Whitepaper

Securing the cloud and endpoints

WITH secure | ONEMS

Introduction

The cloud has brought many transformative benefits to organizations. The flexibility to deploy services rapidly, without the need for any capital investment in infrastructure or lengthy implementations, has boosted agility and given less well-resourced organizations the chance to take on larger, better-funded competitors.

Yet the cloud also has a dark side. As organizations have opened up systems and processes to the wider networked world, they have become many times more vulnerable to malicious attackers. The complexity of most organizations' systems, and the potential points of entry, have grown exponentially – as has the prevalence of attacks. Furthermore, only a tiny minority have the resources to protect themselves effectively from the threats that are now part and parcel of being cloud-enabled.

Enlist the help you need to deliver the right outcomes

Despite the complexities of effective cloud security, rolling back the use of cloud is not the answer. Instead, organizations need to think differently about how they keep their risks to a minimum. The true cost of cloud ownership must include the cost of meeting the security challenges it presents – a fact that can be hard to appreciate until a breach occurs. Organizations should focus on outcomes, and in many cases the most cost-effective way to bring cloud security risks down to an acceptable level is to work with specialist providers that have the experience, skills and resources to understand your individual security priorities and ensure you have appropriate defenses in place.

WithSecure™ works with a range of specialist partners to help close the gaps in organizations' cloud security. Our expert partners variously supply, deploy, configure and – in the case of our Managed Security Service Provider partners - fully manage customers' cloud security, with the help of our state-of-the-art, modular cloud security technologies.

You can’t secure what you can’t see

The first major issue to address if you want to minimize cloud security risk levels is lack of visibility. The cloud has made it simple for anyone to access computing resources, storage and applications as and when they need them, but this flexibility has made it harder for organizations to track precisely what cloud resources are being used, how and where.

IT departments have long faced the challenge of ‘bring your own device’ (BYOD), but this is rapidly being eclipsed by ‘bring your own cloud’ (BYOC). Even before you account for SaaS applications, it can be very difficult to work out what cloud assets are deployed across an organization. Teams can spin up cloud instances containing sensitive data and systems with only a credit card. Some – although not all – of these instances can be difficult to see and track, and this can cause all kinds of dependency complications between known BYOC, corporate-approved cloud and invisible, ‘rogue’ BYOC.

The challenge of visibility is particularly significant in development environments, where cloud instances are easily spun up, production data deployed to them, and links into internal systems created – all with minimal oversight, documentation or security practices.

Aside from the challenge of poor visibility, wholesale, unstructured adoption of cloud also means that individual clouds owned by teams, departments or even single employees often lack consistent configuration.

Moving security management to the cloud can go a long way[1] to improving visibility but you may also need additional tools. For example, a cloud access security broker (CASB) is a means to track who is accessing which cloud services and where. Gartner defines CASB as “on-premises or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed”.

However, CASBs can be complex to set up and manage, covering a multitude of policies including authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and more. CASBs also require access to endpoints to install agents. As a result, many organizations without the in-house expertises to implement CASB will prefer to work with third-party specialists.

1. https://www.withsecure.com/en/expertise/resources/the-benefits-of-moving-security-management-to-the-cloud

Ensure you have comprehensive protection for endpoints

Compromising a workstation, mobile device or server is the most common first step in any serious attack, so it's essential to defend against the threat from endpoints. Growing cloud use has massively expanded the attack surface, particularly given the fact that many organizations need to give employees, partners, customers and others access to cloud systems via endpoints the organization doesn't physically own or control.

There are various tools and technologies available to mitigate the risks posed by both managed and unmanaged endpoints. Precisely what combination of defenses will be most appropriate for your organization depends on your specific circumstances, priorities, levels of risk tolerance and desired security outcomes. Again, a specialist provider will be able to assess your needs effectively, explain your options and make appropriate recommendations.

To stop the bulk of threats automatically, you should deploy an endpoint protection platform (EPP). EPP is a bit like an enhanced antivirus solution that blocks both known threats and anything exhibiting signs of suspicious behavior – even blocking ransomware before it causes any damage.

However, EPPs won't catch everything, so for the most effective endpoint protection you should also consider some form of endpoint detection and response (EDR) or Managed Detection and Response (MDR) that can quickly pinpoint and alert admins to any suspicious behavior or indications of Advanced Persistent Threats (APTs) on endpoints.

EDR is also increasingly morphing into Extended Detection and Response (XDR), fully cloud-based solutions updated with the latest intelligence on threat characteristics – for example, via integration with the continually updated MITRE threat framework.

Indeed, the entire field of endpoint protection is evolving rapidly, so it makes sense to work with specialist providers who can future-proof your protection. For example, future solutions are likely to feature better integration with cloud control panel logs and advanced capabilities to detect when credentials are stolen from an endpoint.

Stay safe without stifling cloud collaboration

The use of cloud collaboration platforms like Microsoft 365 saw a huge step change in use during the Covid pandemic, and in future such platforms will only become more important. After two years where remote working became 'business as usual', many more organizations now accept there are considerable cost, productivity and staff satisfaction benefits to be had from allowing a greater number of employees to work remotely either some or all of the time.

However, as WithSecure's "red teamers" (security experts that attempt to infiltrate systems on an organization's behalf in order to expose any security weaknesses) can attest, collaboration and real-time communication platforms are often the most fruitful targets when it comes to bypassing an organization's defenses.

For example, email is still the largest attack vector. Over half – 51% [2] – of small- and medium-sized businesses have seen an attack in the past two years. This is down to the fact that many attackers now look for easy prey, regardless of company size or sector. Mass automated email attacks are cheap to carry out and have a high return on investment for the criminal.

Training your staff to be more aware of phishing attacks so that they know what to look for and are less likely to click on suspicious emails is part of the solution, but we all know this is not foolproof. The growing use of collaboration platforms during the pandemic led to a simultaneous growth in attackers successfully using phishing to infiltrate systems. The technique was used in 36% of all breaches, up from 25% in 2019. In addition, some 46% of malware is delivered via email and the same suspicious email links and malicious files are frequently shared via collaboration platforms.

However, the answer is not to make it more difficult for people to access data via collaboration platforms, even if that might be the simplest way to ensure security. Instead they must strike a balance where they can be confident they are protected from attack without stifling the considerable benefits remote collaboration brings. That means ensuring they have the capability to prevent people from taking unauthorized actions such as sharing confidential data in places they should not, and the visibility to trace unusual activity before any major damage occurs.

As the largest and most commonly used platform, Microsoft365 protection is where we have initially focused development of these capabilities with our WithSecure™ Elements Collaboration Protection. We're also enhancing our email protection solution to protect Sharepoint, OneDrive and Teams to offer full platform protection, as well as incorporating capabilities to detect if a user account has been compromised.

2. https://www.ibm.com/security/digital-assets/ cost-data-breach-report/#/

Conclusion

At WithSecure™, we believe more collaboration and openness is a good thing, as is empowering people to make decisions individually. The days of locking down systems to the detriment of employees' and your organization's agility are over. Today, you should be talking to your security provider about how they can help you develop an outcome-based approach to security based on a positive, devolved approach to securing the cloud.

Our partners are fully versed in the various tools and technologies we offer, and are best placed to advise you on the right solutions for your organization. And because our solutions are fully modular and cloud-based, they can tailor your security solutions to meet your precise needs.

3. https://withsecure.com/en/expertise/resources/the-future-of-corporate-cyber-security-is-all-in-one

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

WITH secure