The 7 Hidden Truths of Cloud Security

WITH secure

Contents

Introduction

For nearly two decades, cloud computing has offered – and delivered – a utopian dream. Organizations short on resources can tackle bigger, better-equipped and well-funded competitors, and those behemoths in turn enjoy the freedom and flexibility that cloud brings.

The dream has become everyday reality; now it's time to face some hard truths about what the cloud means for organizational security, and that starts with an understanding of how the underlying principles differ from what's gone before.

Of course, the cloud can mean many different things – from the Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) offerings that we all rely on but most end users are blissfully unaware of, to the Software-as-a-Service (SaaS) tools such as Microsoft 365 and Salesforce that many people use every day.

The thing that unites all these cloud flavors is the concept of shared responsibility for security: customers are on the hook for everything cloud providers exclude from their built-in security controls.

Only a tiny minority of organizations have the resources to protect themselves from the threats that now come as part and parcel of being cloud-enabled, and there's very little that can be easily done to change this. The true cost of owning (or renting) cloud includes meeting the security challenges that come with it; this is often hard to appreciate until a breach occurs.

Here, we present seven hidden truths about cloud security in 2022 and show how organizations are writing new rule books that restore the benefits of a cloud approach and an assurance that their clouds are helping, not hindering, their goals.

The benefits of cloud should outweigh the risks[1]. Taking an outcome-based approach to tackling this is the way forward.

> **"I can't think of more than one or two organizations that I could credibly say I would turn to for attack-detection in the cloud space. Pretty much all the significant capabilities we've seen organizations wielding are entirely in-house developed. That's fine when you're a Tier 1 bank, less so when you're the other 99.5%."**

Nick Jones,
Principal Security Consultant, WithSecure™

1. https://www.withsecure.com/en/expertise/resources/cloud-security-striking-the-balance

Hidden Truth 1

You can’t secure what you don’t see

W / T H
secure

Hidden Truth 1

You can’t secure what you don’t see

Ishan Singh-Levett
Director, Product Management

You can’t secure what you don’t see, and cloud visibility is a different twist on an outstanding challenge for IT departments: shadow IT. Bring Your Own Device (BYOD) is now joined – if not eclipsed – by BYOC (Bring Your Own Cloud).

One of the strengths of cloud is that anyone can buy their computing, storage or applications with minimal effort in easily digested chunks. This flexibility also makes it hard for IT departments and security teams – and thereby entire organizations – to track what cloud resources are being used, and where.

It’s very difficult to work out what cloud assets are deployed at an organization – even before SaaS applications are accounted for. 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. On-premises equivalents are easier to spot using agents and scans.

The challenge of visibility is 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. Of course, aside from the security and privacy issues, it’s also very likely that organizations are paying well over the odds for their cloud services.

Facing the truth

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. This feeds into our second and fifth truths: consistent and secure configuration and protecting the gaps.

A cloud access security broker (CASB) is a means to track and control which internal users access which cloud services and from where. These are powerful capabilities but they won’t reveal systems that are never accessed and potentially vulnerable, perhaps because they’ve been forgotten but never decommissioned. By contrast, WithSecureTM Attack Surface Management helps organizations discover, understand and secure their internet-facing systems against external threats, even those systems which nobody knew about.

Hidden Truth 2

Cloud misconfiguration is everywhere

W / T H
secure

Hidden Truth 2

Cloud misconfiguration is everywhere

Nick Jones
Principal Security Consultant

A combination of flexibility and public access means that secure configuration for cloud is both vital and difficult. Attackers don't need sophisticated skills or tooling if misconfiguration leaves organizations open to attack.

Cloud providers have made the process of securing an environment straightforward; it's a basic tenet of the products they sell. Getting a perfect configuration for a single account for a single workload is completely attainable for any IT department. The big cloud providers all have excellent documentation and tooling for identifying basic issues, built on years of experience.

The challenge is securing at scale across multiple accounts, hundreds of workloads, and multiple cloud providers. Given that organizations now typically run across three to five cloud providers[2] this is a common problem.

Tooling and services exist to make a start on securing multiple environments, but they also need to be configured to reflect one's desired security posture, adapted to constantly changing workloads. They must also be usable by the people charged with detecting breaches. This runs up against a problem familiar to WithSecure™, both from a consulting and a managed services perspective: organizations rarely lack the vision for these things, but the resources to realize that vision are often in short supply[3].

That said, plenty of teams can, and do, make this work, either by enforcing standard security policies across a small number of providers, or by devoting significant time to embracing the complexity that comes with flexibility[4]. Either way, tackling cloud configurations at scale is not for the faint-hearted, and requires close collaboration between security and the engineering teams building and maintaining the workloads.

2. https://www.cio.com/article/228677/it-governance-critical-as-cloud-adoption-soars-to-96-percent-in-2018.html

3. https://www.withsecure.com/en/expertise/resources/detect-to-respond

4. https://www.withsecure.com/en/expertise/resources/webinar-replay-cisos-step-up-on-cloud-and-cyber-priorities-for-2022

Some organizations – think top-tier global financial institutions – have the resources and expertise to build out massive in-house capabilities. But this is a tiny proportion of the organizations that use cloud.

Part of the problem is the sheer number of cloud users; while cloud providers are adept at supplying tools and guidance, as we've said before, it is impossible to reach down to customers with security guidance in anything but the broadest sense. Add the complication of multiple clouds and multiple configurations, and it's easy to see why the problem exists.

The creative license that cloud providers allow users is both significant and part of the cloud's appeal, and that presents a challenge to the security industry. There is no single diagnostic tool that will fix all of the security holes in an environment.

Further adding to the complexity is the issue that what is a misconfiguration in one environment is entirely correct in another, making misconfigurations hard to spot with automated tools. The answer is to take a more human approach to the problem; it is better to have a few skilled and adaptable individuals than a well-stocked chest of inflexible diagnostic tools.

Facing the truth

If the solution to this problem sounds familiar, then perhaps it is because specialist consulting businesses, incident response and MDR providers have been fixing problems such as this for on-premises IT for a very long time.

Cloud security comes with its own complications, but it's worth noting that many existing techniques are often readily adapted – if not already adjusted – to meet this challenge.

Advice from third parties such as WithSecure™'s cloud security consultants, as well as MDR services with cloud security posture management capabilities such as WithSecure™ Countercept, can address the gap between a cloud provider's security provisions and those of most end-user organizations.

Hidden Truth 3

Cloud has changed the game for everyone

W / T H
secure

Hidden Truth 3

Cloud has changed the game for everyone

Jennifer Howarth
Product Manager - Cloud

Identity-based attacks are on the rise as more and more organizations move to cloud and applications delivered as a service, commonly referred to as XaaS. Why? The attack surface is fundamentally different from what we've all become used to in the traditional on-premises IT environment, where endpoints[5] are the most obvious target for attackers and the best place for defenders to focus their attention.

Aside from IaaS, where the cloud is essentially used as an off-site data center to host VMs, cloud workloads simply don't expose an OS to attack. Concepts like exploits and attacker code execution are no longer relevant, nor are the defensive measures that have been honed over the years to counter them. Instead, attackers achieve their ends by calling the cloud API with legitimate credentials. From a defensive perspective, there's nothing inherently malicious about each API call on its own, but a sequence of calls unlike a user's normal operation, or unusual in the context of a particular workload, is cause for suspicion. This is where user and entity behavior analytics (UEBA) comes in.

UEBA builds a picture of what usually takes place in a particular workload, in a particular environment, linked to user identity wherever possible. This understanding of what is normal and what is anomalous was a useful detection aid in the on-premises world, but in the cloud it is the very foundation of an effective monitoring approach. It's important to note that the identity-based detection provided by UEBA covers more than just human beings. End users are a great place to start when monitoring SaaS, but for raw cloud services, system-to-system identities are just as important. Recent incidents addressed by WithSecure™'s Incident Response Team have revealed attackers pursuing machine credentials to wreak havoc, rather than end-user accounts.

Cloud brings new technologies and ways of working that defenders have had to adapt to understand and learn to defend[6]. Some attacks happen at the cloud management layer and don't require interaction with any traditional on-premises infrastructure, or anything resembling it. It is therefore essential that organizations build detection and response capability specifically for the cloud. WithSecure™'s Incident Response Team increasingly deals with cloud-only investigations, and we expect this to increase in the future.

5. https://www.withsecure.com/en/expertise/resources/detecting-attacks-in-the-cloud

6. https://www.withsecure.com/en/expertise/resources/how-the-cloud-has-changed-response

Facing the truth

Cloud security at present is a challenge. There is little-to-no threat intelligence, data can be hard to come by, the known volume and scale of attacks is still low, and those organizations that have been hit hard are often reluctant to talk. But there are several reasons to be positive.

Threat detection is adjusting. The correct strategic preparation and adjustment of existing functionality in cloud platforms also equips digital forensics and incident response (DFIR) practitioners to perform their tasks in cloud-based incidents.

Another ray of light is MITRE[8], which is actively working to pull more threat intelligence into its attack framework. Yet it remains the case that, in the short term at least, cyber security providers and practitioners are in experimental and research mode.

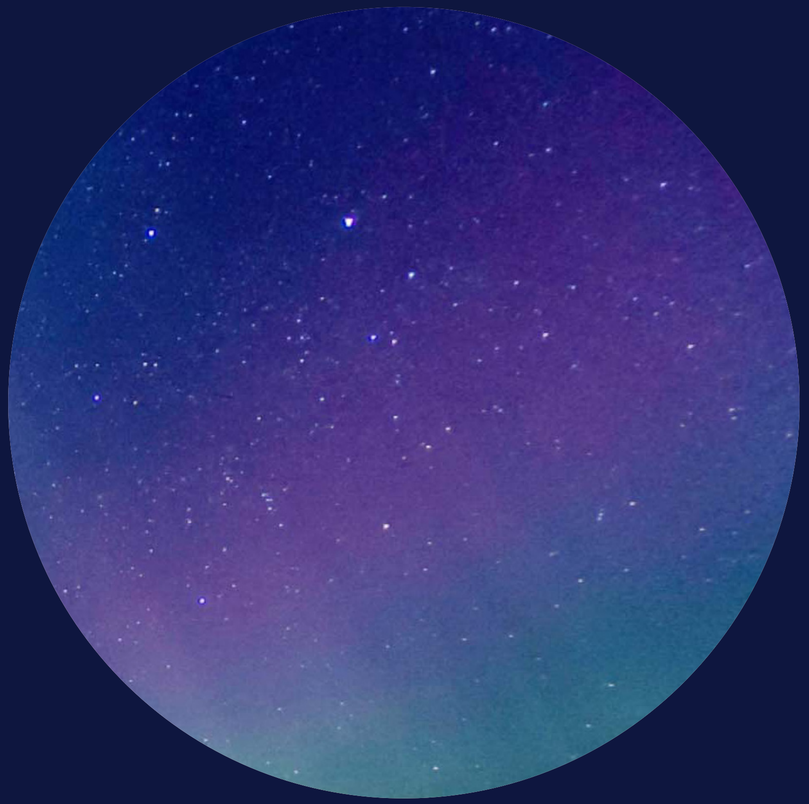
Find out more about how WithSecure™'s Incident Response Team conducts its work in the cloud: the correct strategic preparation and adjustment of existing functionality in cloud platforms[9].

8. https://attackevals.mitre-engenuity.org/enterprise/participants/f-secure/?adversary=carbanak_fin7

9. https://www.withsecure.com/en/expertise/resources/how-the-cloud-has-changed-response

Hidden Truth 4

Endpoints must still be defended



W / T H
secure

Hidden Truth 4

Endpoints must still be defended

Harri Ruusinen
Director, Global Sales Engineering

Even with UEBA in place, endpoints become entry points to the cloud. The attack surface has increased.

Despite mass adoption of cloud services, it's still the case that the computers and other devices you're using to access those services must be defended. This is where EDR continues to be useful in a cloud security scenario. But that's the starting point, and not where EDR's impact ends.

Cloud services are generally built with different levels of security. For example, multi-factor authentication (MFA) prevents attackers from accessing systems using stolen credentials. If the device that is using that service is compromised remotely, or physically stolen, the session could still be active, allowing an attacker to bypass that additional security control. A lack of MFA or encryption on endpoints is a problem: if an attacker has the right keys to gain access, the responsibility lands on the end-user organization, not the cloud provider. EDR, then, remains vital for devices used to access any organization's cloud service.

Facing the truth

We can’t afford to lose sight of bad actors once they’re in the cloud; so, we adapt. EDR is evolving into XDR (Extended Detection and Response) solutions to extend visibility and security to the cloud applications accessed from the endpoint as well. At WithSecure we are exploring enhancements that will help our customers keep pace with the growing security demands around cloud access.

When an endpoint is compromised, our EDR raises an alert before an attacker has time to move forward or laterally - for example into cloud environments. EDR gives excellent visibility into everything happening on an endpoint, allowing organizations to fortify their security posture and make it more difficult for attackers to move laterally across endpoints.

Cyber insurers and most businesses agree, EDR is essential for securing endpoints and keeping attackers out of the cloud. At WithSecure, we look forward to its evolution with more synergy between EPP/ EDR and cloud security, which will ensure our customers and partners maintain their resilience as they adopt new ways of working.

For more guidance on what to look for in a cloud-ready EDR set-up, read our guide for 10 things that should be on every EDR buyer’s wish list[10].

10. https://www.withsecure.com/en/expertise/resources/10-things-to-consider-before-buying-an-edr-solution

Hidden Truth 5

Split defenses result in weaknesses

W / T H
secure

Hidden Truth 5

Split defenses result in weaknesses

Domenico Gargano
Director, Technical Operations

It's incredibly difficult to only inhabit the cloud; every organization will have at least a small physical endpoint presence when it comes to IT. Splitting services and applications across on-premises and cloud increases the attack surface that attackers can aim at. More than one cloud? That's just multiplied the problem.

Identifying and plugging these security gaps is vital, of course – and it's also quite likely that your organization, intentionally or otherwise, is taking active steps that will address this challenge.

The 'shift left' approach of devolving responsibility for security to developers[11], and the recent trend towards chief information security officers (CISOs) emerging from under the wing of the IT department to become a cross-business leader, mean that more attention is being paid to the 'glue' between cloud services and applications.

So, why does this problem exist in the first place? For the same reason that software and OS vendors (and the rest of us) have had the same challenge with traditional on-premises IT since desktop computing became the dominant force in enterprise IT. Cloud providers have enormous security resources and the means to equip customers with some amazing tools and knowledge. But the service stops there. Cloud providers have no affordable way for these providers to reach down to each customer and tailor security for them without increasing the cost of cloud computing to a prohibitive level.

Cloud providers – at both the infrastructure and the application layers – operate at enormous scale, and they need to manage user expectations. An array of impressive security tools and configurators is the way forward, but they are only part of the puzzle when it comes to securing a cloud-enabled organization.

11. https://www.withsecure.com/en/expertise/resources/tech-not-culture-is-key-to-devsecops

Split defenses, split teams?

WithSecure™'s consultants have observed a significant number of organizations running separate security operations centers (SOCs) for their cloud estates. This practice has met with mixed success and often appears to go hand in hand with a second phenomenon: the continuing struggle to recruit and retain cloud security experts. This shortage is hardly news amid the multi-decade background noise of skills gaps across the IT sector.

The solution to this particular shortage is, however, quite different from most: cloud teams resort to building their own security capability, sometimes side-stepping the security organization entirely. In some cases, WithSecure™ cloud security consultants end up engaging more and more with the engineering side of companies as they tend to have a better understanding of what their cloud security looks like than the IT security team. The typical security organization is more fragmented than it was in the past.

If you don't have the right data sources, you're going to have an incomplete view of activity within the environment, and this makes it very difficult to identify meaningful anomalies or join the dots between different parts of your environment. This is good news for attackers.

It's important to be able to correlate data points across both on-premises infrastructure and that held in the cloud or clouds to build a full picture of what an attacker might be doing; this provides the best possible chance of detecting and responding to the threat.

WithSecure™'s investigation of activities involving the NOBELIUM threat actor have highlighted that group's ability to enter via an on-premises vector and then move from that to the cloud, maintaining persistence and taking its pick of the information that it needs.

Researchers at Microsoft published further details, revealing approaches NOBELIUM has used to steal credentials that ultimately allow them access to a target organization's active directory federation services (ADFS). From there, the attacker can access and persist in the cloud.[12]

WithSecure™ has replicated this approach in 'red team' exercises, finding that, even if defenders remove on-premises implants, the red team can maintain a presence in the client's cloud environments until the end of an engagement.

Sygnia has described how, once ADFS administration rights have been won, NOBELIUM then compromises the victim's security assertion markup language (SAML) certificate[13].

This 'golden SAML' attack effectively grants no-questions-asked access to services that trust tokens issued via SAML, granting persistence across both cloud services and XaaS.

CISA has further described[14] NOBELIUM's techniques, tactics and procedures (TTPs) in an alert.

Without the ability to correlate ADFS authentication logs against cloud activity logs, it was impossible for victims to spot users that had successfully accessed cloud environments without having to authenticate to the on-premises systems ADFS server that would grant access.

12. https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/

13. https://www.sygnia.co/golden-saml-advisory

14. https://www.cisa.gov/uscert/ncas/alerts/aa21-008a

Securing the build pipeline

This comes back to the silo issue touched on in the misconfiguration point. Infrastructure engineering and security teams don't always understand the context of logged activities, and that expertise from the teams responsible for supporting the pipelines and other development tooling will also be required. Misconfigurations caused by decentralized DevOps[15] have been the primary reason for cloud breaches that WithSecure™'s Incident Response Team has investigated over the last couple of years.

A few things become imperative, and they're detailed in the article referred to in the footnote above: first, capitalize on the benefits of DevOps and DevSecOps to push responsibility for security into the development cycle early on. The way to achieve harmony between development and security teams is for business functions to start paying for their own security. Second, it's vital to have strong lines of communication between the security team and cloud engineering.

Again, our Incident Response Team sees CISOs making this happen by operating independently of the IT department and security operations distributed down into individual business units. This isn't a case for independent, poorly connected silos, but for decentralized, highly connected teams.

The final aspect of this is that decentralization shouldn't result in vastly different risk appetites across the organization – and that calls for a new middle layer that can translate between the different units.

Unexpected weak points

Both consulting and incident response engagements that WithSecure™ has delivered have revealed that, outside of trivial misconfigurations, weak points are rarely internet-facing cloud assets. Instead, it's often the services, applications and tools that organizations use to establish clouds that prove to be problematic. These 'crown jewels' are more often identity providers, source code repositories, infrastructure code, and the tooling for deploying services into production.

Continuous integration / continuous delivery (CICD) tools such as Jenkins can and do wield enormous power and privilege in a cloud environment; if an attacker can gain access, the battle is already over.

Facing the truth

Cultural change is the key here, and in many organizations it's already underway, requiring only minor tweaks to steer it to a stronger cloud security posture.

Devolving responsibility and spending for security to business functions, with overall accountability held by a CISO independent of the IT team, can put an organization on the path towards a secure cloud footing.

15. https://www.withsecure.com/en/expertise/resources/security-team-of-the-future

Hidden Truth 6

No one knows who is responsible for data in the cloud

W / T H
secure

Hidden Truth 6

No one knows who is responsible for data in the cloud

Dmitriy Viktorov
Head of Product and Technology, Cloud Solutions

It’s a well-known expression that ‘data is the new oil’ – an extremely valuable asset for any organization. Therefore, moving your data into the cloud requires careful deliberation to ensure you maintain the proper control and visibility, and there are many things to think about.

When you buy cloud services you push some of the responsibility for data security onto the cloud provider, which is part of the appeal. But it's important to remember than it's still your responsibility to maintain security hygiene. This is known as the Shared Responsibility Model.

Once again, it’s an issue of visibility; in this case, visibility towards data. You need to be aware of what kind of data you have, how it’s classified, where the data comes from, who can access it, or where the data goes.

If data comes from external and untrusted sources (such as email), you need to block harmful and disallowed content before it reaches internal or external users.

In case of compliance requirements, you also need to monitor access to your sensitive data and have an audit trail, whether it’s the subject of a compliance requirement, and then who can access it.

One of the risks you need to think about is malicious insiders and unauthorized access to data. SaaS cloud services can easily become very complex, leading to misconfiguration or weak access controls, as described in Hidden Truth 2. In turn, misconfigurations can result in data breaches.

Another risk is that data can be accessed by other applications and services that are connected to SaaS cloud via APIs. If these are misconfigured or give more permissions than they should, they can also potentially be the source of a breach. Even if configured properly, it is important to consider that APIs themselves could be compromised, as we have seen in recent supply chain attacks.

Facing the truth

As the usage of SaaS cloud services such as Salesforce, Microsoft 365, Google Workspace and others increases, it makes them lucrative targets for attackers. We believe that future attacks will not always have stealing valuable data stored in the cloud as their end goal. Attackers will try to use cloud services as 'stepping stones' for getting into organizations' networks and attacking other internal and external systems. We have already seen examples of phishing and ransomware attacks conducted via cloud services. As the threat landscape changes, we at WithSecure™ will continue improving our solutions and extending detection and response capabilities across endpoint devices and IaaS, PaaS and SaaS cloud platforms.

One of our existing solutions, WithSecure™'s Cloud Protection for Salesforce[16] provides real-time protection from viruses, trojans and ransomware, and scanning all content shared via Salesforce cloud. WithSecure™'s unique solution compliments the security controls of Salesforce's cloud platform and fills a gap in the shared security responsibilities when it comes to customer data stored in the cloud. The solution helps customers using Salesforce's Sales, Service or Experience Cloud to prevent or disrupt attacks via malicious files or phishing URLs[17]. It also provides full visibility and analytics about content accessed by internal or external users.

WithSecure™ Cloud Protection for Salesforce leverages a cloud-based content reputation and threat analysis platform called WithSecure™ Security Cloud. At its core, the Security Cloud relies on multiple levels of top-notch technologies and a constantly-evolving repository of cyber intel and threat-related data gathered in real time from tens of millions of security sensors across the globe. It forms the cornerstone of our award-winning end-point protection products and other cloud collaboration protection solutions such as WithSecure™ Elements Collaboration Protection.

16. https://www.withsecure.com/en/expertise/resources/salesforce-data-security

17. https://withsecure.com/en/expertise/campaigns/disrupting-the-kill-chain-with-withsecure-cloud-protection-for-salesforce

Hidden Truth 7

Collaboration platforms will only become more important

W / T H
secure

Hidden Truth 7

Collaboration platforms will only become more important

Juha Högmander
Director, Technical Offering

Not many of us work from corporate offices today, and it's likely we won't in the future either. For many, remote working has been 'business as usual' for two years, and there's a good chance some of us will be working remotely permanently.

Collaboration has become super-relevant in these conditions and of course this means that protection is also crucial. You need a digitalized way to share materials, to have workshops and live meetings, and to give presentations. In other words, you need a way to communicate and collaborate. WithSecure™ 'red teaming' exercises have always found collaboration and real-time communication platforms a goldmine when attempting to infiltrate a client's environment.

A crucial part of this conversation is that email is still the largest attack vector. Over half – 51%[18] – of small- and medium-sized businesses have seen an attack in the past two years, which represents a change in the mentality of cyber criminals. Many attackers now look for easy prey, regardless of company size or sector, because 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. Phishing has utilized quarantine to pump up its frequency to being present in 36% of breaches, up from 25% in 2020[19]. Email link is the top malware vector in breaches, and approximately 46% of malware is delivered via email and not only that. The same suspicious email links and malicious files are shared in collaboration platforms.

We don't want to prevent people from accessing data, even if that would be the simplest way to ensure security. But we do want to prevent people from taking unauthorized actions such as sharing confidential data in places they should not, and we do want to have the visibility to trace unusual activity.

18. Ponemon. IBM. 2020. Cost of a Data Breach Report. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

19. Verizon. 2021. Data Breach Investigations Report 2021. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

20. Verizon. 2020. Data Breach Investigations Report 2020 https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

Facing the truth

Microsoft 365 offers a lot of this functionality and is by far the largest platform. That is why WithSecure™ prioritized developing its WithSecure™ Elements Collaboration Protection[21] solution, although other developments are in the pipeline and WithSecure™ Cloud Protection for Salesforce already offers collaboration protection to users in that environment.

We've been working on enhancing our email protection solution to protect Sharepoint, OneDrive and Teams so that we have full platform protection. We've also incorporated capability to detect if user account has been compromised,, which is important to the protection of the whole service.

Thinking about the world and how it currently is, we don't want to be the security guys that are fighting against the trend towards openness. The transformation within technology companies that has spread to the wider economy leans towards empowering people to make decisions individually.

21. https://www.youtube.com/watch?v=rvzXvtXoyF8&t=1s

Conclusion

The latest tools and procedures only go so far – for cloud providers, security vendors and customers alike. Far more effective is cultural change, and the right, outcome-based security approach can magnify the force of good tooling and technique a thousandfold.

Investing in creating a strong, devolved approach to securing cloud, just as you secure your own organization, will reduce the hidden cost overhead that cloud can represent.

Who We Are

WithSecure™ 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 & response is 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™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure