


A complex network diagram with numerous nodes and connecting lines, representing a system architecture or data flow, set against a dark blue background.

# **The security immune system**

An integrated approach to protecting your organization

Find out more 



# Why a security immune system **makes sense now**

We've heard it time and again.  
When it comes to cybersecurity threats, no one is immune.

No business, no government, no individual. In fact, the entire conversation has shifted from focusing on "if you're attacked" to "how quickly you can respond." And that's not likely to change in the foreseeable future.

So let's think about the concept of immunity for a minute. As humans, we have finely tuned — and highly adaptive — immune systems ready to help us fight off all kinds of attacks that would otherwise threaten to destroy us. Made up of cells, tissues and organs that work together to defend us against attacks by "foreign" invaders, a healthy immune system can distinguish between the body's own cells and those that don't belong. It's an intelligent, organized and efficient system that can instantly recognize an invader and take action to either block its entry or destroy it.

But when we look at cybersecurity, the traditional defense strategy is to layer on another point-product tool or technology to an already fragmented and disjointed IT environment.

That's why IBM has developed an integrated and intelligent security immune system.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



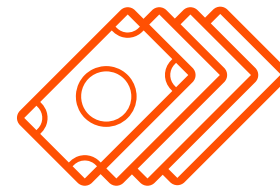
How it works:  
Four use cases tell the story



Why IBM



There will likely be  
**20.8 billion**  
“**connected things**”  
by 2020<sup>1</sup>



The average  
total cost of a data  
breach in 2016  
was **\$3.62 million**<sup>2</sup>



Unauthorized access accounted for  
**45 percent** of security incidents in 2015<sup>3</sup>

*Click on any bar at left to navigate the IBM Security immune system story.*

Next 



Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# Integration and intelligence take the lead

Today's expanded security arsenal of fragmented, disconnected point products has added complexity without significantly improving the overall security posture of the organization. The result? A bloated infrastructure that makes it more difficult to monitor the network as a whole, often leaving security teams to operate in the dark.

It's time to take a more holistic view  
of your security portfolio.

The IBM Security immune system is a fully integrated approach that allows its components to grow and adapt within the infrastructure — working together to deliver intelligence, visibility and actionable insights across the entire system.

And once the IBM Security immune system is fully engaged with your entire ecosystem — allowing collaboration across third-party vendors, technology providers and business partners — it can provide you with the intelligence you need to understand existing threats and adapt to new ones.

Next 



*Some organizations report they're using as many as 85 security products — from more than 40 vendors — at once. As each tool is added, the costs associated with installing, configuring, managing, upgrading and patching continue to grow. And with the skills gap plaguing the industry, it's easy to see how more threats are continuing to generate more vendors, more tools — and more headaches.*



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection

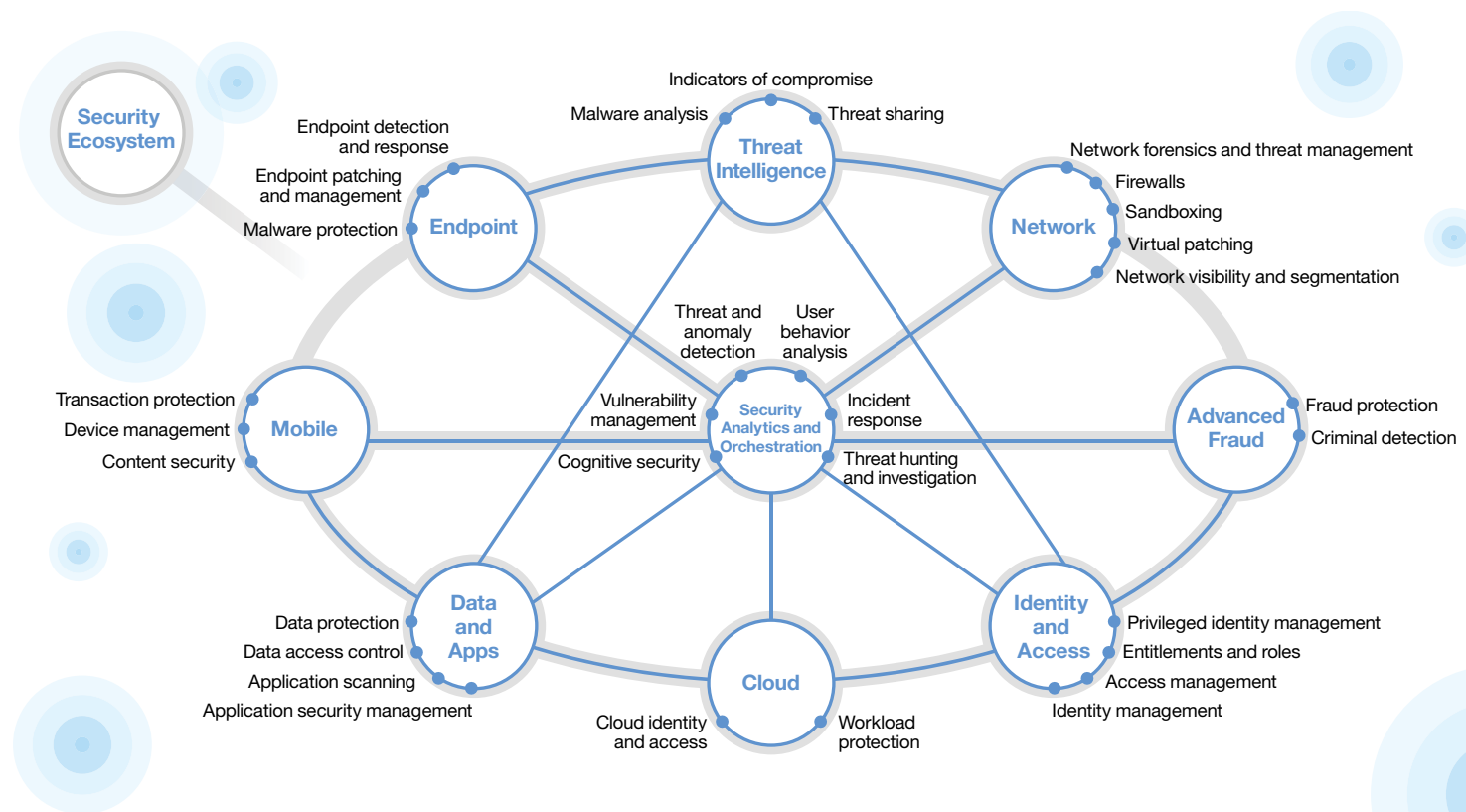


How it works:  
Four use cases tell the story



Why IBM

# Integration and intelligence take the lead



*The IBM Security immune system looks at a security portfolio in a more organized fashion—as an integrated framework of security capabilities that transmits and ingests vital security data to help gain visibility, understand and prioritize threats, and coordinate multiple layers of defense. At its core, the system uses security intelligence and analytics to automate policies and block threats—just as the human immune system can automatically assess and identify a virus, for example, and trigger an immune response.*

Next



Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# Integrating security **planning,** **response and readiness**

The [IBM Security immune system](#) delivers a full range of security solutions and services designed to address your organization's specific needs across three key areas.

## Security Transformation Services

Transform your  
security program



## Security Operations and Response

Build a  
cognitive SOC



## Information Risk and Protection

Take control of  
digital risk



Next 





Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# Security Transformation Services

## Helping to simplify your view of the big picture

[Security Transformation Services](#) let your organization take a more proactive, preemptive and mature approach to security. So you can:

- Access the right skills — with trusted security advisors, responders, testers, analysts and engineers — available 24x7x365 globally
- Build strategy that accelerates new IT trends, including BYOD, cloud, mobile, social and IOT
- Optimize security programs with technology that manages and protects against the latest threats
- Reduce complexity and consolidate fragmented solutions into an integrated solution
- Gain access to global threat intelligence for improved visibility into the threat lifecycle
- Build protected and connected systems to reduce operating costs and complexity



Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



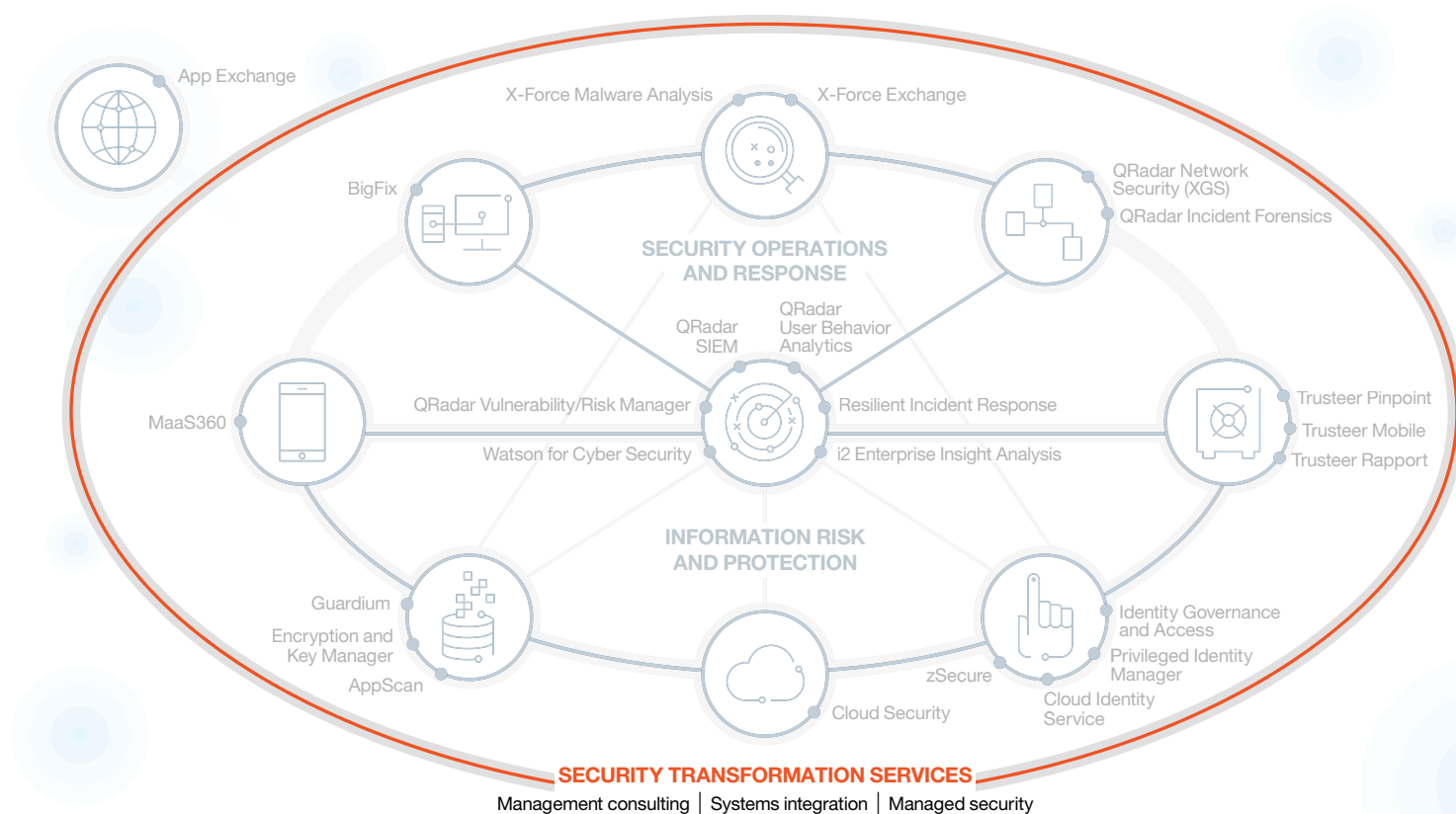
How it works: Four use cases tell the story



Why IBM

# Security Transformation Services

## Helping to simplify your view of the big picture



Next >





Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# Security Operations and Response

## Orchestrate your defenses throughout the entire attack lifecycle

Criminals are relentless. Hoping you aren't a target is not enough to keep the bad guys out—especially because they may already be inside your organization. And relying on perimeter solutions, periodic scans and compliance-driven methods won't keep you ahead of the threat.

The [Security Operations and Response](#) platform offers an integrated, end-to-end approach to safeguarding your systems. That means you can prevent, detect and respond to threats in an intelligent, orchestrated and automated manner. It's an approach that lets you:

- Continuously stop attacks and remediate vulnerabilities
- Take advantage of cognitive analytics to sense, discover and prioritize unknown threats
- Respond to incidents quickly and effectively, using deep threat intelligence provided by the IBM X-Force® Research team—and their massive threat databases—to hunt for indicators



Next



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



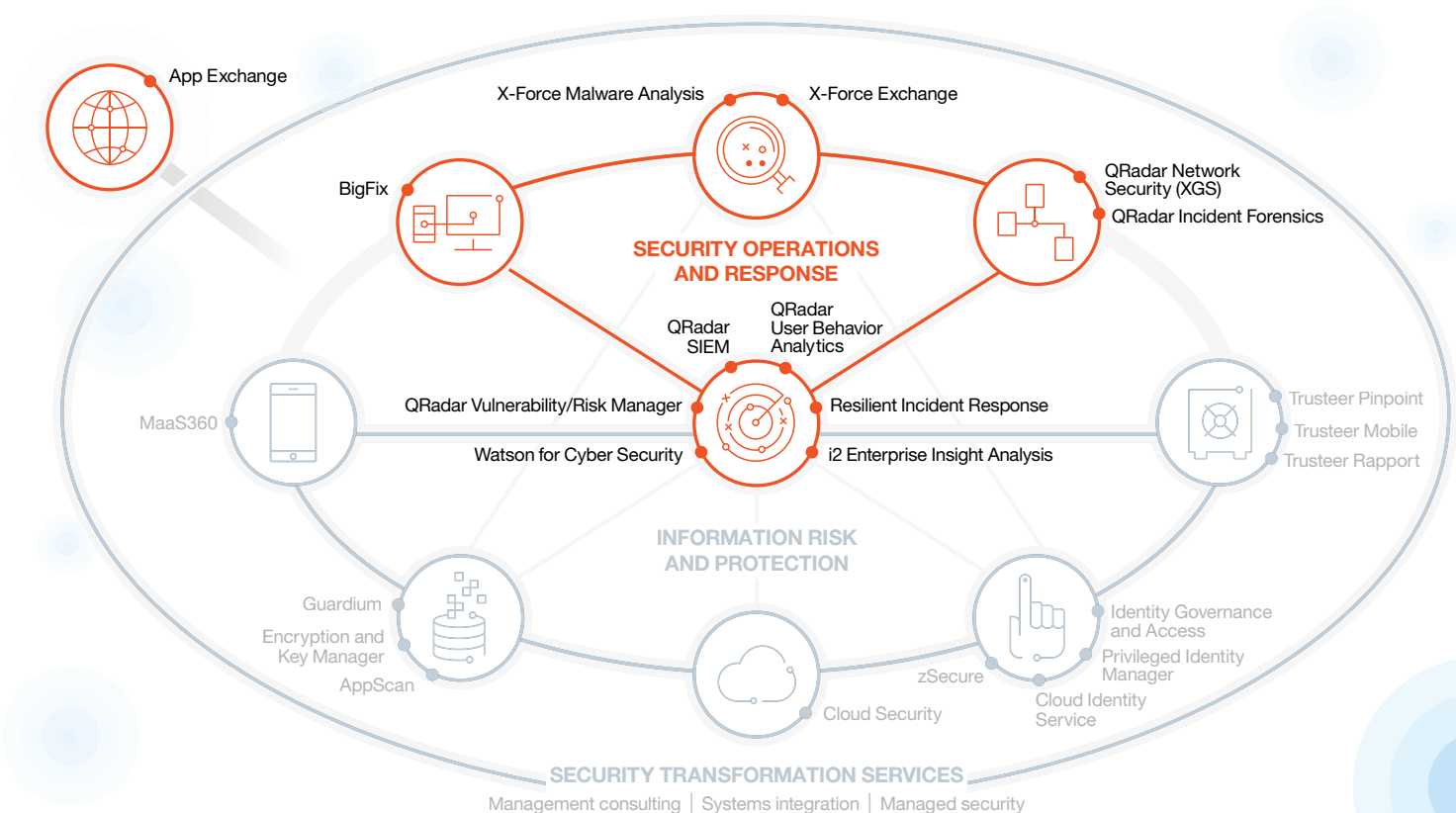
How it works: Four use cases tell the story



Why IBM

# Security Operations and Response

## Orchestrate your defenses throughout the entire attack lifecycle



Next >



Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# Information Risk and Protection

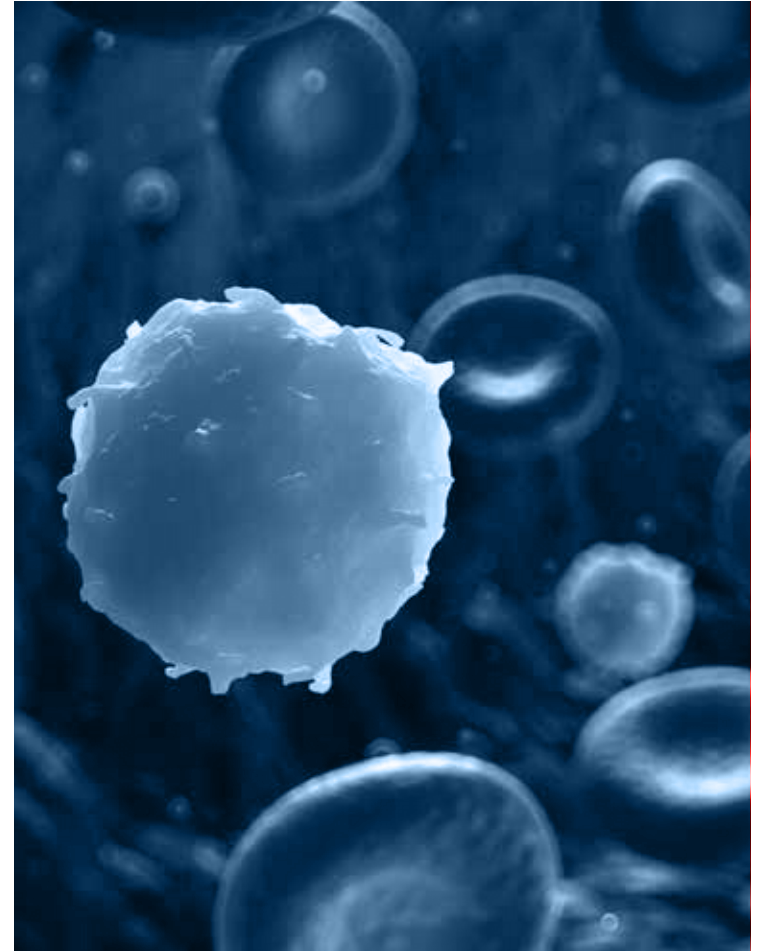
## Keep your critical information protected while accelerating business

Cloud and mobile computing, social media, big data and IOT are just a few of the innovations making dramatic changes to the business landscape. The result is more connectivity across users, apps, data and transactions than ever before. And that means more security issues for everyone involved.

The solutions and services that comprise the [Information Risk and Protection](#) domain can help protect your information while keeping your employees productive. They're designed to help safeguard critical data, users, apps and transactions wherever they live—in the cloud, on mobile devices or on local servers and media. They allow you to:

- Identify business risks — such as abnormal insider activity, rogue cloud app usage or web fraud — with identity analytics and real-time alerts
- Gain control of users, access and development, using identity governance and intelligence, app and data protection, DevOps security and mobile security
- Safeguard interactions with adaptive access and web app protection, identity federation to and from the cloud, data compliance and secure mobile collaboration

Next 





Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



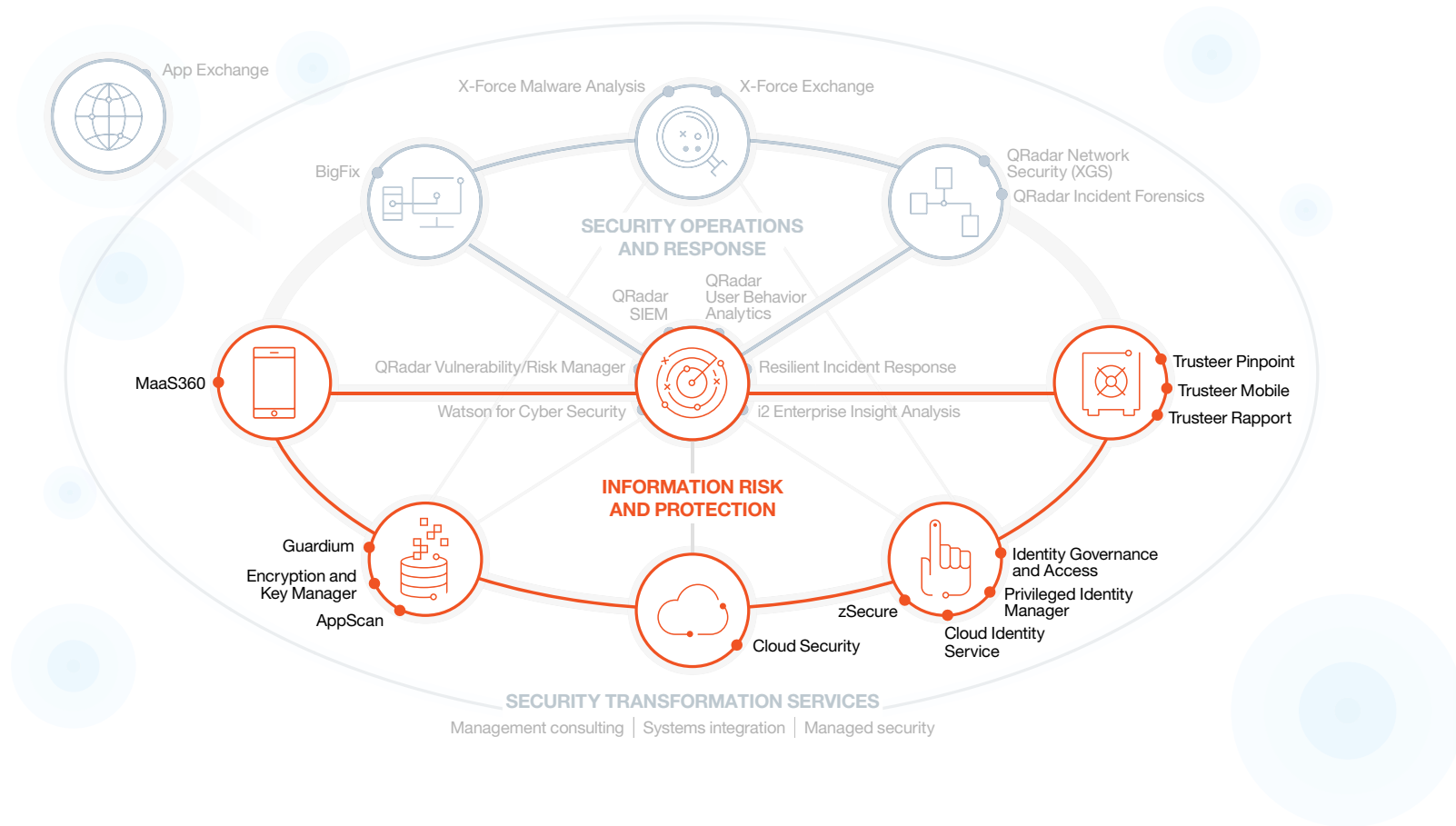
How it works: Four use cases tell the story



Why IBM

# Information Risk and Protection

## Keep your critical information protected while accelerating business



Next >



Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# How it works: Four use cases tell the story

Every organization faces its own security challenges. The following use cases offer a brief glimpse into how the [IBM Security immune system](#) would help four companies identify and respond to those challenges.

## The failed compliance audit



## The drive-by download



## The insider threat



## The potential for fraud



Next 



Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# A case in point: The failed compliance audit

Like most large organizations around the world today, Company A works hard to stay on top of an expanding — and ever-changing — security compliance environment. But despite the company's best efforts, it has failed a recent regulator-led audit and was found to be noncompliant with a set of newly released rules. The incident results in a fine and considerable reputational damage. This is where elements of the [Security Transformation Services](#) domain come into play.

**See how the story unfolds...**

①

**Gap  
assessment**

②

**Remediation**

③

**Ongoing  
monitoring**

④

**Continuous  
improvement**

⑤

**See the  
big picture**

Next 





Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works: Four use cases tell the story



Why IBM

# A case in point: The failed compliance audit

Like most large organizations around the world today, Company A works hard to stay on top of an expanding — and ever-changing — security compliance environment. But despite the company's best efforts, it has failed a recent regulator-led audit and was found to be noncompliant with a set of newly released rules. The incident results in a fine and considerable reputational damage. This is where elements of the [Security Transformation Services](#) domain come into play.



## Gap assessment

The failure also triggers an automatic security immune system response, which calls upon [IBM Security Strategy, Risk and Compliance Services](#) to help evaluate the audit findings — along with Company A's IT risk management framework, metrics and risk objectives.

In addition, [Security Framework and Risk Assessment from IBM](#) provides Company A with a list of existing gaps — prioritized according to business impact — and a set of recommended solutions for addressing any potential regulatory compliance gaps. Company A also receives a proposal for updated security education and training to help head off future audit issues.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works:  
Four use cases tell the story



Why IBM

# A case in point: The failed compliance audit

Like most large organizations around the world today, Company A works hard to stay on top of an expanding — and ever-changing — security compliance environment. But despite the company's best efforts, it has failed a recent regulator-led audit and was found to be noncompliant with a set of newly released rules. The incident results in a fine and considerable reputational damage. This is where elements of the [Security Transformation Services](#) domain come into play.



## Remediation

[Deployment and Migration Services from IBM](#) allow Company A to implement the necessary risk management solutions and align its governance practices. Remediation measures also establish new metrics to allow for better visibility into the effectiveness of the company's controls.

Next



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works: Four use cases tell the story



Why IBM

# A case in point: The failed compliance audit

Like most large organizations around the world today, Company A works hard to stay on top of an expanding — and ever-changing — security compliance environment. But despite the company's best efforts, it has failed a recent regulator-led audit and was found to be noncompliant with a set of newly released rules. The incident results in a fine and considerable reputational damage. This is where elements of the [Security Transformation Services](#) domain come into play.



## Ongoing monitoring

Once new metrics are established, [IBM Automated IT Risk Management Services](#) allow Company A to automatically monitor those metrics. It's a cost-effective solution that can align multiple aspects of the company's security program, offering increased visibility into control and compliance gaps and facilitating quick resolution.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works:  
Four use cases tell the story



Why IBM

# A case in point: The failed compliance audit

Like most large organizations around the world today, Company A works hard to stay on top of an expanding — and ever-changing — security compliance environment. But despite the company's best efforts, it has failed a recent regulator-led audit and was found to be noncompliant with a set of newly released rules. The incident results in a fine and considerable reputational damage. This is where elements of the [Security Transformation Services](#) domain come into play.



## Continuous improvement

With help from [IBM Security Strategy and Planning Services](#) and [IBM Security Architecture and Program Design Services](#), Company A can ensure that the key components of its compliance management efforts will be continuously evaluated and improved, allowing for ongoing compliance monitoring over the months and years to come.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



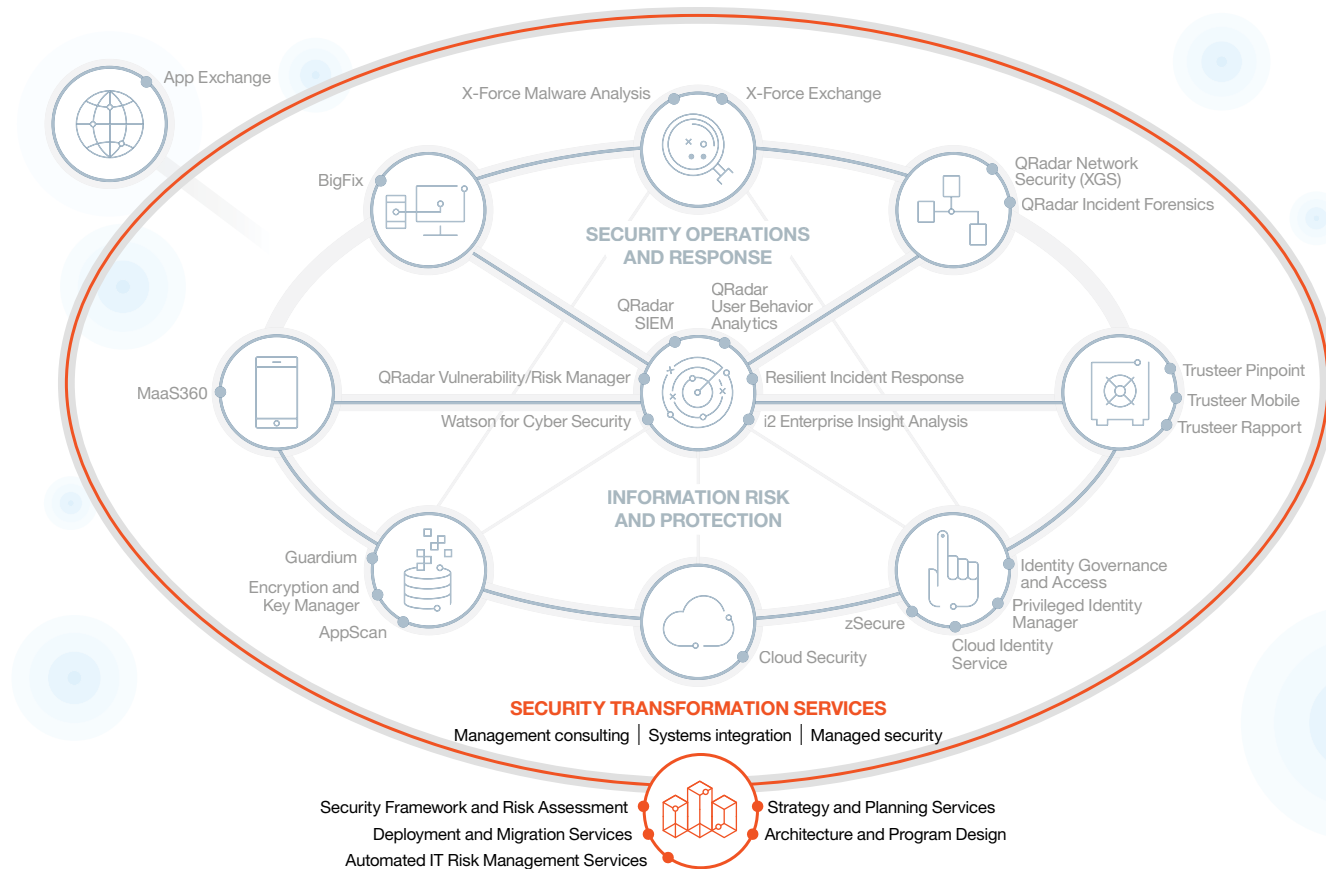
How it works: Four use cases tell the story



Why IBM

# A case in point: The failed compliance audit

Here's how the IBM Security immune system would call upon specific solutions to address the issues raised in the case of the failed compliance audit.



Next >



Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story




Why IBM

# A case in point: The drive-by download

There are countless ways in which determined attackers might go about getting into your systems without your knowledge. It happens all the time. Just check today's headlines for details on the latest high-profile break-in or data breach. Here's an example of how one such attack might be played out—and how several Security Operations and Response solutions can help disrupt the attack chain in real time.

## Here's how it all begins...



Next 





Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



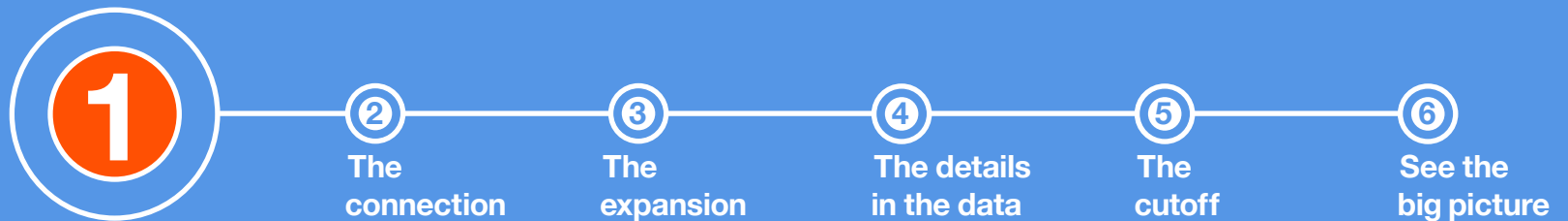
How it works: Four use cases tell the story



Why IBM

# A case in point: The drive-by download

There are countless ways in which determined attackers might go about getting into your systems without your knowledge. It happens all the time. Just check today's headlines for details on the latest high-profile break-in or data breach. Here's an example of how one such attack might be played out—and how several [Security Operations and Response](#) solutions can help disrupt the attack chain in real time.



## The break-in

One of Company B's account executives is in a taxi, on his way to the airport for a trip to a customer site. Stuck in traffic, he pulls out his laptop, checks the company's intranet for some project details and sends out a few emails. What he doesn't know is that he triggered an attack via drive-by download. And because he's almost always on the road, he hasn't had much contact with the company's IT security team. So his laptop may not have been updated with the latest patches.

[IBM BigFix®](#) would allow Company B's IT security team to discover unmanaged endpoints (such as this employee's laptop) and get real-time visibility into all its endpoints to identify vulnerabilities and those endpoints that are noncompliant.

Next



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



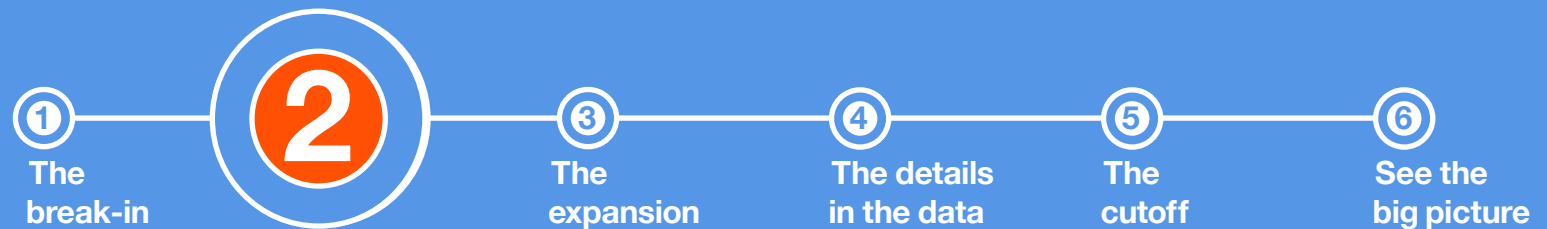
How it works: Four use cases tell the story



Why IBM

# A case in point: The drive-by download

There are countless ways in which determined attackers might go about getting into your systems without your knowledge. It happens all the time. Just check today's headlines for details on the latest high-profile break-in or data breach. Here's an example of how one such attack might be played out—and how several [Security Operations and Response](#) solutions can help disrupt the attack chain in real time.



## The connection

As it turns out, Company B's account executive had indeed missed getting the latest patches installed on his laptop. By the time he reaches the airport, the download has already latched onto the company's network and infects its internal system as part of a botnet.

With [IBM QRadar® Network Security \(XGS\)](#), Company B would be able to gain visibility into the network traffic, automatically analyze suspicious files with [IBM X-Force Malware Analysis on Cloud](#) and actively block communication with the botnet's command and control server, based on intelligence provided by [IBM X-Force Exchange](#). It can also effectively block zero-day exploit traffic and then send those traffic flows to [IBM QRadar Security Information and Event Management \(SIEM\)](#) for anomaly detection.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works:  
Four use cases tell the story



Why IBM

# A case in point: The drive-by download

There are countless ways in which determined attackers might go about getting into your systems without your knowledge. It happens all the time. Just check today's headlines for details on the latest high-profile break-in or data breach. Here's an example of how one such attack might be played out—and how several [Security Operations and Response](#) solutions can help disrupt the attack chain in real time.



## The expansion

Without those safeguards in place, however, Company B unwittingly allows the attack to continue, targeting internal email sent to high-profile employees.

At this point, [QRadar SIEM](#) could still help halt the attack by correlating network traffic flows and security events from other security controls—and external intelligence on active botnets from [IBM X-Force Exchange](#)—into a list of priority offenses.

Next



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works:  
Four use cases tell the story



Why IBM

# A case in point: The drive-by download

There are countless ways in which determined attackers might go about getting into your systems without your knowledge. It happens all the time. Just check today's headlines for details on the latest high-profile break-in or data breach. Here's an example of how one such attack might be played out—and how several Security Operations and Response solutions can help disrupt the attack chain in real time.



## The details in the data

The attackers soon come within striking distance, gaining the authorization needed to access Company B's resources. QRadar Incident Forensics would now be able to reconstruct abnormal user and database activity from the associated network packet data. This would allow investigators to discover less obvious data connections and previously hidden relationships across multiple IDs.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



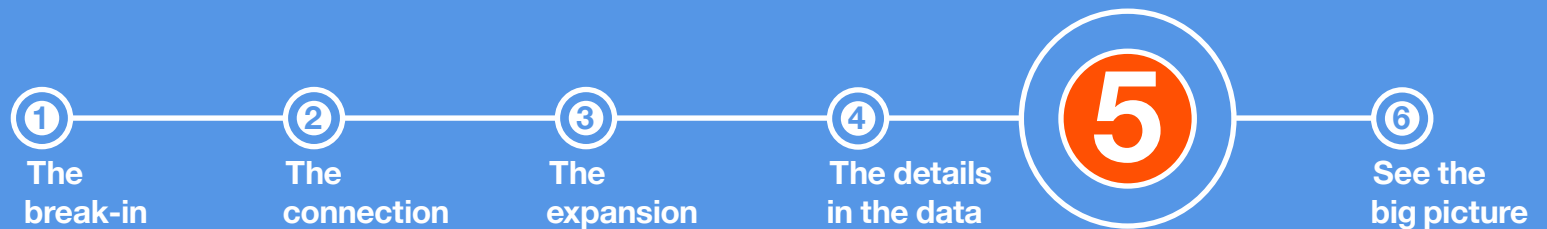
How it works:  
Four use cases tell the story



Why IBM

# A case in point: The drive-by download

There are countless ways in which determined attackers might go about getting into your systems without your knowledge. It happens all the time. Just check today's headlines for details on the latest high-profile break-in or data breach. Here's an example of how one such attack might be played out—and how several Security Operations and Response solutions can help disrupt the attack chain in real time.



## The cutoff

If the attackers manage to reach the point of siphoning out Company B's data, the IBM Resilient® Incident Response Platform™ could help the company's security team analyze, respond, resolve and mitigate the incident as quickly as possible. So they could take action to prevent or mitigate the damage inflicted by the attack.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



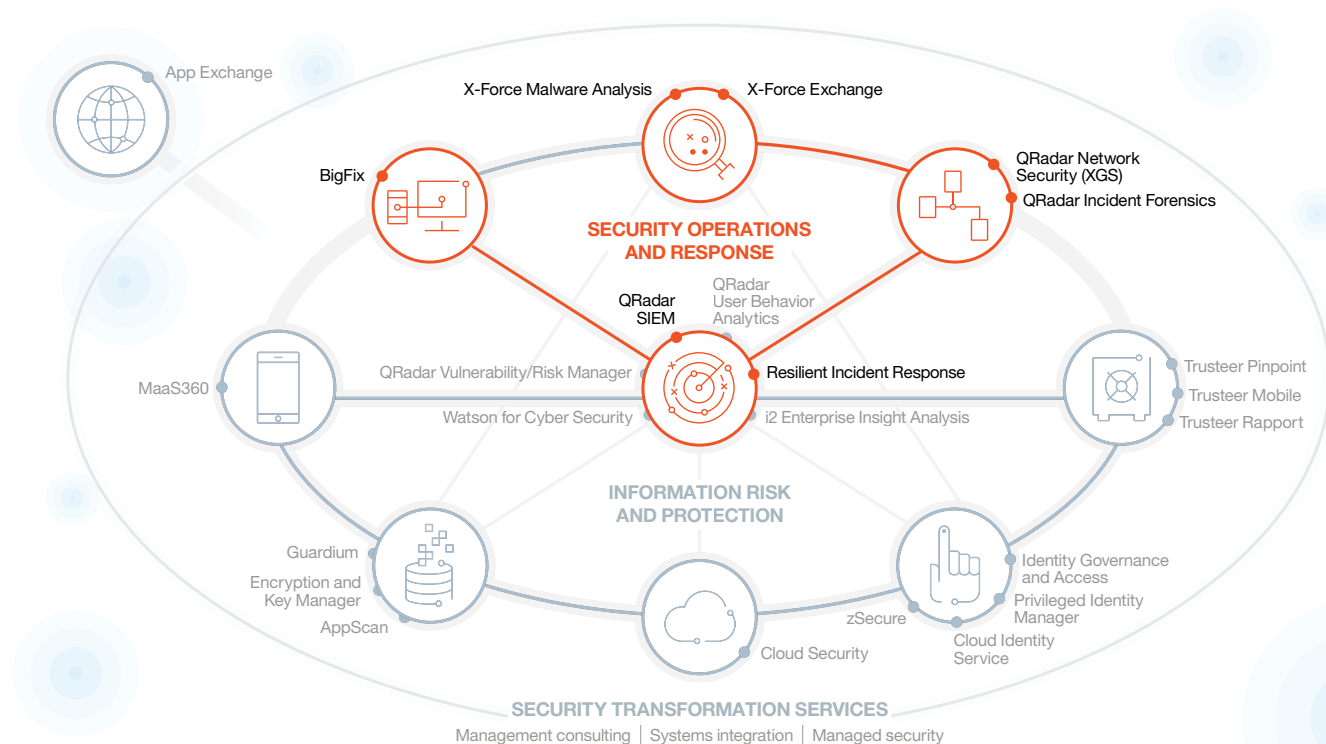
How it works: Four use cases tell the story



Why IBM

# A case in point: The drive-by download

Here's how the IBM Security immune system would call upon specific solutions to address the issues raised in the case of the drive-by download.



Next





Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# A case in point: The insider threat

Company C is aware that in 2015, 60 percent of attacks were carried out by insiders, either ones with malicious intent or inadvertent actors.<sup>4</sup> In other words, those attacks were instigated or initiated by people you would likely trust with access to your company's assets—including hard copy documents, disks, electronic files and laptops. Insiders could be employees of the company, or business partners, clients or even maintenance contractors. Here's an example of how [Information Risk and Protection](#) solutions help thwart insider threats.

## Follow the process...

①

**Privileged identity  
management**

②

**Activity  
monitoring**

③

**Security intelligence  
and analytics**

④

**Identity  
governance**

⑤

**See the  
big picture**

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works: Four use cases tell the story



Why IBM

# A case in point: The insider threat

Company C is aware that in 2015, 60 percent of attacks were carried out by insiders, either ones with malicious intent or inadvertent actors.<sup>4</sup> In other words, those attacks were instigated or initiated by people you would likely trust with access to your company's assets—including hard copy documents, disks, electronic files and laptops. Insiders could be employees of the company, or business partners, clients or even maintenance contractors. Here's an example of how [Information Risk and Protection](#) solutions help thwart insider threats.



## Privileged identity management

With multiple locations in both urban and suburban settings, Company C employs a large number of individuals—including part-time hourly workers and several levels of management personnel. In addition, there are often teams of contractors brought in to work on special projects. The one thing they all have in common? A need for ongoing access to the company's systems and data. That's why the company uses [IBM Security Privileged Identity Manager](#) to help prevent advanced insider threats. It provides a centralized approach to managing access to privileged accounts, allowing users to "check out" these accounts when they need access to sensitive systems. Each of these special sessions is automatically recorded, providing an audit trail and helping to ensure that privileged access is not misused. In addition, the company relies on [IBM Security Guardium®](#) to cross-reference that information as it audits user access to data that's either at rest or in motion.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works: Four use cases tell the story



Why IBM

# A case in point: The insider threat

Company C is aware that in 2015, 60 percent of attacks were carried out by insiders, either ones with malicious intent or inadvertent actors.<sup>4</sup> In other words, those attacks were instigated or initiated by people you would likely trust with access to your company's assets—including hard copy documents, disks, electronic files and laptops. Insiders could be employees of the company, or business partners, clients or even maintenance contractors. Here's an example of how [Information Risk and Protection](#) solutions help thwart insider threats.



## Activity monitoring

While monitoring and auditing privileged user access, [Guardium](#) can also identify abnormal or suspicious behavior and block illicit data and file access with real-time response. One day the system observes that several large files have been downloaded onto a thumb drive by one of Company C's part-time employees. Because the system recognizes that action as unusual activity—given the employee's responsibilities—it issues an alert flagging that behavior. Or it could deny access to the data in question. Company C might also take advantage of [IBM QRadar User Behavior Analytics](#) to gain early visibility into related insider threats by analyzing other employees' usage patterns to determine if their credentials or systems have been compromised. It can identify users by name, add suspects to a watch list or drill down into underlying log and flow data. What's more, [Guardium](#) can share any illicit activity it finds to help [QRadar User Behavior Analytics](#) fine-tune its analytics, and then go on to share any anomalous activity it finds with Guardium.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works: Four use cases tell the story



Why IBM

# A case in point: The insider threat

Company C is aware that in 2015, 60 percent of attacks were carried out by insiders, either ones with malicious intent or inadvertent actors.<sup>4</sup> In other words, those attacks were instigated or initiated by people you would likely trust with access to your company's assets—including hard copy documents, disks, electronic files and laptops. Insiders could be employees of the company, or business partners, clients or even maintenance contractors. Here's an example of how [Information Risk and Protection](#) solutions help thwart insider threats.



## Security intelligence and analytics

Taking matters a step further, [QRadar SIEM](#) can help Company C pull together a clearer picture of potential problems by using analytics to correlate [Privileged Identity Manager](#) credentials with [Guardium](#) activities—to detect anomalies and trigger alerts. And [IBM MaaS360®](#) lets the company manage and safeguard its mobile devices, applications and content—while maintaining data security and personal privacy.

Next



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works: Four use cases tell the story



Why IBM

# A case in point: The insider threat

Company C is aware that in 2015, 60 percent of attacks were carried out by insiders, either ones with malicious intent or inadvertent actors.<sup>4</sup> In other words, those attacks were instigated or initiated by people you would likely trust with access to your company's assets—including hard copy documents, disks, electronic files and laptops. Insiders could be employees of the company, or business partners, clients or even maintenance contractors. Here's an example of how [Information Risk and Protection](#) solutions help thwart insider threats.

①

**Privileged identity management**

②

**Activity monitoring**

③

**Security intelligence and analytics**

④

## Identity governance

[IBM Security Identity Governance and Access](#) lets Company C's IT managers and auditors govern insider access and ensure regulatory compliance across the organization. It helps the company mitigate access risks and access policy violations by combining intelligence-driven, business-driven identity governance with end-to-end user lifecycle management. What's more, it checks for segregation of duties violations and runs access certification campaigns to help ensure the validity of privileged access rights.

⑤

**See the big picture**

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



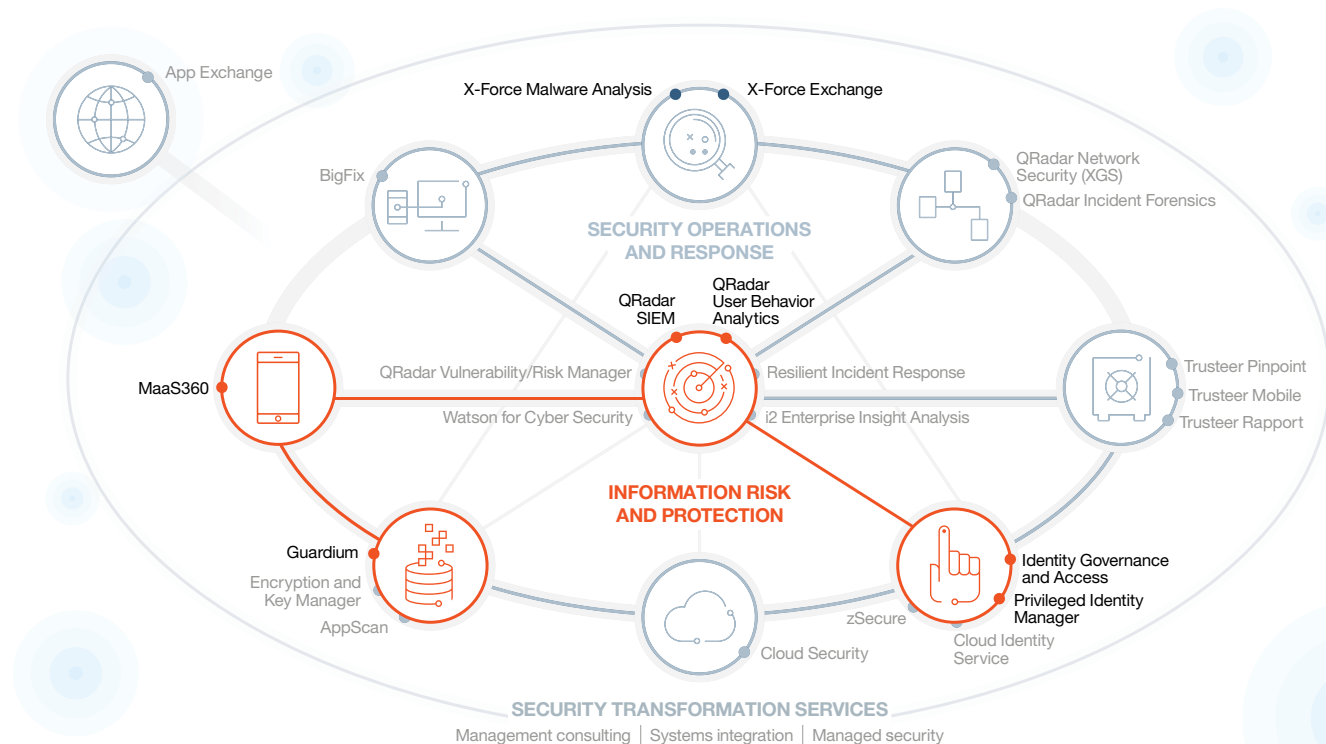
How it works: Four use cases tell the story



Why IBM

# A case in point: The insider threat

Here's how the IBM Security immune system would call upon specific solutions to address the issues raised in the case of the insider threat.



Next >





Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# A case in point: The potential for fraud

Most companies would find it difficult to discuss IT security without talking about fraud. And that's especially true for financial services organizations. Company D is engaged in the consumer side of the financial services business, where it's important to recognize that some of the very conveniences that banks now routinely offer customers—including automated teller machines, credit cards and mobile banking apps—have introduced a level of accessibility that goes a long way toward making the financial system highly vulnerable to cyber attacks. But [Information Risk and Protection](#) solutions can help significantly reduce the risk of fraud—without complicating the user experience.

**Learn what happens behind the scenes...**

①

Logging in

②

Protecting customers  
from fraud

③

Exercising  
necessary caution

④

See the  
big picture

Next 



Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# A case in point: The potential for fraud

Most companies would find it difficult to discuss IT security without talking about fraud. And that's especially true for financial services organizations. Company D is engaged in the consumer side of the financial services business, where it's important to recognize that some of the very conveniences that banks now routinely offer customers—including automated teller machines, credit cards and mobile banking apps—have introduced a level of accessibility that goes a long way toward making the financial system highly vulnerable to cyber attacks. But [Information Risk and Protection](#) solutions can help significantly reduce the risk of fraud—without complicating the user experience.



2

Protecting customers  
from fraud

3

Exercising  
necessary caution

4

See the  
big picture

## Logging in

Laura M. is a Company D customer who wants to move money from one of her accounts to another via mobile phone. It takes just a few seconds for her to log in, using her online ID and security code. But in those few seconds, [IBM Security Access Manager \(ISAM\)](#) is validating Laura's password, determining her location, making note of the date and time, and identifying the IP address for the device she's using. Doing so helps Company D block fraudulent and high-risk transactions by analyzing user information and correlating user behavior and device attributes in real time—so it can determine whether Laura is who she says she is.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works: Four use cases tell the story



Why IBM

# A case in point: The potential for fraud

Most companies would find it difficult to discuss IT security without talking about fraud. And that's especially true for financial services organizations. Company D is engaged in the consumer side of the financial services business, where it's important to recognize that some of the very conveniences that banks now routinely offer customers—including automated teller machines, credit cards and mobile banking apps—have introduced a level of accessibility that goes a long way toward making the financial system highly vulnerable to cyber attacks. But [Information Risk and Protection](#) solutions can help significantly reduce the risk of fraud—without complicating the user experience.



## Protecting customers from fraud

Next, [IBM Trusteer® solutions](#) help figure out whether Laura is a true customer or a fraudster—by determining whether the device she's using is valid, analyzing her behavior and helping to verify that neither her credentials nor her phone have been compromised. [Trusteer](#) also notes that Laura isn't just checking her account balance, but wants to transfer funds from one account to another. If it finds any evidence to suspect that it's dealing with a fraudster, it can restrict functionality based on bank policies, without alerting him or her that they've been detected. All this happens behind the scenes—in seconds—without giving Laura any reason to know or care about what's going on.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



How it works: Four use cases tell the story



Why IBM

# A case in point: The potential for fraud

Most companies would find it difficult to discuss IT security without talking about fraud. And that's especially true for financial services organizations. Company D is engaged in the consumer side of the financial services business, where it's important to recognize that some of the very conveniences that banks now routinely offer customers—including automated teller machines, credit cards and mobile banking apps—have introduced a level of accessibility that goes a long way toward making the financial system highly vulnerable to cyber attacks. But [Information Risk and Protection](#) solutions can help significantly reduce the risk of fraud—without complicating the user experience.

①

Logging in

②

Protecting customers from fraud

3

④

See the big picture

## Exercising necessary caution

Of course there are certain circumstances under which Laura's actions might be subject to additional scrutiny to help protect both the bank and herself. For example, [ISAM](#) could move to enforce additional rules, asking Laura to perform a second authentication step (such as getting a second password) if she wanted to transfer over \$10,000. And if she wanted to transfer millions of dollars, even multi-step authentication would likely be insufficient. She would instead be told to visit the bank in person.

Next 



Integration and intelligence take the lead



Integrating security planning, response and readiness



Security Transformation Services



Security Operations and Response



Information Risk and Protection



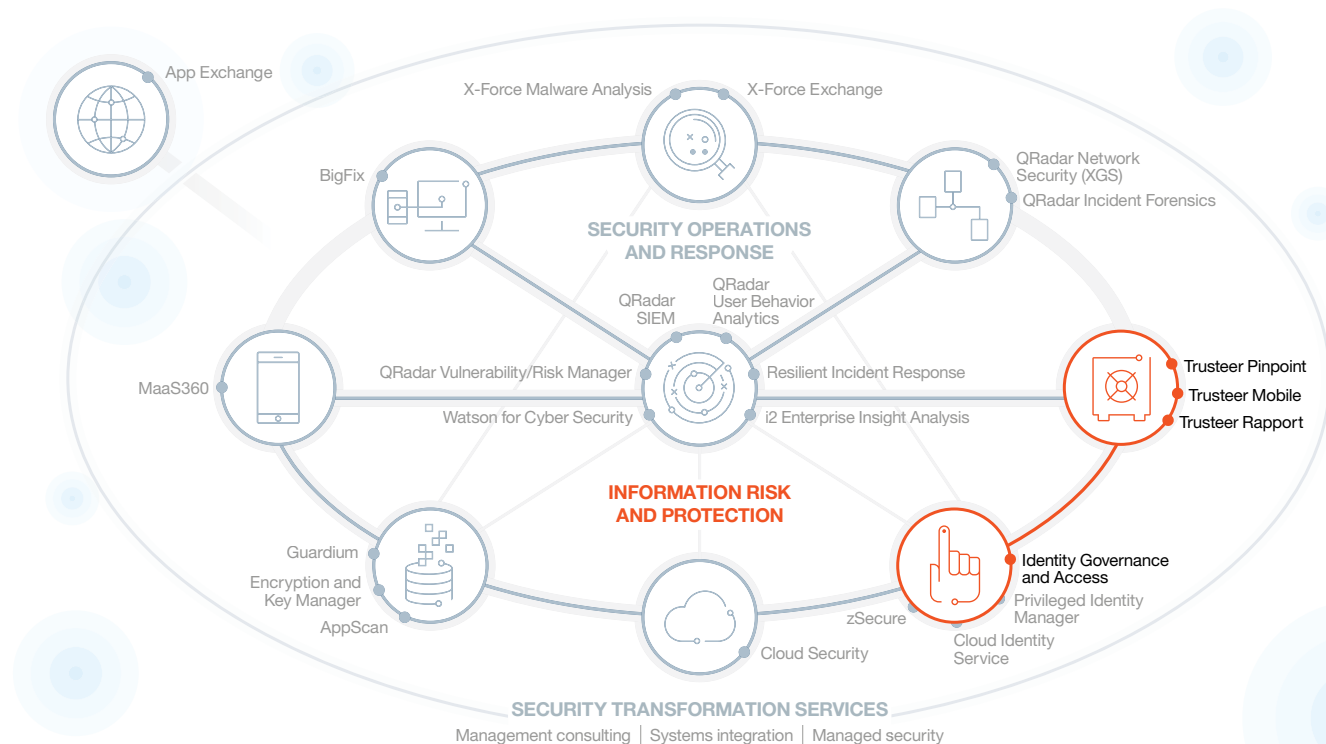
How it works:  
Four use cases tell the story



Why IBM

# A case in point: The potential for fraud

Here's how the IBM Security immune system would call upon specific solutions to address the issues raised in the case of potential fraud.



Next >



Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# Why IBM

Today's threats continue to rise in numbers and scale, as sophisticated attackers break through conventional safeguards every day.

The demand for leaked data is trending toward higher-value records containing personally identifiable information and other highly sensitive data, with less emphasis on the emails, passwords and even credit card data that were the targets of years past.<sup>5</sup>

And hardly a week goes by when the media isn't reporting that yet another prominent organization has fallen victim to a data breach, costing many millions of dollars. In fact, the average cost of a data breach is now \$3.62 million.<sup>6</sup>

A piecemeal approach to security simply will not work. It's time to move beyond methods that assemble defenses for specific needs but lack the integration to extend security across enterprise assets and vulnerabilities. It's time for a comprehensive, integrated security immune system that delivers leading technology, best practices and flexibility. To protect your valuable resources, you need a system that relies on today's intelligence, not yesterday's narrow definition of known threats.

Next 

When you partner with IBM, you gain access to a security team of more than 8,000 people supporting more than 12,000 customers in 133 countries. As a proven leader in enterprise security, we hold more than 3,500 security patents. And by combining the security immune system with advanced cognitive computing, we let organizations like yours continue to innovate while reducing risk. So you can continue to grow your business — while securing your most critical data and processes.

## For more information

To learn more about the IBM Security portfolio of solutions, please contact your IBM representative or IBM Business Partner, or visit:

[ibm.com/security](https://ibm.com/security)

Additionally, IBM Global Financing offers numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit:

[ibm.com/financing](https://ibm.com/financing)

Appendix 

Legal 





Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM

# Appendix

Click on the links below for more information on the following IBM products and services mentioned in this brochure:

[IBM Security Strategy, Risk and Compliance Services](#)

[Security Framework and Risk Assessment from IBM](#)

[IBM Automated IT Risk Management Services](#)

[IBM Security Strategy and Planning Services](#)

[IBM Security Architecture and Program  
Design Services](#)

[IBM BigFix](#)

[IBM QRadar Network Security \(XGS\)](#)

[IBM QRadar Security Information and  
Event Management](#)

[IBM X-Force Exchange](#)

[IBM X-Force Malware Analysis on Cloud](#)

[IBM QRadar Incident Forensics](#)

[IBM Resilient Incident Response Platform Standard](#)

[IBM Resilient Incident Response Platform Enterprise](#)

[IBM Security Privileged Identity Manager](#)

[IBM Security Guardium](#)

[IBM QRadar User Behavior Analytics](#)

[IBM MaaS360](#)

[IBM Security Identity Governance and Intelligence](#)

[IBM Security Access Manager \(ISAM\)](#)

[IBM Trusteer Solutions](#)

[IBM Application Security Solutions](#)

[IBM Security App Exchange](#)

Next 

Legal 



Integration and  
intelligence take  
the lead



Integrating security  
planning, response  
and readiness



Security  
Transformation  
Services



Security  
Operations and  
Response



Information  
Risk and  
Protection



How it works:  
Four use cases  
tell the story



Why IBM



© Copyright IBM Corporation 2017

IBM Security  
75 Binney Street  
Cambridge MA 02142

Produced in the United States of America  
July 2017

IBM, the IBM logo, ibm.com, BigFix, Guardium, Maas360, QRadar, Resilient Incident Response Platform, Trusteer, X-Force and zSecure are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

- <sup>1</sup> [Gartner Press Release, Gartner Says 6.4 Billion Connected “Things” Will Be in Use in 2016, Up 30 Percent From 2015, November 10, 2015.](#)
- <sup>2</sup> [Ponemon Institute, 2017 Cost of Data Breach: Global Overview, June 2017.](#)
- <sup>3,4</sup> [Reviewing IBM a year of serious data breaches, major attacks and new vulnerabilities, April 2016.](#)
- <sup>5</sup> [IBM X-Force Threat Intelligence Report – 2016.](#)
- <sup>6</sup> [Ponemon Institute, 2017 Cost of Data Breach: Global Overview, June 2017.](#)