IBM Security: A new way

IBM provides thousands of security experts and an integrated portfolio of security solutions to help you detect and prevent advanced threats

We enable people to do business. We make IT work through partnership, knowledge and passion: trusted to run IT infrastructure and services for leading business across Europe for 40 years.

Contents

Introduction

We live in a golden age of information. Advances in data science, analytics and smart networks are helping produce breakthroughs across a range of endeavors—how doctors treat disease, students learn, and businesses innovate, to name just a few.

But a new breed of criminal—the cyber attacker—is poisoning the well. Invisible, patient and deliberate, these intruders electronically tunnel into an organisation's network and computers, blending in with the environment so they're not noticed. Then, when the time is right, they steal sensitive data such as credit card numbers, trade secrets and personal information. They cause enormous damage—one estimate puts the annual cost of cybercrime at more than USD400 billion.[1]

This is more than just a group of amateur hackers. This is a fundamental shift in the nature of organised crime that could destroy the progress reaped from the revolution in computing, software and connectivity. It's a new kind of threat that demands innovative thinking about security.

Modernise security with an intelligent, end-to-end approach

To fight today's cyber threats, you have to move past the "moats and firewall" and compliance-driven approaches of traditional security practices. Instead, you need to harness adaptive analytics, intelligent defenses, and integrated controls to uncover and disrupt attacks in real time.

But technology by itself isn't the "silver bullet." In fact, no single solution is. You need rigorous policies and management systems as well—programs that proactively protect all parts of the organisation, across your users, data, applications and infrastructure.

To do it right, you need to focus on four key outcomes: optimising your security programs, stopping advanced threats, protecting critical assets, and safeguarding cloud and mobile environments.

[1] "Net Losses: Estimating the Global Cost of Cybercrime,"Center for International and Strategic Studies/McAfee, June 2014. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

How are you optimising your security program?

An optimised security program means clearly stated policies and strategies, rigorous programs and a strong, cohesive team to implement them. Yet the challenges can be enormous. Some of the most common issues include:

- **No clear strategy:** You haven't yet taken a careful inventory of your security strategy. You're addressing critical challenges with no roadmap for the future – and no big-picture guidance.
- **Fragmentation woes:** Your team has to play "whack-amole" – responding to security concerns with a new tool foreach emerging risk. And now you have a maze of disparate solutions with limited views of the landscape. This can be costly, complex and ineffective at stopping today's sophisticated attacks.
- **Lack of adequate skills:** It's a seller's market for security skills—with many openings for a limited number of candidates. And because the battle to secure your organisation constantly evolves as new threats emerge, the skills gap inevitably widens. If you can't adequately measure your organisation's security effectiveness, you won't know where to begin—whether you have an effective strategy in place or not.
- **C-level priority:** Headlines about security breaches have ratcheted up boardroom concern over potential data breaches. Now you're being asked to present to the CEO and the board at least once a year, and possibly even more often. How do you communicate your priorities and results in a way—free of "security lingo"—that speaks to their way of thinking?

The way forward

IBM can help you design a security roadmap for the future. We'll work with you to evaluate and benchmark your security capability against your competition. Then, we can apply our security expertise and solutions to help you move toward an integrated security approach.

A new approach to optimizing security:

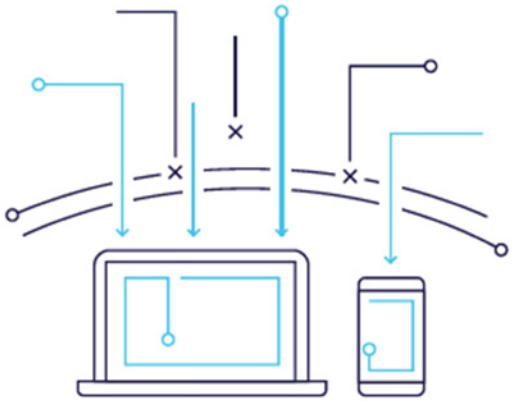
- **Assess and transform your security posture:** You need to grade your security maturity against your peers and relentlessly test for compliance with industry standards. We can help you analyse the effectiveness of your controls and develop a roadmap to reduce future risk. Importantly, we'll show you how to guide the conversation as you work with key stakeholders and top executives to quickly implement change.
- **Build next-generation security operations:** Are you treating security as a path to reduce risk and grow your business? If not, start now. Be systematic. Define the capabilities your organisation needs to stay secure. Then, apply intelligence and automation to minimise surprises and ease routine tasks. We excel at this. We're eager to help.
- **Get help from worldwide experts 24x7x365:** Engage professional "cyber hunters" to help detect attackers, deploy new solutions or run operations. The IBM consulting and managed services team is ready to help your security staff shore up skills gaps and understand complex threats. We do this by using our advanced expertise and access to worldwide threat information. We want to build a valuable partnership with you and your team.

Can you stop advanced threats?

Sophisticated cyber threats are on the rise. More than 95 percent of chief information security officers (CISOs) think they'll experience an advanced attack in the next 12 months.[2] And nearly 90 percent of CISOs believe today's advanced security threats cause substantially more damage than traditional threats.[3]

What's an advanced threat? A sophisticated, targeted attack on a system, executed by organised cyber attackers motivated by financial gain, politics or fame. Unlike worms, Trojans or viruses—which can easily be blocked by network and endpoint security defenses—advanced threats are quietly planted, can remain in a system for months or even years, and are far more difficult to detect. Once implanted, they collect information and maximise damage to your organisation.

At IBM, our experts use extensive research and detective work to thoroughly understand the origins and distinctive features of attackers. This allows us to pinpoint, outsmart and stop them. If a client is breached, we have teams of "first responders" who can diagnose and fix the problem.



The way forward

Intelligence is built into every aspect of our security portfolio. Along with integration, it's the path to a strong security posture. Use analytics and insight to stop advanced threats and create a unified defense. At the same time, move toward a fully-integrated system design.

Top ways to stop advanced threats:

- Prevent targeted attacks in real time: We can help you stop sophisticated threats with next-generation defenses. Armed with our latest cybercrime solutions, you'll be able to detect threats faster and make informed decisions by correlating massive sets of data in real time.
- Detect advanced threats with security intelligence: You can respond to breaches faster and actually stop sophisticated threats in real time with IBM big-data analytics.
- Defend against web fraud and cybercrime: Integration is key to stopping advanced threats. Maintaining visibility and coordination across security domains is vital. We'll help you reduce operating costs and infrastructure complexity with integrated controls and managed services.

[2] CEB Information Risk Leadership Council, "2015 Security Outlook – Ten Imperatives for the Information Security Function," November 2014.

[3] Corporate Executive Board, "Responding to Advanced Threats," February 2014.

How safe are your critical assets?

Not long ago, your organisation only had to worry about employees accessing a few highly controlled applications within your network. All that has changed. Everything and everyone is interconnected. As a result, you may be facing any of these challenges:

- Your enterprise has potentially millions of customers, partners, vendors and other users coming into your system seeking access to records.
- Data use has increased exponentially, and the rate of new applications being developed in the world of mobile applications is astonishing. This explosive velocity and volume is probably stressing your security systems.
- Well-funded and highly effective cyber attackers are working night and day to find vulnerabilities in these new platforms. Worse, they now use social media to track down your authorised users to steal their credentials and exploit vulnerabilities.
- The Internet of Things, with potentially billions of connected devices and new applications, introduces a new level of vulnerability. Your current security policies may not address machine-to-machine communications, and connected devices may not be protected by traditional security solutions.
- New applications can present vulnerabilities and have major security flaws.

It's no wonder security breaches are occurring more and more often. To protect your sensitive data, you must adopt a new, risk-based approach.

The way forward

IBM offers a variety of software and services to help you protect critical assets—from advanced security controls and analytics to commonsense methods of strengthening your data protection program.

How to protect critical assets:

- **Govern and administer users and their access:** Validate "who's who" across the enterprise and the cloud, and use context-aware and role-based controls to help prevent unauthorised access. These controls are smart enough to know where users are, what they want to do and what their normal behavior looks like – all before they're granted access. Hunt for breaches by collecting data that's security-relevant from across the enterprise. Deploy security intelligence technologies for real-time analysis, fraud prevention and anomaly detection. Expand your security prowess with external threat intelligence.
- **Identify and protect sensitive data:** Discover and classify critical data assets. Protect this information with intelligent controls that monitor who is accessing that data and from where. Detect anomalies and unauthorized access. Look for subtle attack indicators using deep security analytics.
- **Manage application security risk:** Analyse the security vulnerabilities of applications before they go into production—avoiding the costs of fixing them later and the potential damages from addressing victims' losses. Address security from day one.
- **Manage and secure your network and endpoints**: Enforce compliance, block threats and remediate vulnerabilities with near real-time visibility.

Are you effectively safeguarding cloud and mobile?

Has your organisation adopted a mobile platform, launched social media initiatives or embraced cloud computing? If so, you know that more and more business transactions are being pushed outside company walls. One example: as cloud platforms continue to be adopted, the traditional perimeter around the data center is dissolving, making it difficult to protect critical data from the increasing gaps in security.

Beyond the cloud, many enterprises are adopting bring-your-own-device (BYOD) policies and other mobile initiatives to better engage employees and customers. But as the linesbetween personal and work life blur, mobile security is paying the price.

If your security team has been grappling with these challenges,you are not alone.

Security executives have many concerns around these new initiatives. Keeping data private and secure in a cloud environment is now the primary concern of CISOs.[4] They also fear the danger of mobile device theft and loss. In fact, 76 percent of CISOs see device theft or the loss of sensitive data on a device as a major concern.4 Still, fewer than half of security leaders feel that they have an effective mobile device management approach. A clear gap exists between business demands and security realities.[5]

The way forward

IBM can help your firm avoid being compromised. We have experts who can work with your security team to build a new, stronger security posture designed for cloud and mobile initiatives. Remember, it's vital to address security at the initial deployment of cloud and mobile technologies.

Ways to safeguard cloud and mobile:

- **Gain cloud visibility and control:** Harden workloads and monitor attack activity while supporting compliance in the cloud. The IBM portfolio of security products is cloud-ready. That means we can help protect your organisation's employees and customers, data, applications and infrastructure as you build your private cloud. We work with many cloud service providers to build security into their offerings.
- **Help protect the mobile enterprise:** Protect devices, content, applications and transactions. These are the capabilities most requested by our clients today for mobile security. Commit to addressing mobile security from day one.
- **Adopt a security infrastructure-as-a-service model:** Leverage the ease of use, global availability and flexibility of cloud-based security. Hosted solutions can help reduce the costs of maintaining your own security infrastructure, while also addressing the growing shortage of skilled security staff.

[4] IBM MDI, "Chief Information Security Officer Survey," 2013.

[5] IBM Center for Applied Insights, "Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment," IBM Corp., December 2014. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGL03061USEN&attachment=WGL03061U=SEN.PDF#loaded

The IBM Security difference

Cyber attackers aren't the number one threat to an organization's security. Complacency and procrastination are.

Delaying a security program audit, postponing a major upgrade to your threat protection system, confusing regulatory compliance with a strong security posture – all are signs that you could be left vulnerable to an attack that damages your organisation's revenue, reputation and success. You must address security issues sooner rather than later, and it helps to have a worldwide industry trailblazer on your side.

At IBM, our new approach to security is centered in three key areas:

- **Intelligence:** Security intelligence is at the core of the IBM Security portfolio. IBM Security can provide the deep analytics and visibility organisations like yours need to help ward off a wide range of threats.
- **Integration:** IBM Security solutions and services integrate new and existing security capabilities across domains. This delivers critical visibility, provides comprehensive controls and helps reduce complexity.
- **Expertise:** IBM expertise stems from more than 6,000 hands-on professionals and researchers supporting customers in more than 130 countries. Our deep insight comes from monitoring more than 270 million endpoints and managing 15 billion events each day—and is built into IBM products and services, provided via real-time client feeds and embedded in professional engagements.

Get the strong defense you need against new and unknown threats by partnering with IBM, a proven leader in enterprise security. We're committed—through research and development investment, hiring and retaining the best talent, and extensive thought leadership—to helping you safeguard your organisation. Our new approach to security can enable organisations like yours to innovate while reducing risk. We can provide you a pathway for growing your business—while helping secure your most critical data and processes.

Premier Business Partner

We make IT work

People do business. We make it work.

T: 0121 281 8618 E: online@scc.com W: www.scc.com