Microsoft

Six Steps to Build a Holistic Security Strategy

This information is for you

if you are a chief information security officer or IT security lead who:

- Needs a quick, no-nonsense guide to overall security strategy.
- Wants to stay informed on the latest practices for security.

🕘 **Estimated reading time:** <9 minutes

Contents

Meeting the challenge

Securing data and systems is a top priority for organisations. But meeting this challenge gets more difficult every day as attacks grow more sophisticated, employees use a wider array of devices and applications and data flows into and out of your business in more ways. With the mass move to remote working, security becomes even more compromised.

Leaders have to balance these challenges with the need to collaborate, innovate and grow a business. You need a multifaceted security approach that constantly protects all endpoints, detects early signs of a breach and responds before damage occurs. And no matter how strong your defences are, preventive measures are no longer sufficient – you also need to adopt an 'assume breach' posture that includes detection and response measures.

Today's chief information security officers (CISOs) need agile security frameworks that enable digital transformation and are supported by holistic strategies embedded into technologies, processes and training programmes. While all of this is available for on-premises solutions, the truth is that a move to the cloud immediately improves security capabilities across your organisation.

> **This eBook shares the six best practices of CISOs who have made security the cornerstone of business success. These best practices apply to an on-premises scenario, but are infinitely easier to achieve in a cloud scenario.**

1. Use integrated security products to enable rapid response

75

Number of security products that the average large organisation uses.[1]

Threat actors have evolved from 'smash-and-grab' attacks that compromise systems in hopes of maintaining a persistent, long-term presence. Attackers now use a variety of vectors and an increasingly advanced array of tools and techniques: stealing credentials, installing malware that erases itself to avoid detection, modifying internal processes and rerouting network data, social engineering scams and even targeting employee mobile phones and home devices.

Organisations are deploying more and more security tools against these threats. While meant to address specific issues, these solutions rarely work together. Many use proprietary dashboards, consoles and logs. Difficulty of integration makes it hard to have an overarching view and prioritise threats quickly. It becomes an even greater challenge when dealing with both cloud and on-premises resources. As a result, attacks can go undetected for more than 140 days.[2]

[1] 'Symantec Introduces New Era of Advanced Threat Protection', Businesswire, October 2015.

[2] 'Threat Landscape: By the Numbers', Mandiant, A FireEye Company, 2016.

Try this

As rapid detection and response become more important, these best practices have emerged:

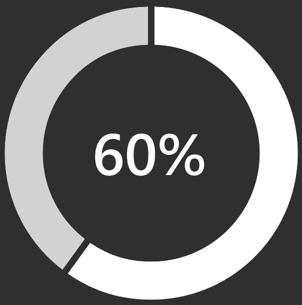
- Gain a holistic view of security for your entire network, including cloud and hybrid environments.
- Build an ecosystem of security products and platforms that integrate with each other and provide insights.
- Partner with technology vendors who collaborate and share information across the security industry.

Key takeaways

✓ The lack of integration among security products makes it hard for security teams to quickly see and combat threats holistically.

✓ Seek out products designed to integrate with others.

2. Manage access through identity, not endpoints



of breaches stem from a compromised endpoint.[3]

A data breach can have enormous costs. Establishing sufficient security controls to gain visibility into threats and attacks is one way to combat the high cost. But security teams also have to support consumerised IT, where employees no longer work exclusively on tightly controlled, corporate-issued devices and expect to work anywhere, on any device or any platform, regardless of whether it has been sanctioned by corporate IT.

In this world, identity-driven security strategies tie access to identity, not to devices. Apply controls based on role and need – no matter how the user connects. This focus on authenticating and managing users as they access corporate assets also lets organisations protect their data regardless of where it's stored, how it's accessed or with whom it's shared.

[3] 'Top Five Security Threats Facing Your Business and How To Respond', Microsoft Secure Blog, October 2016.

Try this

Shifting from a security strategy that's solely about endpoints gives you a more robust approach. These tools can help:

- **Identity and access management (IAM)** solutions and **mobile application management with data loss prevention (DLP)** solutions. Both help 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 use threat intelligence and analysis from the technology provider to better detect abnormal access attempts and automatically respond appropriately.
- **Multifactor authentication (MFA)** offers another layer of protection, requiring that a user present something they know (their password) and something they have (secondary authentication through a device, fingerprint or facial recognition). Other robust tactics include basing access on 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, essentially letting organizations increase protection at their own front door.

Key takeaways

✓ An identity-driven security strategy turns focus from tracking endpoints (devices) to managing users who are accessing corporate data.

✓ More robust endpoint protection provides post-breach insight into adversary techniques.

3. Adopt a zero trust model to defeat threats

17,000

malware alerts

The average large organisation has to sift through this each week.[4]

Hackers know that every organisation has multiple entry points. They use phishing scams, malware and spyware attacks, browser and software exploits, access through lost and stolen devices, social engineering and other tactics to breach your security. It takes constant vigilance to maintain visibility across the threats you already know – and to become aware of emerging vulnerabilities.

Some tools can help maintain an always-on security approach, but a broader approach makes more sense. Traditional tools focus on prevention, but that's no longer sufficient. Organisations must assume that a breach has either already occurred or that one will occur soon. This is known as zero trust. They then must find ways to significantly reduce the time required to detect and recover from the breach.

[4] 'The Cost of Malware Containment', Ponemon Institute, January, 2015.

Try this

Be an advanced security expert. Staying ahead of threats can mean looking back – to learn from past incidents, activities and steps that hackers took.

- Many security applications use built-in analytics and machine learning capabilities to analyse how a hacker gained access. More advanced security and analytics solutions will use those insights to automatically act to prevent and respond to similar breaches, which helps 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 be powerful tools against fast-moving threat actors.

Key takeaways

✓ Cloud-native applications support a zero trust model more easily than legacy applications.

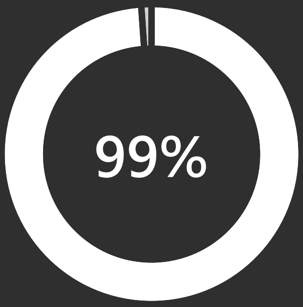
✓ Legacy applications require modernisation to support identity-based conditional access.

4. Move to the cloud securely

Every organisation is at a different stage of their journey to the cloud. Compliance requirements, local regulations and other migration challenges mean that not every organization is ready to move critical workloads to the cloud. Hybrid cloud strategies are one way organisations can ease into the cloud, keeping some workloads on-premises and moving others over.

Cloud service models affect how service providers and customers share responsibilities. This raises issues for CISOs as they navigate the challenges of relinquishing some of the controls of on-premises solutions for the greater security that cloud vendors can provide.

The rule of thumb for cloud security is that it's a shared responsibility. Cloud providers need to have state-of-the-art security and encryption, but customers must ensure that the services they purchase are in fact secure, and that they extend required security policies into their new cloud resources.



of cloud security failures will be the customer's fault through 2025.[5]

[5] 'Is the Cloud Secure', Gartner, October 2019.

Try this

Ask the right questions. Assessing cloud providers isn't just choosing a service, it's choosing who to trust with your data. Critical questions about security and access control that you should ask include:

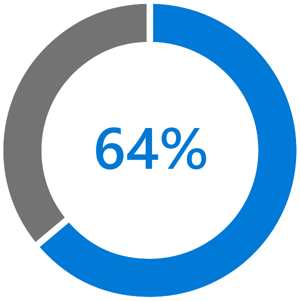
- Is our data protected by strong security and state-of-the-art technology?
- Do you incorporate privacy by design and allow control of our data in our enterprise cloud?
- What sort of investments have you made in robust and innovative compliance processes to help us meet our compliance needs?
- Where will our data be stored, who has access to it, and why?
- Do you conduct annual third-party reviews to ensure security and compliance standards are being met?
- Will you reject any requests for the disclosure of customers' personal data that are not legally binding?
- Do you adhere to the compliance and regulatory standards of different countries and locations, and if so, which?

Key takeaways

✓ **When evaluating cloud service providers, ensure that they adhere to international standards.**

✓ **Look for vendors that publish detailed information about how they operate their services and handle data.**

5. Get a good look at shadow IT



of employees have created at least one account (signing up for a work-related website or app) without involving the IT department.[6]

When an employee creates a cloud-based account without a business authorisation or awareness, this is known as shadow IT. The accounts seem quite harmless: a tool for correcting written grammar, for example. But these accounts create vulnerabilities even in the tightest of security set-ups.

People often accept terms and conditions without reading them and without fully understanding what they're granting access to. Traditional network security solutions aren't designed to protect data in SaaS apps and can't give IT visibility into how employees are using the cloud.

Ultimately, we don't want to suppress the motivations behind shadow IT. Allowing people and teams to use the cloud applications that are best suited for their type of work helps drive productivity and innovation. Gaining visibility, control and threat protection of shadow SaaS apps are the first steps in managing risk and facilitating the digital transformation that has already started at your company.

[6] 'New research reveals risks of shadow IT', 1password, February 2020.

Try this

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

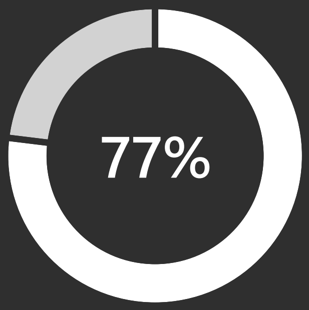
- Which cloud apps are employees using?
- What risk do these apps pose to the organisation?
- How are these applications being accessed?
- What sort of data is being sent to and shared from these applications?
- What does the upload/download traffic look like?
- Are there any anomalies in user behaviour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

Key takeaways

✓ Cloud access security brokers (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.

6. Make protection and productivity seamless



of CISOs say they feel caught between letting people work freely and keeping the enterprise safe.[7]

Data leaves your control now more than ever as your employees, partners and customers share it. This drives productivity and innovation, but it can have significant consequences if highly sensitive data falls into the wrong hands. Security leaders must manage and secure data stored in multiple locations and shared across international borders in compliance with regulations.

Employees will tolerate only so much inconvenience before finding security requirement workarounds. Classifying and encrypting are the best ways to keep data safe while still allowing productive use and sharing of information. You can sidestep human error by automating data classification. Tools 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, visual markings like headers, footers and watermarks, as well as protection such as encryption, authentication and use rights, can be automatically applied to sensitive data.

[7] 'IT security hindering productivity and innovation, survey shows', ComputerWeekly.com, October 2017.

Try this

Get comfortable with the details. Security teams should 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 protects it at all times – regardless of where it's stored or with whom it's shared.
- An identity access management system eases the burden of tracking highly confidential files.

Key takeaways

✓ Security at the data level is everyone's responsibility.

✓ Data classification and labelling should occur at the time of creation, and security teams should be able to monitor activities on files and take rapid action.

Conclusion

The multifaceted nature of cyberthreats means that only solving some of your security challenges is no longer sufficient. Every company's security needs are unique, but companies face the same challenges and share the same responsibility to protect their data, people and systems while encouraging innovation and growth. You need agile security frameworks that promote and support digital transformation, supported by holistic security strategies embedded into technologies, processes and training programmes.

If you haven't considered a move to the cloud, now is a great time to explore the increased security capabilities found there. Microsoft 365 offers a complete, intelligent solution for companies of all sizes that supports your digital transformation with security and compliance functionality built into every level.

Learn more in this free comprehensive webinar series.

Watch the series >