



7 steps to a holistic security strategy



Success starts with security

Security is the number one focus and priority for organisations today. Protecting your organisation continues to be increasingly difficult as employees use their own devices and applications at work and data flows into and out of your business in a variety of ways. While the attack surface has broadened, attacks have also become more sophisticated and more damaging. Today's security leaders must balance these challenges with business needs to collaborate, innovate and grow.

Traditional security models have focused on layered perimeter defences and building "better walls." The world has changed. Today, organisations need to have an always-on and multifaceted approach to security that constantly protects all endpoints, detects the early signs of a breach and responds before that threat can cause damage. The reality

is, with the increasing scale and sophistication of cyber threats, no matter how strong your defences are, organisations need to adopt an "assume breach" approach. Preventive security measures are no longer sufficient, and you must now complement them with detection and response.

Security leaders know that building security frameworks on the presumption of compromise can mean faster detection and threat mitigation. Modern automated tools, including analytics based on machine learning and artificial intelligence, can also help expedite response. These new technologies can increase the effectiveness of security measures while reducing the burden placed on analysts who must otherwise sift through event data and alerts manually.

Today, the goal for modern CISOs centres on how well their organisations can manage risk. The challenge is to make security measures more effective against a backdrop of staffing shortages and an ever-expanding attack footprint of users, devices, applications, data and infrastructure.

Today's CISOs have evolved their approaches and their aims from safeguarding assets to building agile security frameworks that enable digital transformation. These strategies are holistic in that they embed the latest technologies into enduring processes and training programmes. This eBook shares the strategies and best practices of CISOs that have made security the cornerstone of business success.

Sections

1. Integration and rapid response
2. Lack of security talent
3. Growing numbers of endpoints
4. Speed and agility of threat actors
5. Moving to the cloud securely
6. Risks of shadow IT
7. Balancing end-to-end data protection with productivity

"It's like going to the gym every morning. Every hour of the day, you need to be prepared. And so that means you have to exercise this operational security posture on a continuous basis."

- Satya Nadella, Microsoft CEO



Section 1

Integration and rapid response

Threat actors have evolved from "smash-and-grab" methods of attack to compromising systems with the goal of maintaining a persistent, long-term presence.

Today's attackers pursue a variety of attack vectors and use a wide array of advanced tools and techniques: stealing credentials, installing malware that erases itself to avoid detection, modifying internal processes and rerouting network data, employing social engineering scams and targeting employee mobile phones and home devices.

Against this rapidly evolving threat landscape, organisations have deployed more and more security tools, many of them designed to address

specific issues. This means that each solution has its own vendor-specific dashboard, console and logs. In addition, these solutions rarely work together.

This lack of integration makes it difficult for security professionals to see everything that's happening all at once and to prioritise threats quickly. This is even more difficult as professionals manage both cloud and on-premises resources. As a result, industry reports show that today's attacks can go undetected for around 140 days.¹

The common approach has been to use Security Information and Event Management (SIEM) solutions to better correlate the information from a variety of

The average large organisation has

75
security products.²



tools. However, these tools aren't perfect and detection still depends on security teams doing out-of-band processing of logs and data, prioritising incidents and performing investigations. Data gathering and reconciliation are difficult, and the lack of a unified view makes both response and management cumbersome.

As rapid detection and response become bigger priorities, information security leaders should focus on gaining a holistic view across their entire network that includes cloud and hybrid environments. A best practice is to build an ecosystem of security products and platforms that are designed to integrate with each other and can also provide insights across a variety of platforms. Partner with technology vendors who collaborate and share information across the security industry. Some of these tools combine data insights with human intelligence from security analysts, researchers and threat hunters to further enhance your ability and speed to assess and prioritise events.

Microsoft's approach to infrastructure security

Safeguarding your infrastructure involves gaining deep visibility into security health. Today's cloud and hybrid environments require policies that offer IT and network security that can rapidly detect deviations and quickly respond to signs of infrastructure compromise.

[Learn more](#) 

Key takeaways:

- The lack of integration between security products makes it difficult for security teams to see threats holistically.
- Security leaders should look for products designed to integrate with others and partner with companies that actively seek collaboration with the rest of the industry.

Section 2

Lack of security talent

More than 60% of organisations report having too few information security professionals, and by 2022 this shortfall is expected to reach 1.8 million.³

Realistically, your organisation is not going to be able to hire enough resources to meet the demands your security needs require.

Confronted with this widening gap, some organisations invest in additional security technologies to supplement the tools they've already deployed. This often increases the number of reports, alerts and dashboards that staff must examine, further burdening the already limited resources within an organisation.

There are several effective and realistic approaches that can help. Many organisations are turning to automation. Automated, software-based processes can continuously monitor your environment and take action in response to events according to

policies you have outlined. Modern solutions also use behavioural analytics to learn about your organisation, develop baselines and send relevant alerts when abnormal activities are detected. Some of these solutions will handle events automatically, as well as flag events that require human intervention, to help ensure that your security resources are only focused on the most critical and relevant alerts.

Another approach is to leverage the security expertise of a large-scale cloud provider.

Enterprise-level cloud providers have a greater footprint from which they can gather and analyse threat intelligence. Their scale, resources and investments in defending their platform and their customers give them capabilities and security intelligence that few companies can match. The cloud can also be leveraged for greater efficiencies when analysing security data and providing insights.

The Cyber Defence Operations Centre: How Microsoft defends its platform

The Microsoft Cyber Defence Operations Centre (CDOC) brings together security response experts from across the company to help protect, detect, and respond 24/7 to security threats against our infrastructure and services in real time.

The Microsoft Cloud:

- **Over \$15 billion (USD)** invested on cloud infrastructure
- **More than 200 cloud services**, including Bing, Outlook, Office 365, OneDrive, Skype, Xbox Live and Microsoft Azure
- A globally distributed cloud infrastructure—exceeding **100 datacentres with more than a million physical servers**—and connected through one of the world's three largest networks
- **More than \$1 billion (USD)** invested each year on security

Learn more 





Microsoft Intelligent Security Graph: By the numbers

**400
billion**

emails scanned for
phishing and malware

**450
billion**

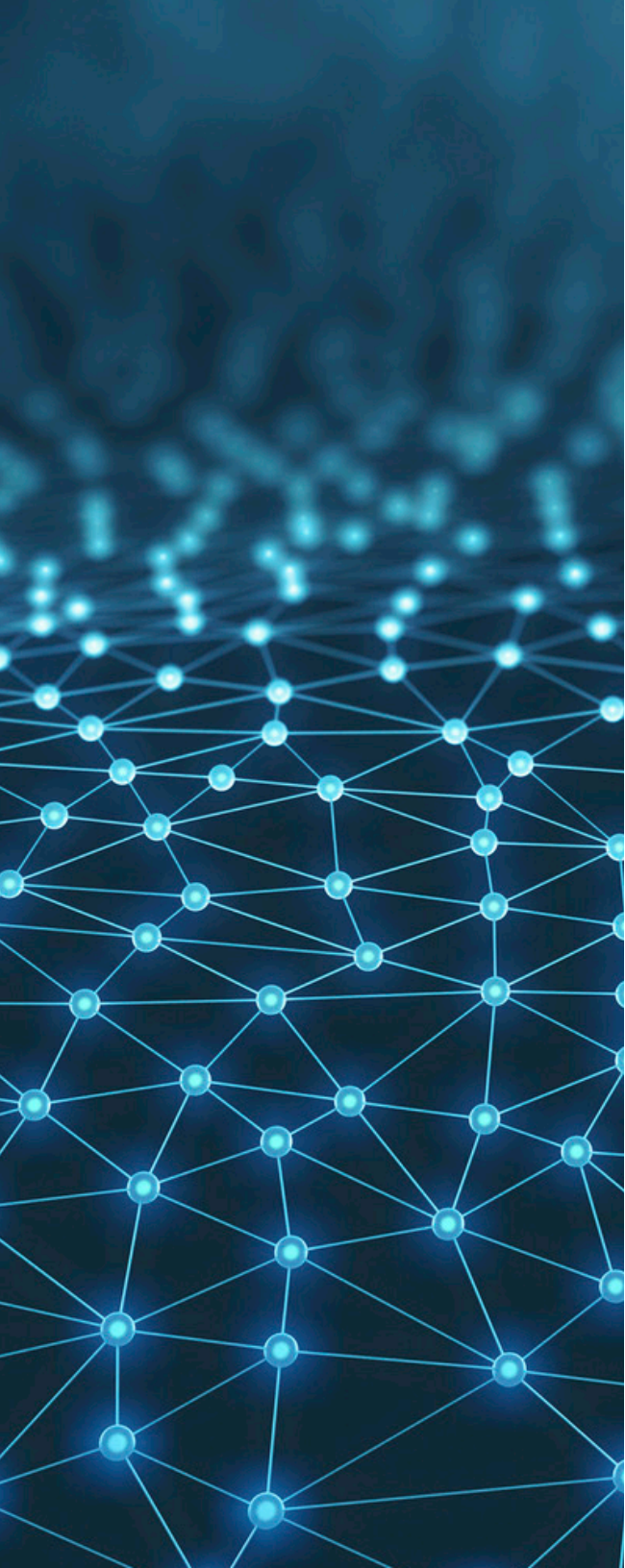
authentications
processed every month

**1
billion**

Windows devices updated⁴

**18+
billion**

Bing webpage
scans per month⁵



Finally, organisations should focus on increasing training and building a security-aware culture across the organisation. A number of industry organisations can provide training for your organisation to foster internal talent to become strong cybersecurity professionals. Cybersecurity is a shared responsibility, and all employees should be considered the front line of defence for your organisation. Focus on training that raises awareness about the tactics, techniques and procedures that threat actors use, as well as internal policies governing the use of external software, devices and data sharing across the organisation.

Microsoft's approach to identity protection and application security

Lessen the burden on your security team by preventing identity compromise and managing cloud applications. Protect data through tools that automatically detect unauthorised access and quickly respond by blocking apps and users.

Learn more about [identity protection](#) and [data security](#).



Key takeaways

- By 2022, the shortfall of security personnel is expected to reach 1.8 million.⁶
- Use automated, software-based processes that analyse and respond in real time.
- Leverage the security expertise of a large-scale cloud provider.
- It is important to invest in training internal security talent as well as building a security-aware culture among employees.

Section 3

Growing numbers of endpoints

Organisations no longer operate within a perimeter of highly controlled, corporate-issued devices. Employees now expect to work anywhere, on any device, and across any platform, whether sanctioned by IT or not.

The approach to overcome this issue is an identity-driven security strategy. Identity transcends devices and enables companies to apply controls based on organisational role and need, regardless of how a user may be connecting. By focusing on appropriately authenticating and managing users trying to access corporate assets, organisations can protect data regardless of where it's stored, how it's accessed or who it's shared with.

Identity and access management (IAM) solutions, as well as mobile application management with data loss prevention (DLP) solutions, can help to reduce risk by protecting access to applications and data in corporate resources and in the cloud. IAM can eliminate the need for multiple credentials by giving employees a single identity to access cloud and on-premises resources. Cloud-based IAM systems can also leverage threat intelligence and analysis from the technology provider to

better detect abnormal logon behaviour and automatically respond appropriately.

Multi-factor authentication (MFA) offers another layer of protection, requiring that a user present something they know (their password), and something they have (secondary authentication using their device, fingerprint or facial recognition). Other advanced tactics include using conditional access—policies that are based upon user risk, device risk, application risk and even location risk. These capabilities can automatically allow, block or require MFA of a user in real time, based on the policies you set. With conditional access policies, organisations can increase protection at their front door.

Modern tools provide endpoint security pre-breach. The best solutions help encrypt devices at all levels from the hardware to the applications, as well as give you enterprise-wide visibility into attack dynamics. More advanced tools also provide a post-breach layer of protection that gives **you** insight into adversary techniques and similarity to known attacks with built-in tools to quickly block, quarantine or wipe company data.



Microsoft's approach to identity protection and device security

Prevent identity compromise and go beyond passwords. Help protect against identity compromise with conditional access and multi-factor authentication while you automatically identify potential breaches before they cause damage. Also, expand your device controls and utilise encryption to protect company and personal devices. Support personal devices throughout your organisation with endpoint security strategies that detect suspicious activity and quickly respond to attacks.

Learn more about [identity protection](#) and [device security](#).



Key takeaways

- 60% of breaches stem from a compromised endpoint.⁸
- An identity-driven security strategy turns focus from tracking an ever-growing number of endpoints to managing users accessing corporate data.
- More advanced endpoint protection provides post-breach insight into adversary techniques.



60%
of all breaches
still originate at an endpoint
through compromised credentials.⁷

Section 4

Speed and agility of threat actors

Hackers know that there are multiple entry points to breach your organisation.

A sophisticated cyberattack will employ a variety of effective tools and tactics: phishing scams, malware and spyware attacks, browser and software exploits, access through lost and stolen devices and social engineering. To maintain visibility across the threats you know, and to become aware of emerging vulnerabilities, takes constant vigilance.

The average large organisation has to sift through

17,000
malware alerts
each week.⁹

While there are certainly tools to help maintain an always-on approach to security, the reality is that security demands a multifaceted approach to ensure your organisation is prepared to handle new attacks no matter when they occur or where they come from.

Traditional security tools have largely been focused on prevention. However, the sophistication and scale of advanced persistent threats means that while preventing a breach is ideal and a critical part of operations, it is no longer realistic to only focus on protection.

Given today's threat landscape, organisations need to assume that a breach has either already occurred or that it is only a matter of time until it will. As a result, looking for ways to significantly reduce the time to detect and recover from a breach has become more crucial.

Many security applications have built-in analytics and machine learning capabilities that produce insights about incidents, activities and steps attackers took. However, this can still be a look backwards into the past and doesn't always help to speed up reaction and recovery. More advanced security and analytics solutions leverage the insights to automatically take appropriate prevention and





response actions, helping to significantly reduce the time to mitigation. Tremendous breadth and depth of signal and intelligence are behind these solutions, and when combined with the experience and knowledge of human experts, these solutions can prove to be powerful tools against fast-moving threat actors.

Security leaders should focus efforts on working with the C-suite and the board to understand and maintain an acceptable level of risk and to balance it with the available budget for investments in security. Each organisation is different, and there's no "one size fits all" solution. Taking a risk management approach to security will not only help you decide where and how to invest, but also where not to invest, all in the context of what's most appropriate for your organisation.

Microsoft's approach to security intelligence

You can fight back threat actors with the power of security intelligence and analytics that detect threats before they do damage and automatically respond. However, real cyber threat intelligence requires more data than most organisations can acquire or process. You can rely on an unparalleled body of threat intelligence created from the vast sources that Microsoft analyses—over 450 billion authentications processed per month, 400 billion emails scanned for malware and phishing and one billion Windows devices updated.

Learn more [!\[\]\(d66ff64371a51729ac8c1cdaa685ba6f_img.jpg\)](#)

Key takeaways

- Adopt an "assume breach" approach to your security.
- Focus on reducing the time it takes to detect and recover from a breach.
- Take a risk management approach to security to help decide where to invest.



Section 5

Moving to the cloud securely

Moving to the cloud is a journey, and every organisation is at a different stage of this journey. Compliance requirements, local regulations or other migration challenges mean that not every organisation is ready to move critical workloads to the cloud.

However, moving to the cloud does not have to be a departure from your existing systems and processes. In a fully integrated hybrid IT environment, the cloud becomes an extension of your datacentre and the policies through which you control it.

Hybrid cloud strategies also offer security leaders a measured approach to moving to the cloud, allowing them to move business functions to the cloud only when they are confident that the service offers the right amount of control.

Different cloud service models affect the ways that responsibilities are shared between cloud service providers and their customers. This raises new issues for CISOs as they navigate the challenges of relinquishing some of the controls of an on-premises solution for the greater security that a cloud vendor can provide.

"Public cloud providers offer better security than a small business or even a big enterprise is able to achieve. This is due to the investments that cloud providers are making to build and maintain their cloud infrastructure."¹⁰

Security is a shared responsibility. While the cloud provider needs to provide state-of-the-art security and encryption, you as their customer must ensure that the services you're purchasing are in fact secure and you're extending required security policies into your cloud resources. When planning, look for vendors that are transparent and

publish detailed information about the security, privacy and compliance of their cloud services. In addition to this, a good cloud service provider should also produce audit reports and other materials to help you verify that their statements are in fact valid and understand where their responsibilities end and yours begin.

Questions to Ask Your Cloud Provider

When you select a cloud provider, you're not just choosing a service; you're entrusting them with your most precious commodity. Make sure to ask the important questions about security and access control, such as:

- Is your data protected by strong security and state-of-the-art technology?
- Do you incorporate privacy by design and allow control of our data in our enterprise cloud?
- Do you make deep investments in robust and innovative compliance processes to help my organisation meet its compliance needs?
- Will you tell me where my data is stored, who has access to it and why?
- Does the cloud service provider subject itself to yearly reviews from third parties?
- Will the cloud service provider reject any requests for the disclosure of customers' personal data that are not legally binding?
- Does the cloud service provider adhere to the compliance and regulatory standards of different countries and locations?

	SaaS	PaaS	IaaS	On-Prem
Data Governance and Rights Management	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)
Client End-points	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)
Account and Access Management	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)
Identity and Directory Infrastructure	Customer or Microsoft manages	Customer or Microsoft manages	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)
Application	Microsoft manages	Customer or Microsoft manages	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)
Network Controls	Microsoft manages	Customer or Microsoft manages	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)
Operating System	Microsoft manages	Microsoft manages	Customer manages (shared responsibility to protect)	Customer manages (shared responsibility to protect)
Physical Hosts	Microsoft manages	Microsoft manages	Microsoft manages	Customer manages (shared responsibility to protect)
Physical Network	Microsoft manages	Microsoft manages	Microsoft manages	Customer manages (shared responsibility to protect)
Physical Datacentre	Microsoft manages	Microsoft manages	Microsoft manages	Customer manages (shared responsibility to protect)
Security	Microsoft manages	Microsoft manages	Microsoft manages	Customer manages (shared responsibility to protect)
Privacy and Control	Microsoft manages	Microsoft manages	Microsoft manages	Customer manages (shared responsibility to protect)
Compliance	Microsoft manages	Microsoft manages	Microsoft manages	Customer manages (shared responsibility to protect)
Transparency	Microsoft manages	Microsoft manages	Microsoft manages	Customer manages (shared responsibility to protect)
Reliability / Availability	Microsoft manages	Microsoft manages	Microsoft manages	Customer manages (shared responsibility to protect)



The Trusted Cloud

Businesses and users are only going to use technology if they can trust it. You can move to the cloud securely when you're armed with the knowledge from your cloud provider on their security, privacy, compliance and transparency. The Microsoft Cloud is built on these four foundational principles, and the Trusted Cloud Initiative drives a set of guidelines, requirements and processes for delivering rigorous levels of engineering, legal and compliance support for our cloud services.

[Learn more at the Microsoft Trust Centre](#) 

Key takeaways

- Moving to the cloud does not have to mean a departure from existing systems and processes.
- A hybrid cloud offers organisations a measured approach to migrating to the cloud.
- When evaluating cloud service providers, consider the international standards they adhere to.
- Look for vendors that publish detailed information about how they operate their services and handle data.

Section 6

Risks of shadow IT

Even if your organisation doesn't use cloud-based solutions, chances are your employees do.

Only 8% of companies know the scope of shadow IT in their organisations,¹² and the number of cloud services used by corporate employees is rapidly outpacing internal IT estimates.

"By 2022, a third of successful attacks experienced by enterprises will be on their shadow IT resources."¹³

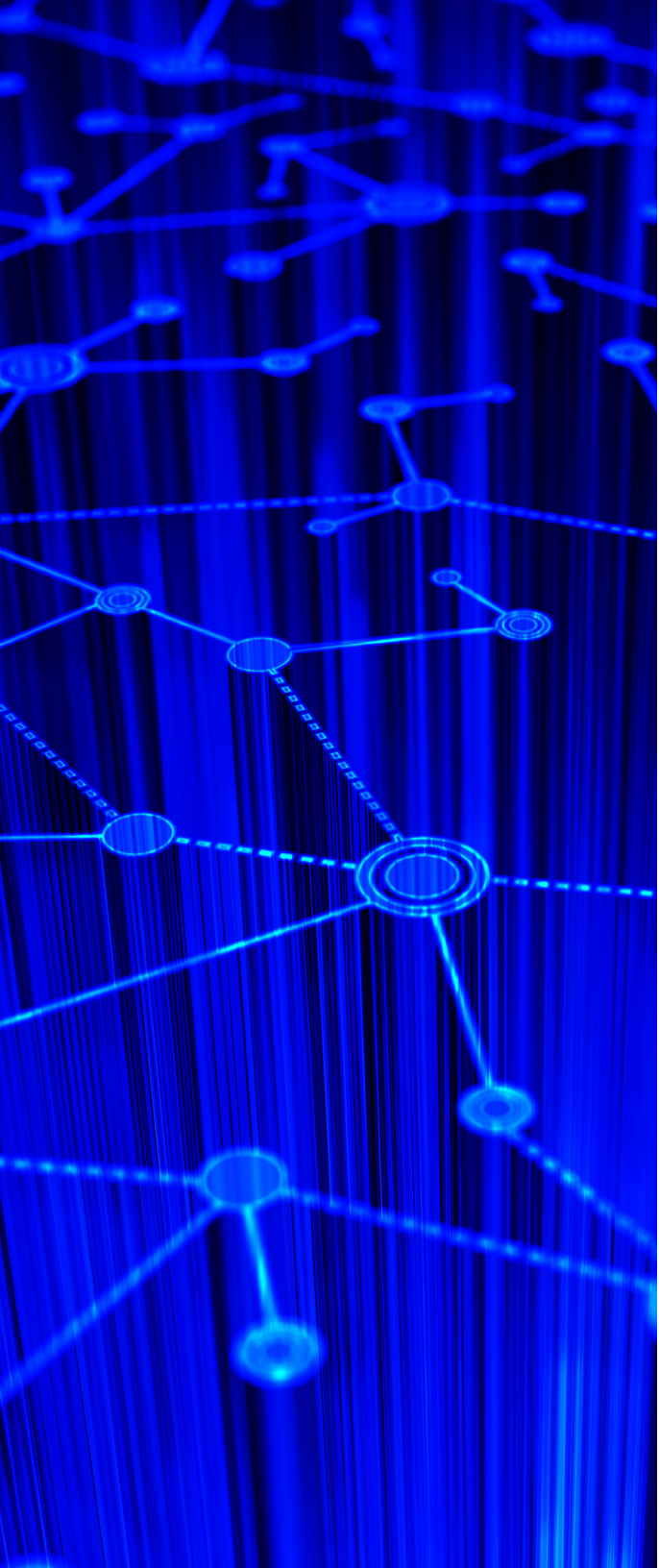
- Gartner's Top 10 Security Predictions 2016

This trend, called shadow IT, creates challenges for organisations in IT and application management, security and compliance. Not knowing what applications your employees are using and where sensitive data might be going introduces tremendous risk into your organisation. End users often accept applications' terms and conditions without reading

them and without a full understanding of what they are granting access to. Traditional network security solutions are simply not designed to protect data in SaaS apps and cannot give IT visibility into how employees are using the cloud.

Blocking shadow IT is not the solution. Employees will always find ways around restrictions. If control is too rigid, it deters innovation, conflicts with unplanned and demanding technology requirements, stifles productivity and can have a negative impact on your organisation's ability to keep high-calibre talent engaged.

The reality is that shadow IT is the new normal of modern enterprises. Allowing end users and teams to use the cloud applications that are best suited for their type of work helps drive productivity and innovation. Gaining visibility of shadow SaaS apps, controlling them and protecting them from threats are the first steps in managing risk and facilitating the digital transformation that has already started at your company.



Cloud access security brokers (CASBs) provide organisations with a detailed picture of how their employees are using the cloud:

- Which cloud apps are employees using?
- How risky are these apps for the organisation?
- How are these applications being accessed?
- What sort of data is being sent to and shared from these applications?
- What does the upload/download traffic look like?
- Are there any anomalies in user behaviour such as impossible travel, failed logon attempts or suspicious IPs?

With better visibility and control over the cloud apps and services being used by employees, security leaders can develop and enforce a reasonable and effective SaaS policy without sacrificing the security and compliance the organisation demands.

Microsoft's approach to application and data security

Your organisation can use cloud applications without putting corporate information at risk. Identify cloud application use, assess risk levels, develop policies and take appropriate action to protect your organisation and minimise risk.

[Learn more](#) 

Key takeaways

- Rather than blocking shadow IT, look for solutions that allow you to monitor and assess risk.
- CASBs can give you a detailed picture of how employees are using the cloud.
- With better visibility, you can then set policies that track and control how employees use these apps.



Section 7

Balancing end-to-end information protection and productivity

More than ever before, data is travelling outside your control—it's being shared by co-workers, as well as with partners and customers. While this helps to drive productivity and innovation, it can result in significant consequences if highly sensitive data gets into the wrong hands.

Security leaders are needing to manage and secure data stored in increasingly more locations and shared across boundaries. Global organisations doing business in the EU are especially prioritising data protection as the General Data Protection Regulation (GDPR) is set to begin being enforced in May 2018. GDPR is going to have significant implications on

how companies store and manage customer data, report breaches, communicate policies and invest in internal resources.

Employees will tolerate a certain level of inconvenience before finding workarounds to security requirements. Focusing on security at the data level can enable productive use and sharing of information to get work done while providing protection end to end. Common ways of protecting data against leakage are data classification and encryption.

Look for ways to classify and label data at the time of creation. Expecting employees to always know exactly what data needs protecting and always remember to classify can introduce errors and delays. Instead, your solution should take human error out of the equation and automate data classification. Tools that are available today can understand the context of data, such as credit card numbers within a file, or the sensitivity of data based on data origination. Once labelled, actions such as visual markings (headers, footers and watermarks) and protection (encryption, authentication and use rights) can be applied to sensitive data.

Security teams should also be able to track activity on highly confidential or high business impact shared files and revoke access if needed. This persistent protection travels with the data and ensures it is protected at all times—regardless of where it's stored or who it's shared with.

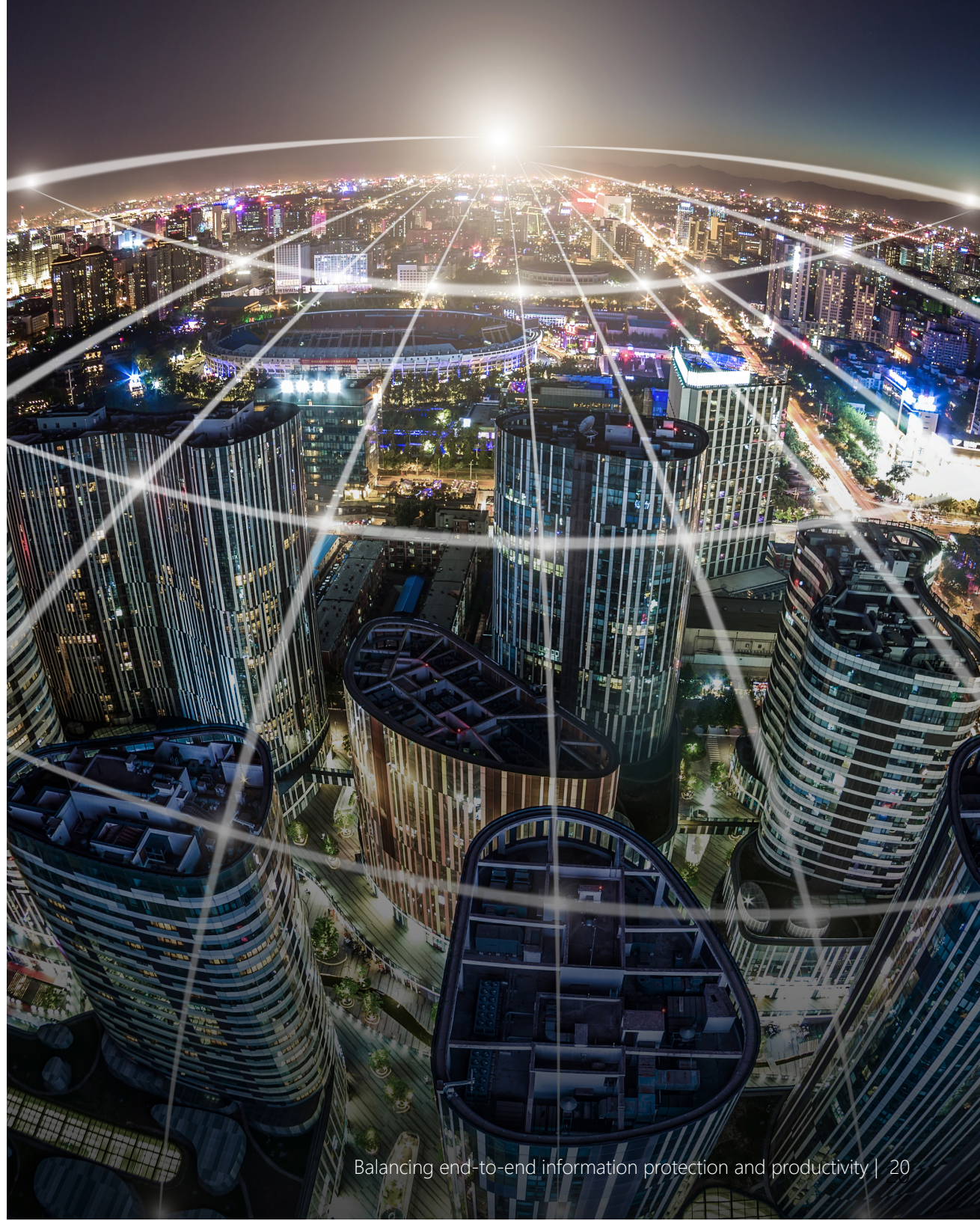
Microsoft's approach to information protection

Protect against data leaks and accidental mishandling by utilising rights management, and contain, classify and encrypt data. Enable security by not interfering with the employee experience. Information protection can start on the device—whether it's corporate owned or personal, and extend beyond it through email and into the cloud.

[Learn more](#) 

Key takeaways

- Security leaders need to focus on security at the data level.
- Data classification and encryption are becoming increasingly important.
- Classification and labelling of data should occur at the time of creation, and security teams should be able to monitor activities on files and take rapid action.



"We have to reconsider how we're going to protect data in this mobile-first, cloud-first world. The reality is, nobody has the expertise, the time and the resources to do this on their own."

- Brad Anderson,
Microsoft Corporate Vice President
for Enterprise Mobility

Conclusion

The multifaceted nature of modern cybersecurity means that it's no longer sufficient to solve just some of the security challenges your organisation faces.

While security leaders continue to seek solutions that help them better protect critical endpoints, detect the early signs of a breach and respond before it can cause damage, there is an urgent need for those solutions to now integrate and provide a holistic approach to cybersecurity.

This holistic approach will also require organisations to address the persistent nature of advanced cyber threats with an equally persistent, always-on defence.

It's vital for security solutions to address the realities of modern cybersecurity. Without this as a guiding principle, the solution you deploy to address one aspect of your security stack may well create a vulnerability in another.

Every company has security needs that are unique to their organisation. However, we all face the same security challenges and share the same responsibility to ensure that our organisations are protected.

For more information about how Microsoft can help with your holistic cybersecurity, please visit

Microsoft Secure 

References

- 1 According to Balaji Yelamanchili, executive vice president and general manager of Enterprise Security Business, Symantec, as quoted in:
Symantec. "Symantec Introduces New Era of Advanced Threat Protection." 27th October, 2015.
https://www.symantec.com/en/in/about/newsroom/press-releases/2015/symantec_1027_01
- 2 "Threat Landscape: By the Numbers." FireEye. 2016.
<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/Infographic-mtrends2016.pdf>
- 3 Reed, Jason, Yiru Zhong, Lynn Terwoerds and Joyce Brocaglia. "The 2017 Global Information Security Workforce Study: Women in Cybersecurity." Frost & Sullivan. 2017.
<https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf>
- 4 Microsoft.
- 5 Anderson, Brad. "Secure and Manage your Digital Transformation." Microsoft. 2017.
<https://myignite.microsoft.com/videos/34952>
- 6 Ibid. Reed, 2017.
- 7 Johnson, Ann. "Top Five Security Threats Facing Your Business and How to Respond." Microsoft Secure Blog. 18th October, 2016.
<https://blogs.microsoft.com/microsoftsecure/2016/10/18/top-five-security-threats-facing-your-business-and-how-to-respond/>
- 8 Ibid. Johnson, 2016.
- 9 Ponemon Institute. "The Cost of Malware Containment." Sponsored by Damballa. 2015.
<http://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf>
- 10 Trotter, Paul. "Top Cloud Security Fears & How the C-Suite Is Tackling Them." 20th May, 2015.
<http://www.cio.com/article/2924390/cloud-security/top-cloud-security-fears-and-how-the-c-suite-is-tackling-them.html>
- 11 Microsoft.
- 12 "Cloud Adoption Practices & Priorities Survey Report." Cloud Security Alliance. January 2015.
https://downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf
- 13 Gartner, Smarter With Gartner "Gartner's Top 10 Security Predictions 2016." 15th June, 2016.
<http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/>

