



# Sogeti Smart Workspace Secure Workspace

Endpoint protection against modern threats  
with Windows® 10 and 7th Gen Intel® Core™  
vPro™ processors

2019

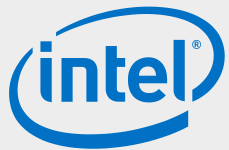


30 Seconds



# It Takes Both Microsoft and Intel to Safeguard Your Business

*Combine Windows® 10 with 7th Gen Intel® Core™ vPro™ processor technology for enhanced protection for systems, identity and data, and to help prevent and combat threats.*



- Intel® Authenticate Solution
- Intel® AES-NI, Intel® Trusted Platform Management (Intel® TPM) 2.0
- Intel® Secure Key
- Intel® VT-x/VT-d
- Intel® Boot Guard, Intel® BIOS Guard, Intel® OS Guard



- Windows Hello\* For Business
- Windows\* Credential Guard
- Microsoft BitLocker\*
- Windows\* Information Protection
- Windows\* Defender Application Guard for Microsoft Edge\*



## Secure Platform Foundation for Better Data and Identity Protection



**Identity and Device Protection:** Hardware-based, multifactor authentication. Secure user credentials, including biometric data and cryptographic keys, using hardware-based protection.



**Information Protection:** Hardware-based, multilevel data encryption. Accelerate encryption, protect keys, and separate personal and work info, allowing IT to manage enterprise content, usage, and access.



**Threat Protection:** Zero-Day exploit prevention and protection for Windows\* System Core and browser exploits.



**Fast Recovery:** Remote recovery and remediation in the scenario of compromise without incurring the cost for a desk-side visit.

*\*Other names and brands may be claimed as the property of others.*

3 Minutes



# Where Are the Vulnerabilities?

*Traditional firewalls are not enough to safeguard your infrastructure, network, and devices from ever-more-sophisticated threats, nor can rotating passwords sufficiently protect identities.*

**To secure business operations today, endpoint protection is critical.**



Identity protection



Data protection



Threat detection and prevention



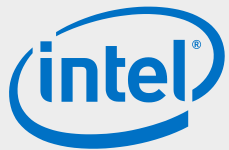
Device protection



Breach detection, investigation, and response

# It Takes Both Microsoft and Intel to Safeguard Your Business

*Combine Windows® 10 with 7th Gen Intel® Core™ vPro™ processor technology for enhanced protection for systems, identity and data, and to help prevent and combat threats.*



- Intel® Authenticate Solution
- Intel® AES-NI, Intel® Trusted Platform Management (Intel® TPM) 2.0
- Intel® Secure Key
- Intel® VT-x/VT-d
- Intel® Boot Guard, Intel® BIOS Guard, Intel® OS Guard



- Windows Hello\* For Business
- Windows\* Credential Guard
- Microsoft BitLocker\*
- Windows\* Information Protection
- Windows\* Defender Application Guard for Microsoft Edge\*



## Secure Platform Foundation for Better Data and Identity Protection



**Identity and Device Protection:** Hardware-based, multifactor authentication. Secure user credentials, including biometric data and cryptographic keys, using hardware-based protection.



**Information Protection:** Hardware-based, multilevel data encryption. Accelerate encryption, protect keys, and separate personal and work info, allowing IT to manage enterprise content, usage, and access.



**Threat Protection:** Zero-Day exploit prevention and protection for Windows\* System Core and browser exploits.



**Fast Recovery:** Remote recovery and remediation in the scenario of compromise without incurring the cost for a desk-side visit.

*\*Other names and brands may be claimed as the property of others.*

# Sogeti SECURE WorkSpace

## Get the essential, need-to-know information to protect your organization.

Join us for a comprehensive security workshop focused on your requirements, workforce configuration and device mix, and strategic goals.

Discover how to implement the new security features, and create a high-level capability implementation timeline to strengthen your endpoint security with Windows® 10.

- Assess end-to-end vulnerabilities, including endpoints
- Identify attack surfaces
- Develop a security roadmap
- Address existing and new technology requirements
- Plan deployment of increased security

## Contact

**Darren Baker,**  
Global Business  
Development Director, at  
[darren.baker@sogeti.com](mailto:darren.baker@sogeti.com),  
or visit [sogeti.com](http://sogeti.com).



30 Minutes





# Agenda

- 01 Security Landscape
- 02 Why Sogeti
- 03 Security Technologies: Windows 10
- 04 Security Technologies: Intel 7<sup>th</sup> Gen
- 05 How Sogeti Can Help: Secure WorkSpace
- 06 Q&A



# In the News

*High-profile breaches in the marketplace are examples of front-door attacks that resulted in high-visibility data loss.*



**InfoWorld**  
FROM IDG

**TECH'S BOTTOM LINE**  
By Bill Snyder | Follow

**Hacking is a business -- and business is good**

*Yahoo Says 1 Billion User Accounts Were Hacked*  
By VINU GOKL and NICOLE PERLAOTH | DEC 14, 2016



**Europol Estimates That WannaCry Cyber Attack Has Hit About 2,00,000 Systems In 150 Countries - Tech2**  
15 May 2017 | 10:29

**Sony's New Movies Leak Online Following Hack Attack**



**POLITICS** | Tue Sep 27, 2016 | 10:28pm EDT

**FBI probes hacks targeting phones of Democratic Party officials: sources**



**USA TODAY** Search

NEWS SPORTS LIFE MONEY **TECH** TRAVEL OPINION 47° CROSSWORDS WASHINGTON VIDEO STOCKS APPS MORE

**Ransomware attack hit San Francisco train system**



**2017- The Year to Take Cyber Security Seriously**  
BY: DARREN BAKER | JANUARY 10, 2017

f 7 G+ 18 in 19 e 1

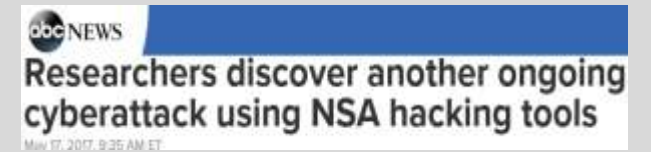
News room > News releases >

**IBM & Ponemon Institute Study: Data Breach Costs Rising, Now \$4 million per Incident**

**Cisco job applicants warned of potential mobile site data leak**

Cisco has emailed users of its mobile careers site, warning of two occasions when their data could have been exposed.

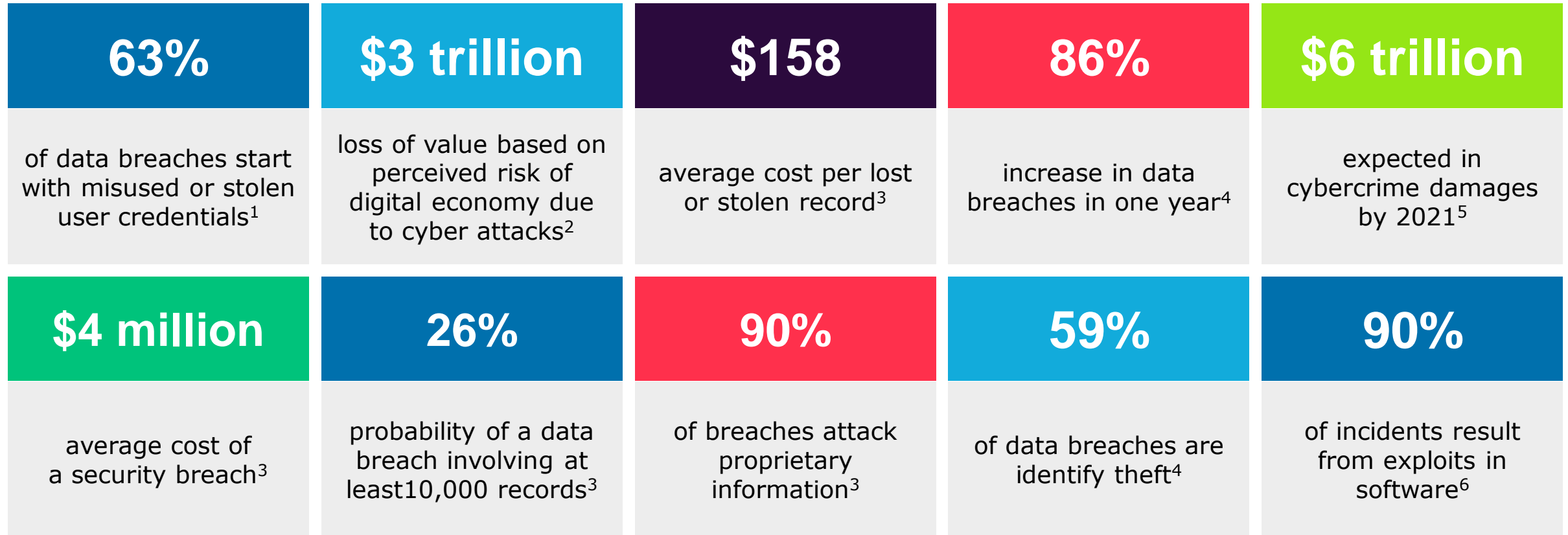
By Chris Guiken | November 4, 2016 -- 11:34 GMT (11:34 PDT) | Topic: Security



**abc NEWS**

**Researchers discover another ongoing cyberattack using NSA hacking tools**  
May 17, 2017, 9:35 AM ET

# The Business Security Landscape



1. Data Breach Investigations Report, Verizon (2016), <http://www.verizonenterprise.com/DBIR/2015/>
2. The rising strategic risks of cyberattacks, McKinsey Quarterly, May 2014., <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-rising-strategic-risks-of-cyberattacks>
3. Cost of Data Breach Study: Global Analysis, Ponemon Institute (2016), <http://www-03.ibm.com/security/infographics/data-breach/>
4. <http://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-2016-Breach-Level-Index.aspx>
5. Cybersecurity Ventures 2016, <http://cybersecurityventures.com/cybersecurity-market-report/>
6. US Department of Homeland Security, <http://www.csoonline.com/article/2978858/application-security/is-poor-software-development-the-biggest-cyber-threat.html>

# Endpoint Security

*"Security is not just a concern of the network administrator and the perimeter of your network. Increased security on users' workstations is instrumental to reduce attack vectors and the financial and reputational risk to an organization. This is of huge importance for organizations in 2017. The security features built into Windows® 10—plus the new technology built into 7th Gen Intel® Core™ hardware—significantly enhance device security."*



**Frédéric Beaufils,**

Head of Corporate Functions: Offerings, Alliances, Innovation, and Sales, Sogeti

# Where Are the Vulnerabilities?

*Traditional firewalls are not enough to safeguard your infrastructure, network, and devices from ever-more-sophisticated threats, nor can rotating passwords sufficiently protect identities.*

**To secure business operations today, endpoint protection is critical.**



Identity  
protection



Data  
protection



Threat detection and prevention



Device  
protection



Breach detection,  
investigation, and response

# How Do Endpoint Attacks Happen?

## Access to one device can lead to access to many.

- Direct hacking against external-facing servers
- Insider knowledge and privileges
- Zero-day exploits
- Vulnerabilities
- Weak defenses
- Social engineering
- Spear-phishing (e.g., crafted emails, "Microsoft support" phone calls, USB key in the parking lot)
- "Watering hole" (e.g., exploited websites)

*Stat sources (from MS Windows 10 Security Story PPT):*

- 1. Ponemon Institute, "The Post Breach Boom," 2013*
- 2. Ponemon Institute, 2014 Global Report on Cost of Cyber Crime*
- 3. Mandiant 2014 Threat Report*

# 23%

of recipients opened phishing messages (11% clicked on attachments)

# 99.9%

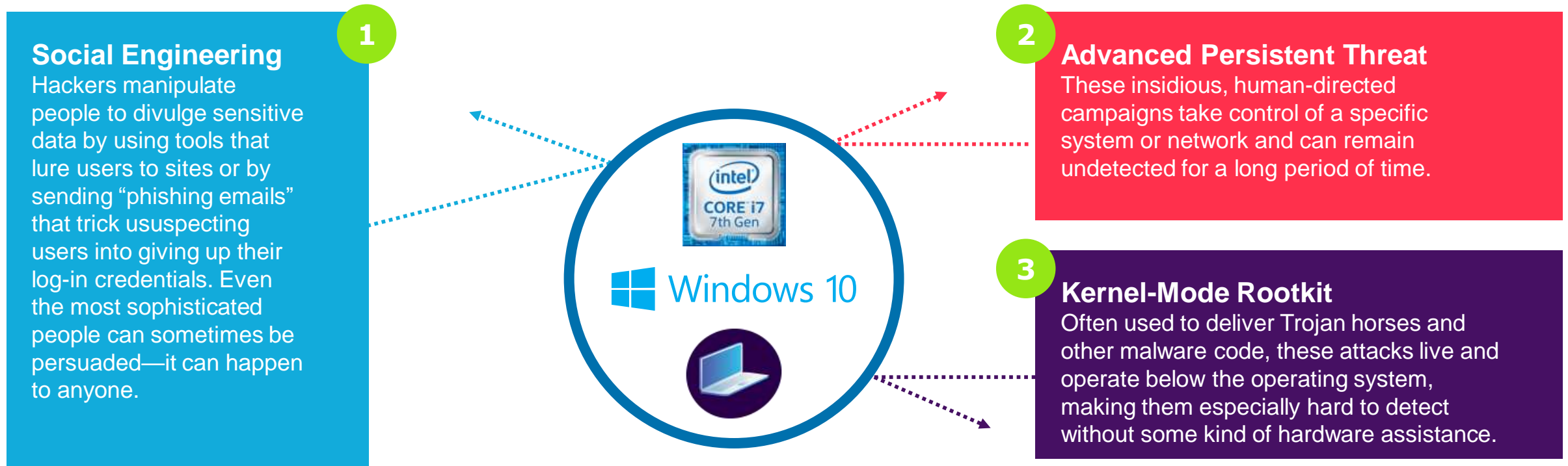
of exploited vulnerabilities were used more than a year after the CVE was published



# What You Are up Against

## Three tools of the modern hacker

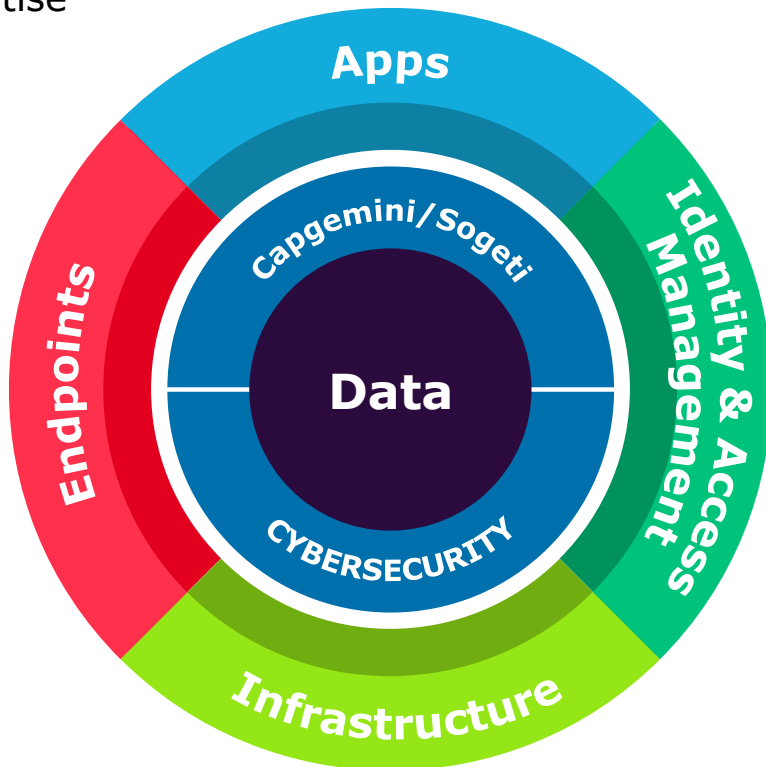
Here are three of the most common and dangerous ways that hackers can attack your desktops, infect them with malware, and harm your business



# Why Sogeti

## Sogeti brings a deep knowledge base on security and device deployment

- **More than 3000** people with cybersecurity skills & certifications
- **End-to-end intelligent cybersecurity** services portfolio
- World wide **digital transformation** device deployment expertise



Security experts hold more than **30 different** industry recognized certifications



More than **20** Microsoft deployment **awards** since 2008

### 4 Families of Cybersecurity Services

Consulting & Assessment  
Protection  
Monitoring  
Threat Hunting



**Microsoft Partner of the Year**  
**2015 Winner**  
Devices and Deployment



Advanced Data Analysis  
Security Operations Center.  
France, UK, Luxembourg,  
India, Spain, Belgium

### Devices and Deployment



More than **10 million** **Windows devices** deployed since 2008



# It Takes Both Microsoft and Intel to Safeguard Your Business

*Combine Windows® 10 with 7th Gen Intel® Core™ vPro™ processor technology for enhanced protection for systems, identity and data, and to help prevent and combat threats.*



- Intel® Authenticate Solution
- Intel® AES-NI, Intel® Trusted Platform Management (Intel® TPM) 2.0
- Intel® Secure Key
- Intel® VT-x/VT-d
- Intel® Boot Guard, Intel® BIOS Guard, Intel® OS Guard



- Windows Hello\* For Business
- Windows\* Credential Guard
- Microsoft BitLocker\*
- Windows\* Information Protection
- Windows\* Defender Application Guard for Microsoft Edge\*



## Secure Platform Foundation for Better Data and Identity Protection



**Identity and Device Protection:** Hardware-based, multifactor authentication. Secure user credentials, including biometric data and cryptographic keys, using hardware-based protection.



**Information Protection:** Hardware-based, multilevel data encryption. Accelerate encryption, protect keys, and separate personal and work info, allowing IT to manage enterprise content, usage, and access.



**Threat Protection:** Zero-Day exploit prevention and protection for Windows\* System Core and browser exploits.



**Fast Recovery:** Remote recovery and remediation in the scenario of compromise without incurring the cost for a desk-side visit.

*\*Other names and brands may be claimed as the property of others.*

# Better Together Security Benefits

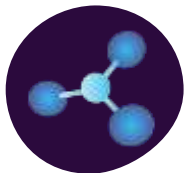
## Strengthen security protections in silicon



Hardened Security: **Combining hardware and software solutions is critical** for stronger, proactive security.



**Mitigate risk, help reduce maintenance costs, and streamline productivity** with the latest Intel® Core™ vPro™ processor-based devices.



**Cryptographic operations, sensitive information channels, and a trusted execution environment** help keep your business productive and profitable.<sup>1</sup>

1. The 2015 Data Breach Investigations Report (DBIR) by Verizon, <http://www.verizonenterprise.com/DBIR/2015/>



# Better Together Security Benefits

## Biometrics innovation



With misused or stolen credentials causing more than half of today's data breaches, **biometrics-based identity protection** raises the bar.<sup>1</sup>



**Support more secure and intuitive login choices**, with Windows Hello\* facial recognition or fingerprint sensors for Intel® Authenticate with the latest Intel® Core™ vPro™ processors.



New Intel®-based PCs and Windows® 10 Pro **decrease vulnerabilities and help reduce password-reset costs.**

1. Verizon Data Breach Investigations Report, Verizon, 2016.



# Better Security is Better Business

## Benefits after implementing Windows® 10



Increasing security and reducing desktop security issue remediation time by one-third.<sup>1</sup>



Improved productivity and mobility.<sup>1</sup>



*1. Forrester Research, Total Economic Impact (TEI) Study, 2016, commissioned by Microsoft.*



# Windows 10

## Business Benefits



### Protect Identities

- Easy to use and deploy multifactor solution with antitheft and phishing detection
- The convenience of a password, and the security of multifactor solutions



### Protect Data

- Market-leading, highly manageable disk encryption
- Fully integrated data loss prevention and data separation



### Protect Applications

- Secure, trusted applications protect data and your network



### Resist Threats

- Mobile lockdown for desktop machines
- Trusted app model for devices



### Secure Devices

- Integrated platform and hardware security
- Protection from power on to power off
- Helps eliminate opportunities to tamper with and hide from systems

# Windows 10 Security Stack

Protect, Detect & Respond



## DEVICE PROTECTION



- Device integrity
- Device control

## THREAT RESISTANCE



- SmartScreen
- Windows Firewall
- Microsoft Edge
- Device Guard
- Windows Defender

## IDENTITY PROTECTION



- Windows Hello
- Credential Guard

## INFORMATION PROTECTION



- BitLocker and BitLocker to Go
- Windows Information Protection

## BREACH DETECTION INVESTIGATION & RESPONSE



- Conditional Access
- Windows Defender ATP

# Windows® 10 Security Technologies

## Windows Device/Credential Guard

Fight zero-day exploits and malware. Device Guard relies on Intel® Virtualization Technology and acts like a bouncer to block zero-day attacks by vetting applications that try to access a Windows 10 machine or its network.

## Windows Hello

Biometric technology that uses the face, iris, or fingerprint as password alternatives to launching Windows. Includes Windows Passport, which utilizes two-factor authentication and grants password-free access to applications, websites, and networks on specific enrolled devices. (This is only possible on devices that have biometric sensors, such as those based on 6th Gen and 7th Gen Intel® Core™ vPro™ processors.)

## Windows BitLocker with Azure Rights Management

Helps protect data through automatic encryption of corporate apps, data, emails, and website content as it arrives on devices from corporate locations or when new content is created. This feature also helps prevent copying corporate data and other sensitive information. Companies have the option to designate all new content created on devices as corporate by policy.



**Windows 10 is Microsoft's most secure operating system.**



# Windows® 10 Security Technologies

## Windows Patch Management

Windows 10 provides patch management automatically and continuously to fix code and security holes.

## Windows Trusted Apps/ Application Guard

Requires apps distributed through its store to be signed by Microsoft or a trusted vendor. An app is also partitioned in its own virtual space. If something happens, this only affects that particular app and not the whole system, making Windows 10 devices more secure.

## Windows Secure Boot

Enhances security in the pre-boot environment and allows only apps that are signed and trusted by administrators. This helps thwart efforts by some of the most dangerous hackers who attack computers by injecting low-level malware like rootkits during the PC boot process.



**Windows 10 is Microsoft's most secure operating system.**





# Windows® 10 Security Technologies

## Windows Edge Browser

Designed to prevent sophisticated and prevalent attacks. The Edge provides more security by not supporting extensions that offer hackers entry through a web browser. Helps prevent a compromised browser from giving admin-level access to the whole system.

## Windows Virtual Secure Mode (VSM)

Uses a PC's CPU virtualization to protect key aspects, including data and credentials on the system's hard drive. The VSM prevents the hacker from obtaining credentials and infiltrating the enterprise infrastructure. For virtualization to be enabled, the CPU has to have hardware virtualization capability, such as that in 6th and 7th Gen Intel Core vPro processors.

## Windows Micro-Virtualization

Automatically isolates each user's unverified tasks at the device level. This helps prevent breaches that involve browser attacks, USB thumb drives, and email attachments.



**Windows 10 is Microsoft's most secure operating system.**



# Windows® 10 Security Enhanced with Intel® Modern Devices

## DEVICE PROTECTION



Trusted Platform Module

Windows Update

Windows Trusted Boot

UEFI Secure Boot

Virtualization Based Security

## THREAT RESISTANCE



SmartScreen

Windows Firewall

Windows Defender

Microsoft Edge

Microsoft Edge Barcelona

Device Guard

## IDENTITY PROTECTION



Windows Hello

Windows Hello Companion Devices

Credential Guard

## INFORMATION PROTECTION



BitLocker to Go

BitLocker

BitLocker Admin and Monitoring

Windows Information Protection

Device Encryption

## BREACH DETECTION INVESTIGATION & RESPONSE



Windows Defender Advanced Threat Protection

Conditional Access

Security Management2

# 7th Gen Intel® Core™ vPro™ Processors

**Fight against identity and data breaches. Reduce exposure to software-level attacks, where the majority of threats happen today.**



Built-in Intel® vPro™ technology: Provide hardware-enhanced security, remote manageability, and productivity-enhancing capabilities.



Built-in Intel® Authenticate: Help solve identity breaches in the most aggressive way possible for enterprises.



*Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at [intel.com](https://www.intel.com).*



# Key Intel® Technologies That Increase Security<sup>1</sup> on Windows® 10 Devices

## Available now in 7th Gen Intel® Core™ vPro™ processors

Intel® VT-x, VT-d	<ul style="list-style-type: none"><li>Intel® Virtualization Technology for CPU and directed I/O. Intel VT-d provides platform infrastructure for I/O virtualization.</li></ul>
Intel® Trusted Execution Technology (Intel® TXT)	<ul style="list-style-type: none"><li>CPU instruction set that hardens platforms against software-based attacks by allowing greater control of launch stack.</li></ul>
Intel® Secure Key	<ul style="list-style-type: none"><li>Provides fast, true random number generation done in the hardware, with minimal user impact.</li></ul>
Intel® Remote Secure Erase	<ul style="list-style-type: none"><li>Intel® SSD Pro Series feature enables IT to remotely and securely erase Intel® SSD Pro Series for repurposing or EOL.</li></ul>
Intel® Platform Trust Technology (Intel® PTT)	<ul style="list-style-type: none"><li>A secure execution environment for firmware components.</li></ul>
Intel® Authenticate	<ul style="list-style-type: none"><li>A hardware-enhanced multifactor authentication solution that strengthens identity protection for the enterprise. It assesses multiple hardware-enhanced factors at the same time to validate a user's identity. IT policies, credentials, authentication factors and decisions are all protected in hardware.</li></ul>

*Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.*

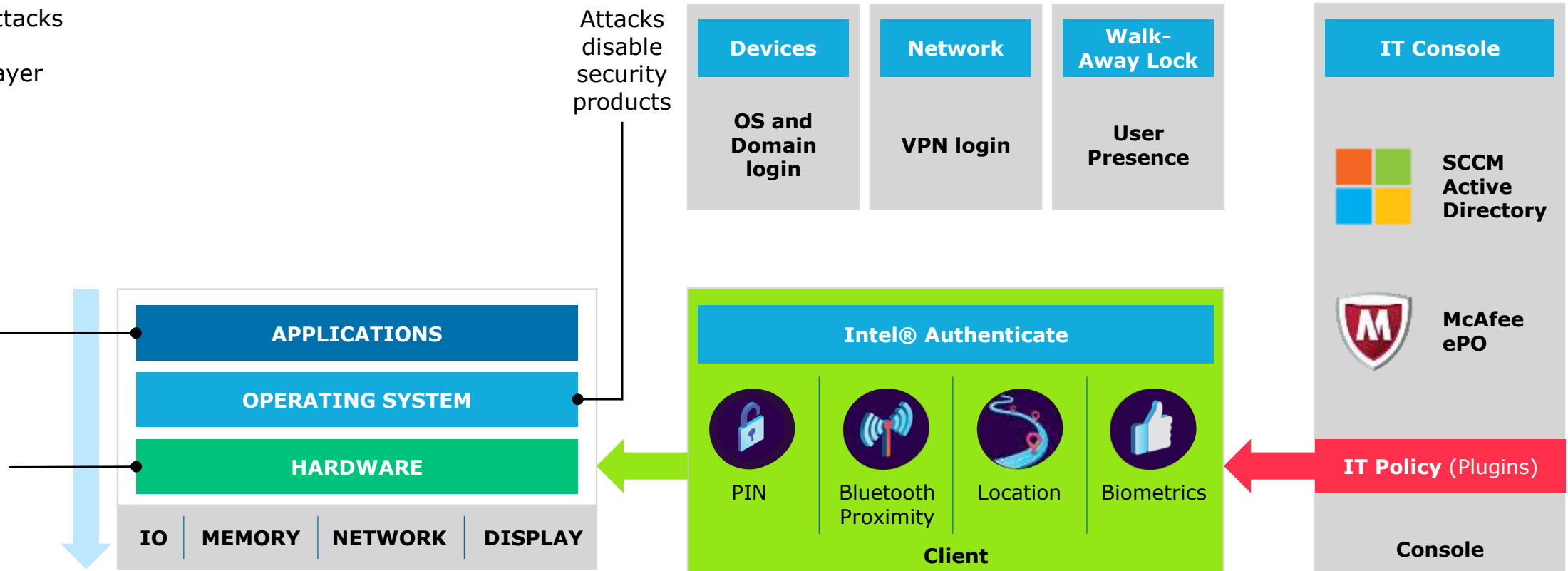
# Intel® Authenticate

Intel® Authenticate protects factors, credentials, policies, and decisions in hardware.

Traditional attacks focus on the application layer

More than 63% of network breaches involve user credentials at the OS<sup>1</sup>

Attacks disable security products



1. Data Breach Investigations Report, Verizon (2016), <http://www.verizonenterprise.com/DBIR/2015/>

# Key Intel® Technologies That Increase Security<sup>1</sup> on Windows® 10 Devices

## Available now in 7th Gen Intel® Core™ vPro™ processors

### Intel® Active Management Technology (Intel® AMT)

- Hardware and firmware technology for remote out-of-band management of devices, in order to monitor, maintain, update, upgrade, and repair them.

### Intel® OS Guard

- Intel OS Guard helps protect the OS from malware by blocking application access to critical OS vectors.

### Intel® BIOS Guard

- Hardware-assisted authentication and protection against BIOS recovery attacks.

### Intel® Boot Guard

- Intel® architecture-based root of trust; provides measurement and verification standard to OEM software; supplies hardware-based boot integrity to OS secure boot process.

### Intel® IPT-PKI

- Provides a hardware-based, tamper-resistant embedded Public Key Infrastructure (Intel® PKI) capability.

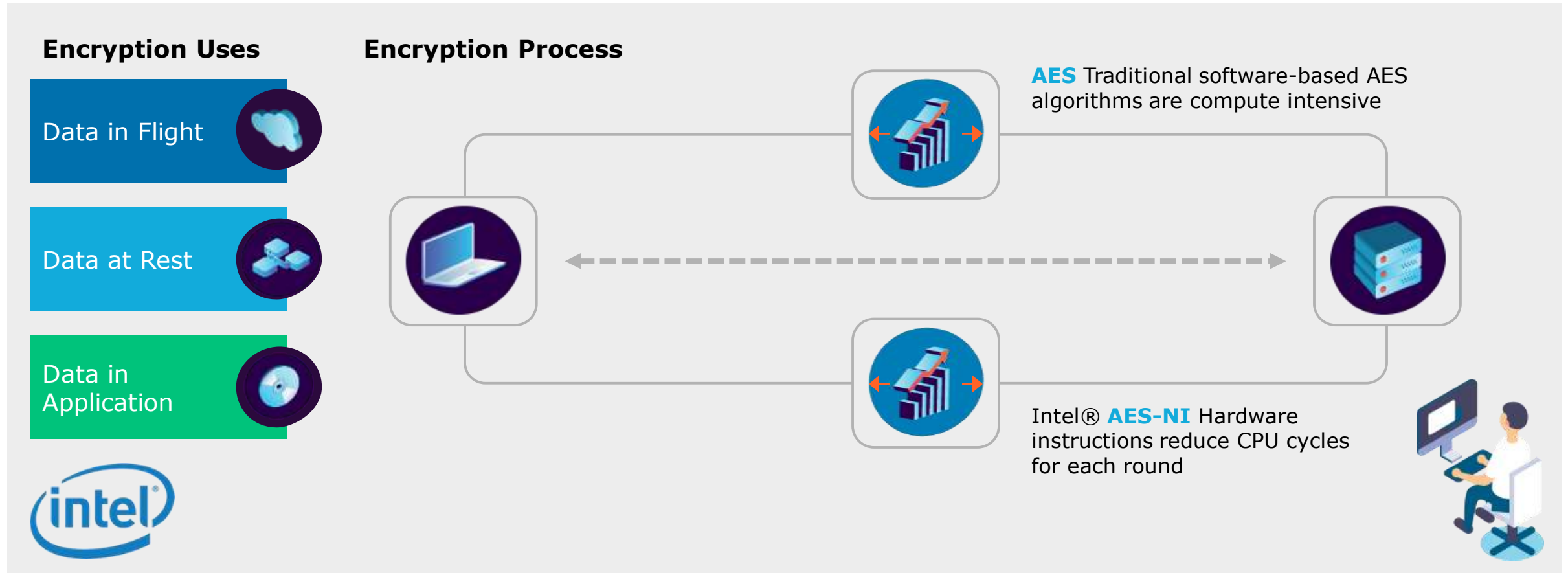
### Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

- Instruction set to help improve the speed of applications performing encryption and decryption.

*Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.*

# Intel® Security Technologies

## Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)



Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

# Key Intel® Technologies That Increase Security<sup>1</sup> on Windows® 10 Devices

## Available now in 7th Gen Intel® Core™ vPro™ processors

### Intel® Memory Protection Extensions (Intel® MPX)

- Protection against buffer overflow attacks. With compiler, runtime library, and OS support, Intel MPX brings increased security to software by checking pointer references whose normal compile-time intentions are maliciously exploited at runtime due to buffer overflows.

### KVM remote control

- Intel AMT features that provides full remote access to your device no matter what state it's in. Allows companies to manage their PCs even when out of band, regardless of the PC power state and even if the OS has failed or there is no hard drive present.

### Intel® Manageability Commander with Microsoft SCCM integration

- Integrates with Microsoft SCCM to deliver Intel AMT out-of-band features from the Microsoft SCCM console.

### Intel® Stable Image Platform Program (Intel® SIPP)

- Aligns and stabilizes key Intel platform components, enabling a predictable transition from one platform generation to the next.

### Intel® Software Guard Extension (Intel® SGX)

- CPU instructions and platform enhancements that enable applications to create private areas to protect sensitive information at runtime and at rest.

*Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.*



# Intel® Security Technologies

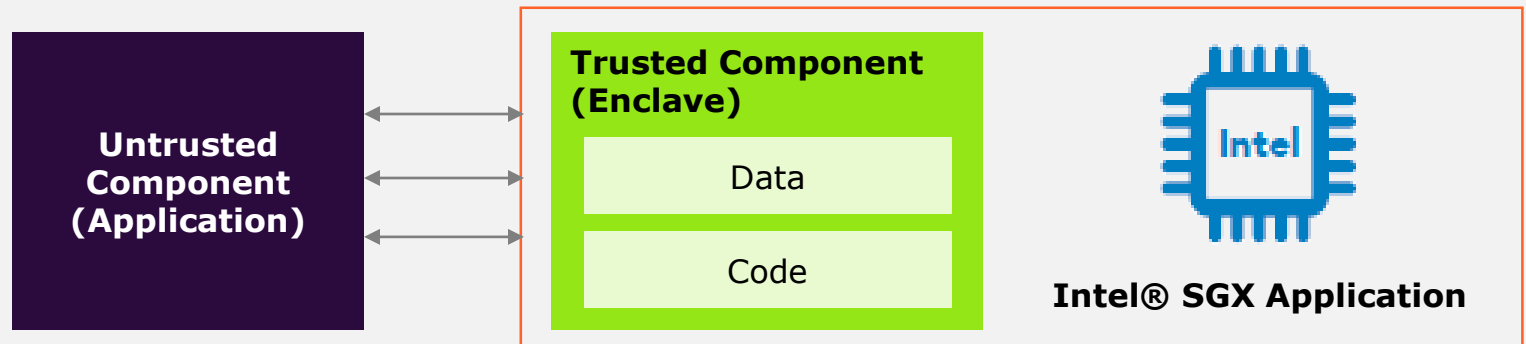
## Intel® Active Management Technology (Intel® AMT)

Manage and repair PC assets, workstations, and entry servers, utilizing the same infrastructure and tools across platforms for management consistency. Intel AMT is a feature of 6th and 7th Gen Intel Core vPro processors and workstation platforms based on select Intel® Xeon® processors.

## Intel® Software Guard Extensions (Intel® SGX)

Helps application developers protect selected code and data from disclosure or modification.

**Trusted Execution Environment Provide a Safe Zone**



*Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at [intel.com](https://www.intel.com).*



# Securing Your Critical Business Assets and Operations Starts with the Endpoints



Investing in Windows 10 with systems featuring 6th and 7th Gen Intel Core vPro processors increases security to protect your valuable systems, data, and, ultimately, your business.

 Windows 10



# Now is the Time to Secure Your Business



Modern security threats are sophisticated, malicious, and persistent.



Many threats are targeted to the most vulnerable part of your infrastructure: end-point devices.



When combined, Windows 10 and 7th Gen Intel Core vPro processors offer a powerful combination of security features for vulnerable endpoints.



Sogeti has the Digital Transformation expertise to modernize and secure your critical data, applications, infrastructure, and devices.

# Sogeti SECURE WorkSpace

**Get the essential, need-to-know information to protect your organization.**

Join us for a comprehensive security workshop focused on your requirements, workforce configuration and device mix, and strategic goals.

Discover how to implement the new security features, and create a high-level capability implementation timeline to strengthen your endpoint security with Windows® 10.

- Assess end-to-end vulnerabilities, including endpoints
- Identify attack surfaces
- Develop a security roadmap
- Address existing and new technology requirements
- Plan deployment of increased security





**Darren Baker**

*Global Business  
Development Director, at  
darren.baker@sogeti.com,  
or visit sogeti.com.*

**Contact**



# Learn More

 Sogeti.com 

 Microsoft Cybersecurity 

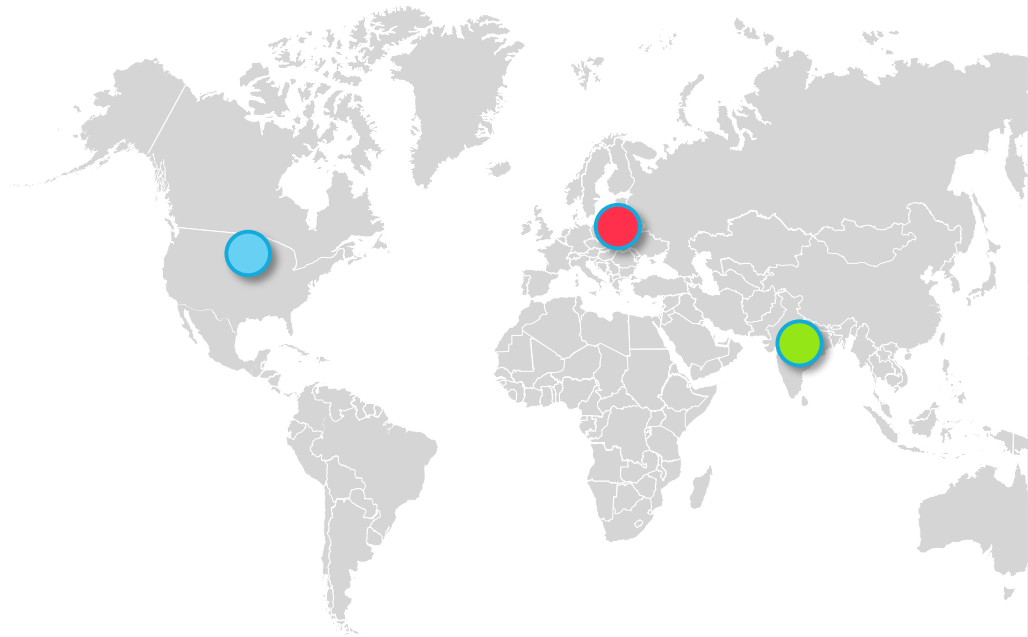
 Intel Data Protection Technology 

# About Sogeti

[www.sogeti.com](http://www.sogeti.com)

**Sogeti is a leading provider of technology and engineering services.**

**250,000+ employees spread over 100 locations in 15 countries.**

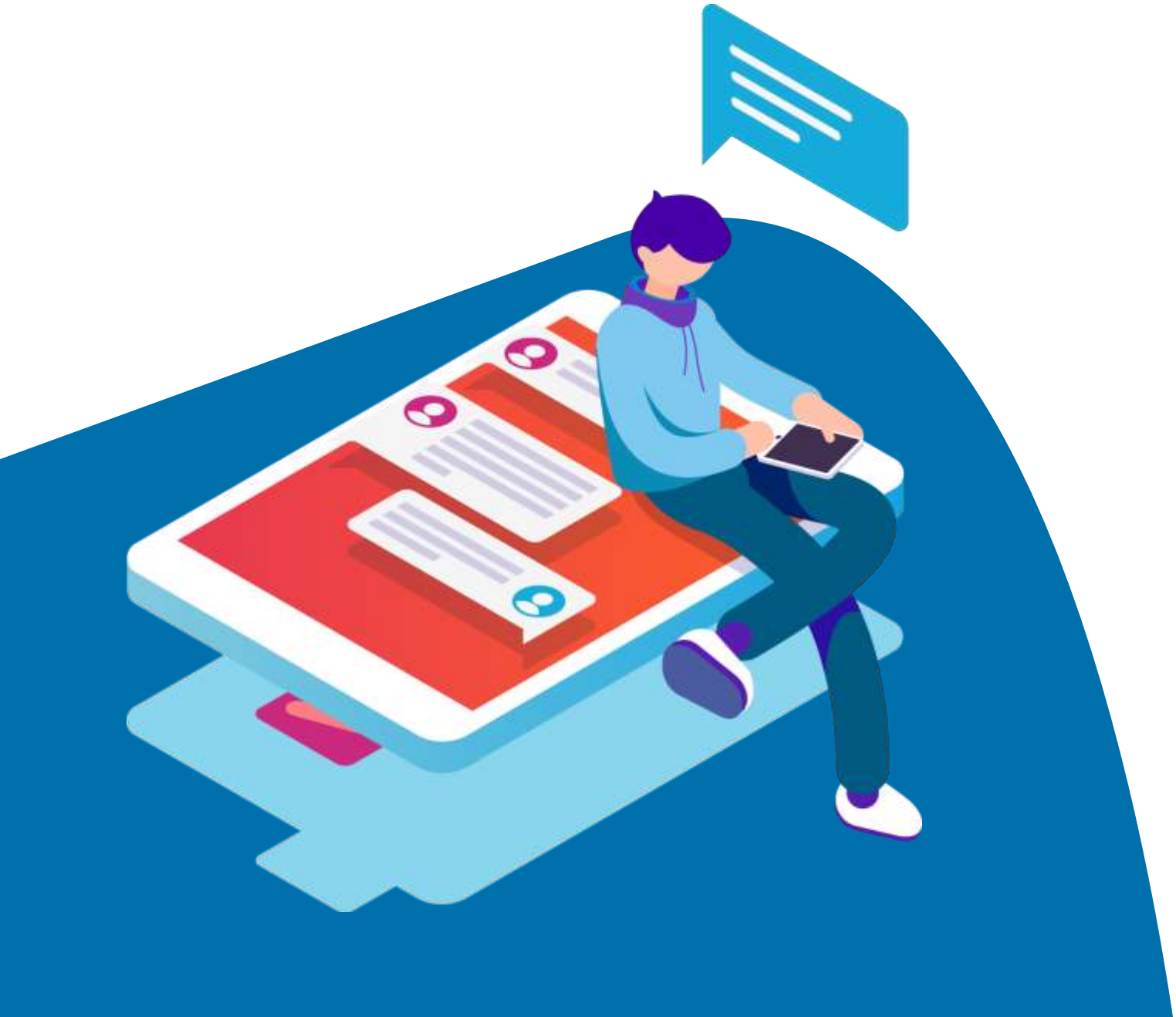


<b>USA</b> Chicago, Cincinnati, Houston, New York, Seattle, Washington... (22)	<b>2,000</b>
<b>Europe</b>	<b>≈17,000</b>
<b>France</b> Paris, Toulouse, Lyon, Marseille... (18)	10,000
<b>Benelux</b> Brussels, Antwerpen, Vianen... (8)	3,500
<b>Spain</b> Madrid, Barcelona	550
<b>Scandinavia</b> Stockholm, Oslo, Copenhagen... (29)	1,500
<b>UK &amp; Ireland</b> London, Dublin, Galway	450
<b>Germany</b> Düsseldorf, Hamburg, Frankfurt... (6)	500
<b>Switzerland</b> Geneva, Basel, Zurich, Lausanne	120

- Cloud
- Cybersecurity
- Digital manufacturing
- Quality assurance and testing
- Emerging technologies



**Sogeti is a wholly owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.**



Q&A

Backup





# Attacks Are on the Rise

**Reducing attack surfaces is more effective than chasing known threats and detecting millions of unknown threats.**



Smart, connected devices; networks accessible to global mobile workers and partners; and the often unmanaged mix of personal and business devices at work outpace the security needed to protect them for many businesses.



# Information, Identities, and IP – End-points Need Protection

## Protect Devices and Data



### Protect

systems and data when devices are lost or stolen.



### Prevent

unauthorized users and apps from accessing and leaking data.



### Protect

data when shared with others, or shared outside of organizational devices and control.

“Security needs to be built from the endpoint outwards.”<sup>1</sup>  
TechPro Research, 2017



1. <http://www.techrepublic.com/article/experts-predict-2017s-biggest-cybersecurity-threats/>

# Will 2017 Be the Year of Ransomware?

“Ransomware attacks have become a billion-dollar business for cybercriminals.”<sup>1</sup>

“30% of NHS trusts have suffered a [ransomware] attack, potentially placing patient data and lives at risk.”<sup>2</sup>

“Extortionists swindled some \$27 million in just 6 months from people whose data they took hostage.”<sup>3</sup>

(2014 FBI estimate for a single ransomware strain)

1. <https://www.wired.com/2017/01/biggest-security-threats-coming-2017>

2. <http://betanews.com/2017/01/17/uk-health-ransomware/>

3. <https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets>



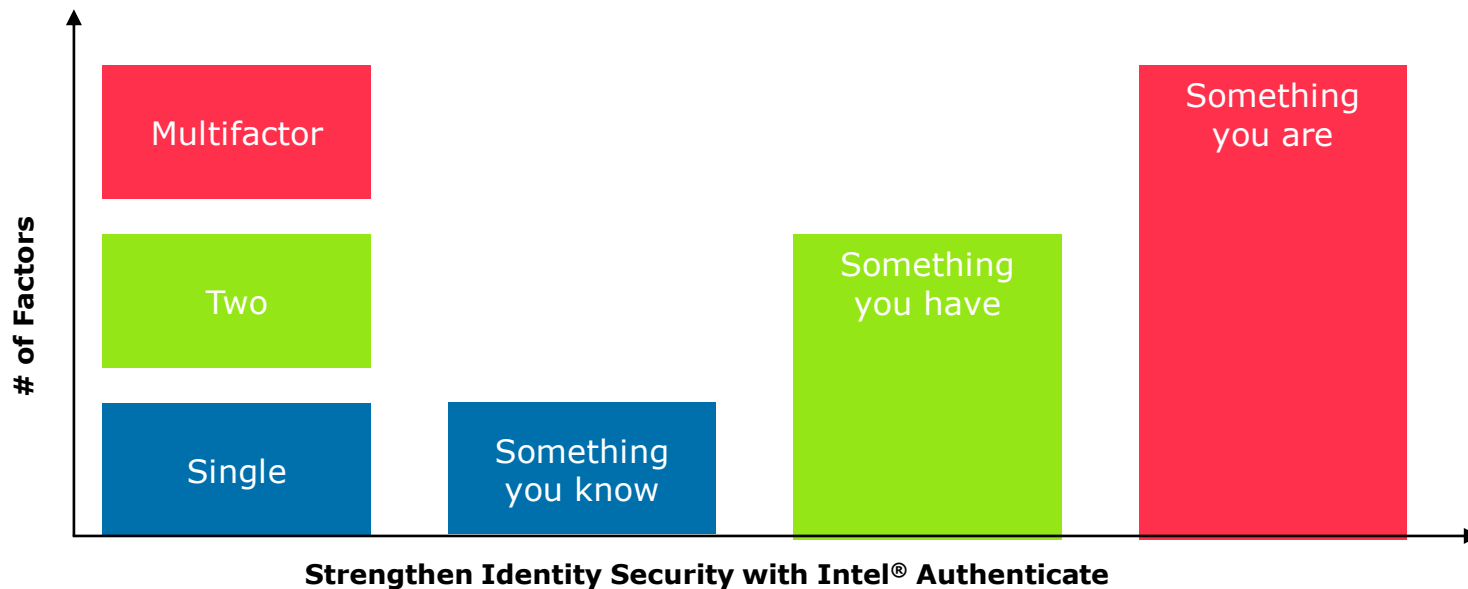
***“...Hospitals more likely to pay a ransom rather than risk delays that could result in death and lawsuits.”<sup>3</sup>***

*Wired, 2017*

# Intel® Authenticate: Multifactor Security1 at the Hardware Level

## Multiple Factors of Authentication (MFA)

Get the enhanced security of multifactor authentication with Intel® Authenticate and verify identities using a combination of two or more factors.



- Hardware-enhanced identity protection
- Multifactor authentication
- Works with your familiar Microsoft and McAfee environments
- Fast to deploy
- Add vendor security

*Additional hardware is not required.*

*Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at [iintel.com](https://www.intel.com).*

# 7th Gen Intel® Core™ vPro™ processors

## Increase Security + Gain Business Advantages



Up to 50% faster productivity<sup>1</sup> and 65 percent faster multitasking<sup>2</sup> than a 5-year-old PC.



Up to 16x improved storage performance with an Intel® Pro SSD over a 5-year-old PC.<sup>3</sup>



Up to 10 hours of untethered battery life for all-day performance.<sup>4</sup>



4K Ultra HD video, 360° video, multiple video streams, and premium playback.

1. As measured by the overall score of SYSmark 2014, which is a benchmark from the BAPCo consortium that measures the performance of Windows platforms. SYSmark tests three usage scenarios, including office productivity, media creation, and data/financial analysis using real applications from independent software vendors such as Microsoft and Adobe.

2. As measured by SEG562, which is an office productivity and multitasking workload using Word (save to PDF), Excel (recalc), PowerPoint (slide sort), and NXPowerLite Desktop (to shrink contents with office documents, kind of like compression), all while playing video in the background (simulating the watching of a business training or webcast).

3. As measured by the HDD Suite in PCMark Vantage, which is a benchmark from Futuremark that measures Windows everyday computing performance. PCMark Vantage is made up of several benchmarking suites: PCMark Suite (produces PCMark Score), Memories Suite, TV and Movies Suite, Gaming Suite, Music Suite, Communications Suite, Productivity Suite, and HDD Suite. The HDD Suite contains an operating system start-up workload that is sensitive to HDD versus SSD boot devices.

4. As measured by Windows 10 EEMBC Browsing Bench Component Average Power.



# Intel® Solid State Drive Pro 6000p Series



**Increase security against advanced threats—from devices and identities to data storage and networks.**

- Optimized for Windows® 10
- Built-in security features help safeguard against identity theft and protect network access<sup>1</sup>
- Automatic encryption and remote management capabilities<sup>1</sup>





01

## Intel® Remote Secure Erase

Intel® Solid State Drive (Intel® SSD) Pro provides remote secure-erase capabilities, so when an employee leaves the organization and the device changes hands, IT can erase the Intel SSD Pro without having to physically remove it, while also providing an audit trail to authenticate the process. Guards against malware beyond the network perimeter and endpoint devices.1



02

## Intel® Boot Guard

Provides hardware-based boot integrity protection and prevents unauthorized software and malware of boot blocks critical to a system's function, thus providing an added level of hardware-based platform security.



03

## Intel® BIOS Guard

Protects the BIOS flash from modification without platform manufacturer authorization, which helps defend the platform against low-level DOS (denial of service) attacks, and restores BIOS to a known good state after an attack.

*Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at [iintel.com](https://www.intel.com).*

01

## Intel® Trusted Execution Technology (Intel® TXT)

Provides a hardware-based security foundation, offering greater protection for information used and stored on the business PC. Intel TXT also provides a sealed portion of storage where sensitive data such as encryption keys can be kept, helping to shield them from being compromised during an attack by malicious code.

02

## Intel® Virtualization Technology (Intel® VT)

Improves application compatibility and reliability, and provides additional levels of manageability, security, isolation, and I/O performance.

Optional cloud management software allows for management of Intel® TXT-protected systems within the cloud.

### Intel® TXT-Protected Systems

Operating system or virtual machine (VM) management software builds upon protected hardware to ensure protection at the software layer. Optional attestation software allows for cloud management of hosts.

Multiple hardware components (BIOS, processors, etc.) work together to verify that the system hardware is protected.



*Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at [intel.com](https://www.intel.com).*





01

## Intel® Secure Key

Generates high-quality keys for cryptographic protocols. Intel Secure Key enables fast, true random number generation done in the hardware, with minimal user impact.



02

## Intel® OS Guard

Prevents malware from executing code in application memory space and from accessing data in user pages.



03

## Intel® Identity Protection Technology (Intel® IPT) with PKI

A second-factor authentication for business and web services that validates when a legitimate user (not malware) is logging in from a trusted PC. PKI is a system that helps verify and authenticate the validity of each party involved in an Internet transaction.

*Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at [intel.com](https://www.intel.com).*

# Enterprise Client Security

## Key Features & Solutions



### Identity Protection

- Intel® Authenticate



### Data Protection

- Intel® Data Guard
- Intel® SSD Pro Series Remote Secure Erase
- Intel® AES-NI
- Intel® Secure Key



### Threat Management

- Threat Management
- Intel® Platform Protection Technology with Intel® BIOS Guard
- Intel® Platform Protection Technology with Intel® OS Guard
- Intel® Memory Protection Extensions (Intel® MPX)



### Recovery

- Intel® Active Management Technology (Intel® AMT)



### Secure Foundation

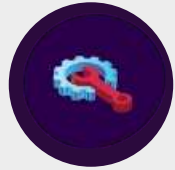
- Intel® Software Guard Extensions (SGX)
- Intel® Boot Guard
- Intel CSME

# Your End-point Security Strategy

## Strategy



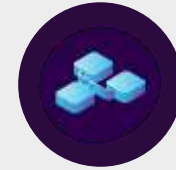
Threat Analytics



Intel® Data Guard



Intel® Authenticate



Intel® AMT  
Advanced Recovery



Comprehensive  
End-Point  
Security

← **Secure Platform Foundation** →

## About Sogeti

Sogeti is a leading provider of technology and engineering services. Sogeti delivers solutions that enable digital transformation and offers cutting-edge expertise in Cloud, Cybersecurity, Digital Manufacturing, Digital Assurance & Testing, and emerging technologies. Sogeti combines agility and speed of implementation with strong technology supplier partnerships, world class methodologies and its global delivery model, Rightshore®. Sogeti brings together more than 25,000 professionals in 15 countries, based in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Capgemini SE, listed on the Paris Stock Exchange.

Learn more about us at

[www.sogeti.com](http://www.sogeti.com)



This message contains information that may be privileged or confidential and is the property of the Capgemini Group.

Copyright© 2018 Sogeti. All rights reserved.