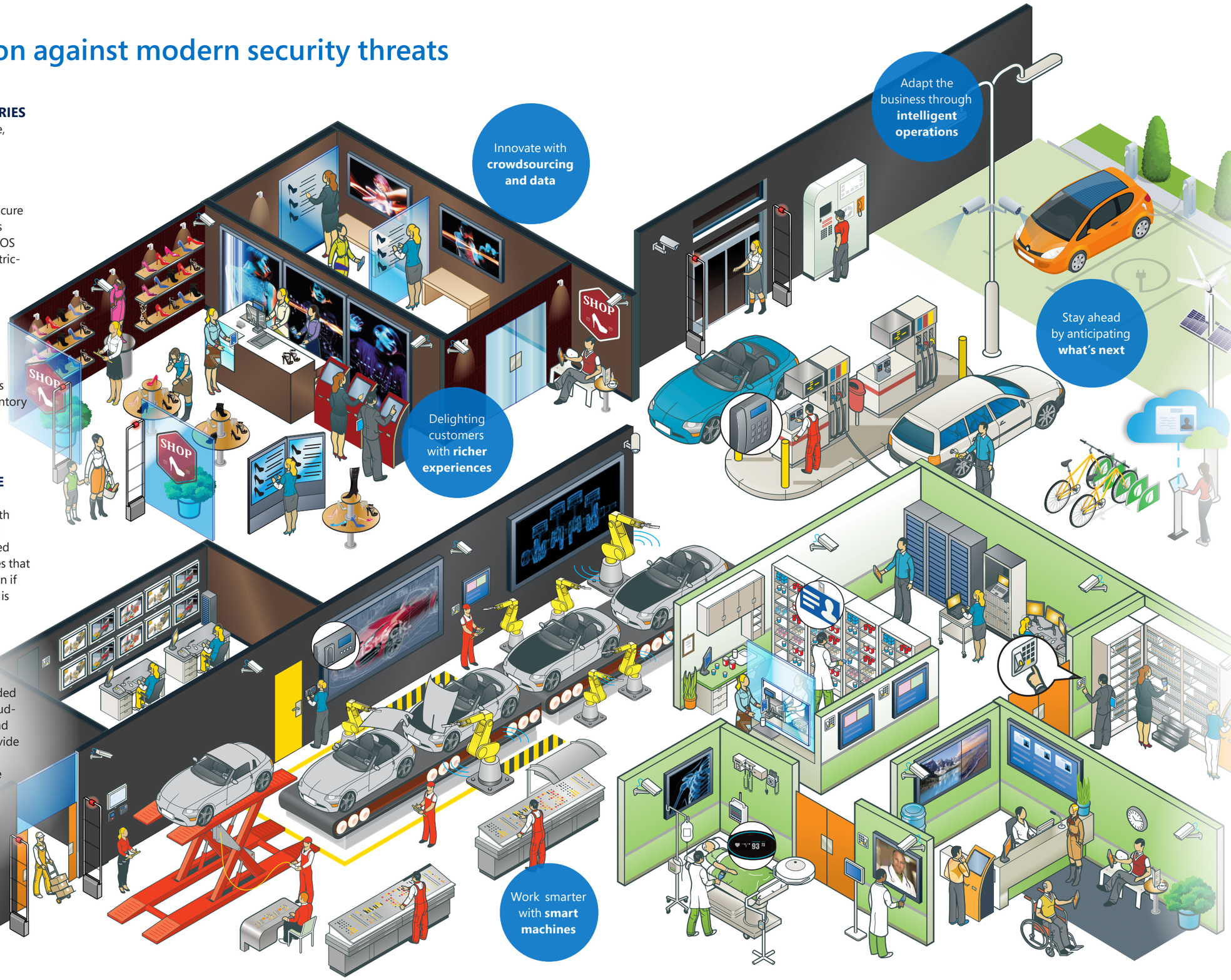
Protection against modern security threats

SECURE BOUNDARIES
with a comprehensive, holistic, end-to-end security model that encompasses your entire omni-channel infrastructure from secure e-commerce websites to FRI tags, modern POS terminals, and biometric-enabled multi-factor authentication.

ENGAGE YOUR CUSTOMERS
with richer, more profitable experiences while protecting inventory and reducing loss.

SECURE YOUR INFRASTRUCTURE
Create edge-to-enterprise security with security features built in, like hardware-based cryptographic services that protect your data even if the operating system is compromised.

EMPOWER EMPLOYEES
with security-embedded on-premises, and cloud-based productivity and BYOD assets that provide mobility, operational control, and real-time collaboration.



ENABLE NEW TECHNOLOGIES
(sustainable energy, smart grids, distributed production) with more secure aggregation of operational and financial data and customer information.

HELP SECURE DATA, IDENTITIES, AND FACILITIES
with two-factor authentication, keycard access points, and biometric sign-in.

SECURITY AND COMPLIANCE
Maximize the security of confidential data and systems, demonstrate compliance more easily, and help ensure records are in the right hands.

IMPROVE CARE OUTCOMES
with quick, security-enhanced access to the right information at the right time.

OPTIMIZE OPERATIONS
Leverage data to enhance patient outcomes and identify health trends and risks.

Give patients security-enhanced self-service access with wearables.

For more information, visit **InnovateOnWindows10IoT.com**

Protection against modern security threats

Secure hardware

Hardware manufacturing is evolving to ensure device integrity. Previously, once malware compromises a key system component, it very likely could hide and possibly even embed itself into the device hardware itself. Modern devices include Universal Extensible Firmware Interface (UEFI) and a Secure Boot feature that helps ensure that the device's firmware hasn't been tampered with. In addition, UEFI will help ensure that Windows, Linux, and other trusted operating systems will be the first software that will start on the device, rather than a low-level malware infection (such as bootkit).

Windows 10 also takes advantage of Trusted Platform Module (TPM), which provides hardware-based cryptographic services, such as certificate protection and key generation, in an isolated, secure execution environment, meaning that even if Windows is fully compromised, the data protected by the TPM can remain secure. By the end of 2016, Microsoft and OEMs expect all new devices will include TPM 2.0.

By adopting the new Microsoft Passport and Windows Hello features of Windows 10, organizations can finally move away from passwords to biometric-enabled, multifactor authentication. In response, OEMs are dramatically increasing the number of biometric-enabled devices in their portfolios.

And processor-based virtualization capabilities (Intel VT-X) now help isolate sensitive Windows components and data from hacking and malware threats. By isolating these components (such as Credential Guard, Device Guard) by using Hyper-V, Microsoft has delivered a client architecture that is similar to virtual machines in the datacenter. In this case, virtualization-based security (VBS) is being implemented at the micro level to protect Windows itself. VBS is one of the most important security changes in Windows 10 and it will also prove to be the most impactful.

Secure identities

One of the biggest challenges facing the enterprise is related to users and customer identities, which are stolen and misused at unprecedented levels. If we look back at the recent breaches, it is easy to see how devastating the impact can be when an identity falls into the wrong hands.

The challenge: User names and passwords are shared or made sharable intentionally, inadvertently, stolen, or maybe even guessed.

Attackers have proven themselves incredibly adept at stealing them. In 2014, one group claimed to have assembled 1.2 billion user name and password combinations from more than 400,000 network breaches.

> "The fifth annual SplashData chart of the Internet's worst passwords is out, and it looks like people just can't learn the lesson. The firm has aggregated the passwords from around 2 million that were leaked in 2015, finding that basic, easy-to-guess terms are still in abundance."
>
> – **Daniel Cooper**, Engadget, January 19, 2016

The solution: There are two key steps in protecting against identity theft. Authentication and derived credentials (what users use after they have authenticated).

Authentication: Deploying a two-factor authentication solution has typically been too complex and costly to provision until now. Windows 10 introduced Microsoft Passport, an easy-to-deploy two-factor password alternative that allows employees to use the devices they already have as one factor and add biometric sign-in using Windows Hello.

With breach, theft, and phish-resistant credentials in a single sign-on experience, it provides convenient, enterprise-grade security for both enterprises and consumers.

Windows 10 has all the convenience of a password while at the same time having the enterprise-grade security of today's two-factor solutions such as smart cards. Unlike those solutions, it's easy to deploy because it can all be provisioned electronically. There is no need to issue a special ID card, buy devices with a reader, use dongles, and so forth.

Derived credentials: The problem with derived credentials is that an attacker can access them, through malware or other means, and impersonate users just as if they have their password or smart card. Derived credentials are part of virtually every known major network breach. The tactic enables an attacker to hide from detection and frequently gives them the opportunity to steal even more credentials. Previous defenses for these thefts really just made the attack harder. They couldn't really stop it. Windows 10 Credential Guard fundamentally breaks derived credential theft using Mimikatz and similar credential-gathering tools.

With the addition of Azure Active Directory and AAD Join, device and solution manufacturers can enable account access for non-domain joined devices with single sign-on and manageability across disparate locations.

Secure data

Data must be secured both at rest and in transit, to be secure even if the written volumes themselves are compromised through loss or theft. The industry-leading Microsoft full-disk encryption technology encrypts the entire system volume and any partitioned data volumes on Windows 10 IoT devices. Comprehensive encryption of data-at-rest will protect written volumes from penetration. But total data security measures do not stop here.

Secured connections and device identity

Ensuring that communications among IoT devices are secured when sensitive information is exchanged is a critical requirement often overlooked with the ubiquitous availability of easily integrated devices.

In many scenarios, connected devices communicate with each other constantly. Generally, user interaction is not required to monitor, manage, or permit ongoing communications. A device that has been granted ongoing access to communicate must remain secured after the initial credentialing handshake. Using security protocols and encrypted communication does not guarantee trust because these mechanisms have historically worked under the assumption that attackers do not have physical access to the device.

The Microsoft perspective is that security implementations that are only external to IoT devices will not suffice. Robust security must be intrinsic to these devices. Enterprise-grade security requires each device be inherently secured and resilient—protecting customer data, maintaining privacy, and limiting access to other systems even if breached.

Windows 10 IoT is designed to natively support multiple encryption methodologies for communications between industry and mobile devices. It supports communications protocols for resource-constrained devices as well, helping to prevent vulnerabilities, regardless of the device types involved.

Advanced security controls within Windows 10 allow the user to differentiate device-identity protocols based on device type—a low-level device (such as a temperature sensor) can be identified with appropriate security protocols to accommodate resource constraints and business scenarios, while more robust demands are applied to more sensitive, mission-critical devices, ensuring all device identities are secured and verified, regardless of resource constraints.

Secure facilities

The security of your physical facilities is mission critical. Access tools like physical keys, key cards, key pads, bio-scanners, and security guards are just the beginning.

In the aftermath of the terrorist attacks on September 11, 2001, a noticeable increase in the number of security and surveillance measures has been observed, not only in off-hours and nighttime but in around-the-clock surveillance. In light of the terrorist attacks occurring worldwide, we are quickly becoming a "surveilled society," in which our everyday lives are permeated by surveillance encounters.

Video cameras, motion detectors, metal detectors, heat sensors, activity scanners, and proximity sensors are just a few of the devices used to monitor facility activities, personnel, and customers' behavior. All of these small devices communicate their data to a gateway, which relays that data to analysis applications.

Even the smallest of devices running Windows 10 IoT can provide support for industry-standard **Trusted Platform Module (TPM)**. Discrete or firmware-based TPM implementations provide the foundation for strong, hardware-bound cryptographic identities for authentication, secured key storage, and policy-based key usage, as well as platform integrity and health attestation through use of tamperproof platform measurements. These security capabilities help ensure that all device identities are secured and verified, regardless of resource constraints.

Systems are secured because each device is inherently secured and resilient—protecting customer data, maintaining privacy, and limiting access to other systems.

Security across industry

Security for healthcare

As recent hacks show, keeping a healthcare organization safe from security threats takes planning, technical expertise, and business knowledge. Security professionals must balance their quest for impenetrable devices, secure data, and software against medical users' demand for easy, accessible data and tools.

Windows 10 advancements in security and identity protection features are easy to deploy and manage without compromising the user experience. Safeguard patient data—both protected health information (PHI) and personally identifiable information (PII) are always encrypted when transmitted or at rest. Windows 10 devices have access controls with biometrics and multifactor authentication, enabling only authorized staff to access patient data. Devices and controls can be designed to isolate key processes and protect operating systems and devices from running unwanted apps.

Advancing healthcare requires innovation, collaboration and trust. In the United States alone, more than 25,000 health organizations use the Microsoft Cloud. Microsoft is the only cloud service provider that can offer a complete hybrid cloud approach, providing health organizations system flexibility that is security-enhanced, transparent, and compliant even as regulations and standards evolve.

Security in manufacturing

The complexity of manufacturing, the vast range of product types, and the challenges of omni-channel supply chain management make a comprehensive security plan a crucial part of the business. Manufacturers face the real-world challenges of theft, pilferage, product control, compliance, confined space monitoring and permitting, access control, HSE standards, and the like every day. From receiving basic materials, to safeguarding the manufacturing process, to protecting the transportation and delivery of final products and empowering a mobile workforce, manufacturers are benefiting from Windows 10 advancements in security and identity protection.

Accessing controls with biometrics and multifactor authentication and the availability of innovative embedded line-of-business (LOB) devices that integrate with what they already have on a single platform provide a competitive advantage. Widows 10 offers new ways to protect critical business information from leaks and thefts, and the ability to separate corporate and personal files on BYOD devices leading to more secure business practices across their enterprise.

"[The topic of network security] is becoming increasingly relevant in industrial plants. Factor in emerging trends in the business [such as bring-your-own-device (BYOD) and the Internet of Things (IoT)] and the touch points for potential security threats are increasing at exponential rates."

– **Aberdeen Research**, "Ensuring the Security of Industrial Networks in an Insecure World"

Security for retail

Target. Adobe. AOL. eBay. What do they have in common? They are all large enterprises that have been the victims of large security breaches during the last year. In the case of online auction site eBay, more than 145 million records were compromised, while Target dealt with upward of 70 million breaches. While the rise of e-commerce and cloud data storage have proven to be a boon for consumers, a host of compliance and security challenges have emerged.[1]

Because retailers process massive amounts of financial data, often from multiple stores across multiple states, there are hundreds of potential access points for an attacker. Most retail attackers are opportunistic outsiders. Their challenges come from end users accessing malware-laden sites or downloading infected files, weak passwords, insecure system configurations, legacy or unpatched technology, or poor network security.

Retailers are on the most-wanted list for hackers and protecting their bottom line begins with strengthening the weak links. It requires a comprehensive, holistic, end-to-end security model that encompasses their entire omni-channel infrastructure from POS terminals, e-commerce websites, third-party vendor links, to employee access points and IoT-based devices such as printers and security cameras. From collecting and analyzing available data for patterns, to reporting odd network behaviors in real time, these all contribute to assessing the scope of threats and designing in-depth solutions that minimize risk.

Security in the energy sector

The rise of sensors, big data, and machine learning is not news to the energy sector. Oil and gas industries have long relied on complex sensors in remote, inhospitable conditions, constantly spinning off huge amounts of data. As other industries race to transform their businesses to be digital-first, oil and gas has a head start.

From data to facilities, security is top of mind across the industry. Geopolitical pressures have introduced threats both cyber and physical that can severely disrupt operations, potentially endangering people and property. The distributed and hazardous nature of industry facilities and systems creates unique vulnerabilities, making them targets for cyber and terrorist attacks. Technological advances in big data analytics, video surveillance and cloud computing are driving innovative security measures and better peace of mind.

Microsoft has decades-long experience building enterprise software, running some of the largest online services in the world. We build on this experience to implement and continuously improve security-aware software development, operational management, and threat mitigation practices that are essential to the strong protection of services and data.

"'We can not say it loud and often enough, ransomware has become the black plague of the internet, spread by highly sophisticated exploit kits and countless spam campaigns,' Talos says. Attackers are going after bigger targets that can afford to pay more, with potentially catastrophic consequences."

– **Steve Dent**, Engadget, March 17, 2016

Looking to the future

As IoT continues to evolve, it becomes increasingly important to build devices on an IoT platform that correctly balances security needs, the user experience, and the resource constraints of diverse devices. Microsoft brings enterprise-grade security to protect user and device identities, data, and connections. Windows 10 empowers organizations to build their Internet of Things today with advanced security technologies on a platform that is always innovating to meet tomorrow's demands.

Microsoft has a rich ecosystem of partners that are ready to help enable digital transformation and harness the power of IoT today. We're working with leading device manufacturers to deliver secure, next-generation devices that help enterprises build connected businesses—and realize the benefits of IoT.

Get ready to transform your business with Microsoft technology

Get started today. Work with Microsoft or one of our global partners to see how you can transform and help secure your business by harnessing IoT, big data, collaboration, and mobile solutions.

- Find a Microsoft partner: *https://partnercenter.microsoft.com/en-us/pcv/search*
- More information on how Microsoft is empowering businesses to harness IoT across their enterprise visit: *www.InnovateOnWindows10IoT.com*
- Learn more about the advanced security built into the Windows 10 Stack: https://blogs.windows.com/business/2016/06/29/advancing-security-for-consumers-and-enterprises-at-every-layer-of-the-windows-10-stack/#msWM7YeDAAdpcQwI.97
- Read Forrester study that shows how Windows 10 can reduce security, IT, and productivity costs: https://blogs.windows.com/business/2016/07/12/forrester-study-finds-windows-10-can-reduce-security-it-and-productivity-costs/#C0dx0i6ROvSV6dR9.97
- Learn more about what Microsoft is doing to ensure security is built right into all of their technology: https://www.microsoft.com/en-us/TrustCenter/Security/default.aspx

Microsoft

[1] Security Intelligence https://securityintelligence.com/cyber-security-challenges-how-do-retailers-protect-the-bottom-line