VECTRA®
SECURITY THAT THINKS

RESEARCH STUDY

Securing Microsoft Office 365 in the new normal:

Closing the gap between attackers and defenders

VECTRA
SECURITY THAT THINKS

Table of Contents

Forward

Microsoft Office 365 dominates the business productivity landscape today, and its place at the heart of enterprise operations was cemented by the need to adopt more flexible and agile working practices during the COVID-19 pandemic. As public cloud usage increases so does the attack surface that can be exploited by threat actors. Businesses must be sure that they can defend Microsoft Office 365 environments from criminals seeking to exploit its powerful capabilities in serious cyber attacks.

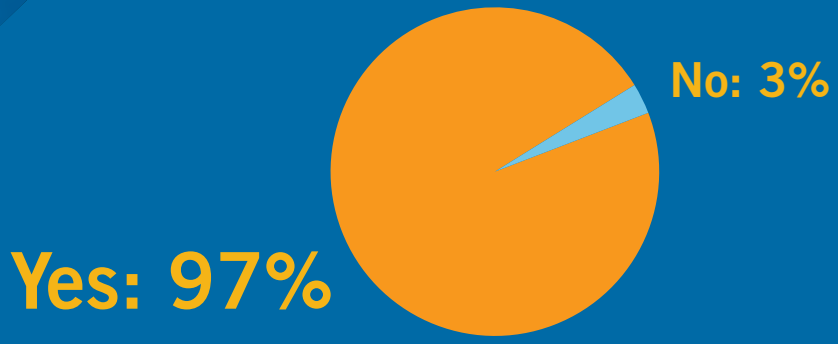
In this eBook you'll find fresh insight into this new and rapidly changing landscape. We surveyed 1,112 IT security decision makers around the world to gather their views about the biggest threats facing Microsoft Office 365 environments, and their ability to defend against them.

We'll also be sharing practical actions you can take to improve the security of your Microsoft Office 365 infrastructure and Azure AD, including how to identify and stop subtle and dangerous threats such as account takeover attacks that seek to use Microsoft Office 365 and other SaaS applications capabilities against you.

VECTRA
SECURITY THAT THINKS

Cloud usage soars during the pandemic

With cloud capabilities swiftly transitioning from strategic advantage to business necessity, cloud adoption and the efficiency and agility it delivers has been at the head of board discussions for several years now. However, it was not until 2020 that most enterprises really found the mettle of their cloud strategies being tested.



97% of IT security DMs interviewed have extended their use of Microsoft Office 365 as a result of the pandemic.

VECTRA
SECURITY THAT THINKS

As many businesses rapidly switch to remote operations, it is no surprise that we saw an almost unanimous increase in organisations extending their use of the ubiquitous Microsoft Office 365 for collaboration. As of March 2020, there were 258 million active users, an increase of more than 70 million from the previous year.

"We went from zero to 100 percent visibility into attacker behaviors with Vectra. We were amazed at what Vectra could see inside network traffic. We get context and details about every attack and know which ones are the most critical."

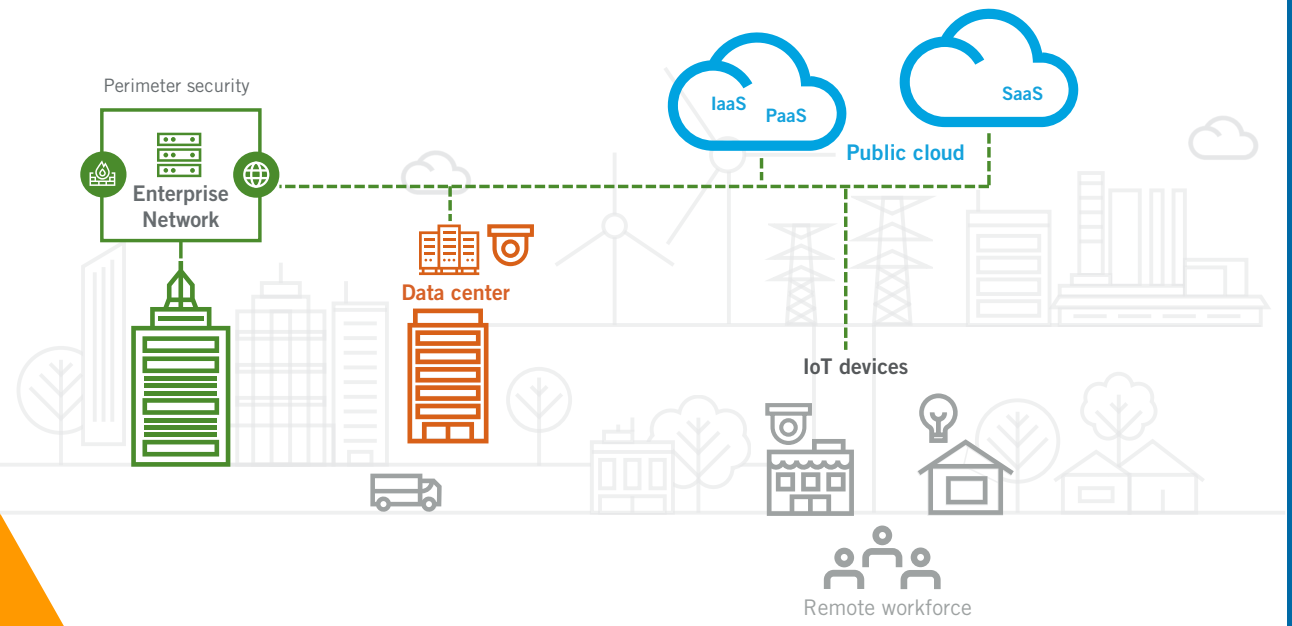
Head of security
Global financial services firm

This imposed shift has massively and permanently altered the IT landscape. When we surveyed IT decision makers around the world about the impact of this move to a decentralised workforce on their operations, almost every respondent told us they had accelerated their cloud and digital transformation strategies as a result, some by as much as two years.

The rapid shift in the IT landscape and forced acceleration of cloud migration has also left most organisations more vulnerable to cyber threats.

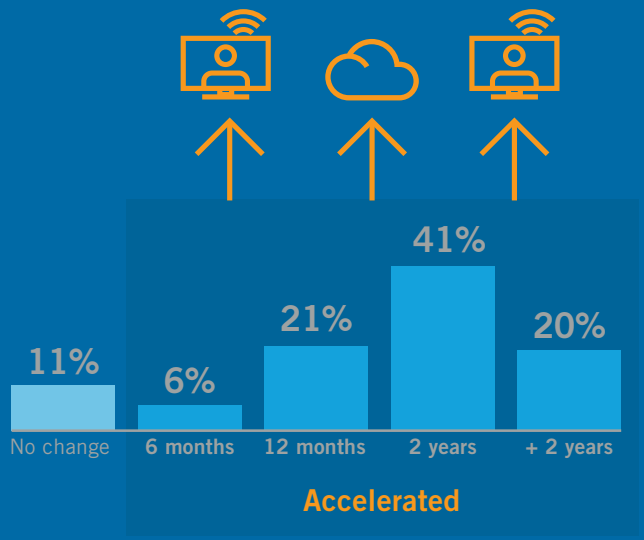
Although it was trial by fire given the circumstances, this accelerated adoption appears to have delivered tangible benefits during the pandemic. Most respondents cited improved productivity, job satisfaction and working hours – though some saw the reverse, most notably the healthcare sector.

However, the travails of global lockdowns have also seen a marked spike in stress levels across all business sectors. Aside from the impact on their personnel, the rapid shift in the IT landscape and forced acceleration of cloud migration has also left most organisations more vulnerable to cyber threats.



88%

have seen their company's move to the cloud and digital transformation **accelerate during the pandemic**, with 20% seeing an acceleration of more than 2 years.



VECTRA
SECURITY THAT THINKS

The rapidly changing threat landscape

Quickly pivoting into increased Microsoft Office 365 and Azure AD deployment has seen many enterprises creating an expanded attack surface and an isolated workforce that they may not be equipped to effectively monitor and protect. In this new norm, security professionals are catching up in understanding and securing their cloud environments, and the existing security tools and policies are often ill equipped to help. Adversaries were quick to capitalise on this and increase their attacks – even by April 2020 Google reported blocking more than 18 million COVID-themed phishing and malware emails globally every day.

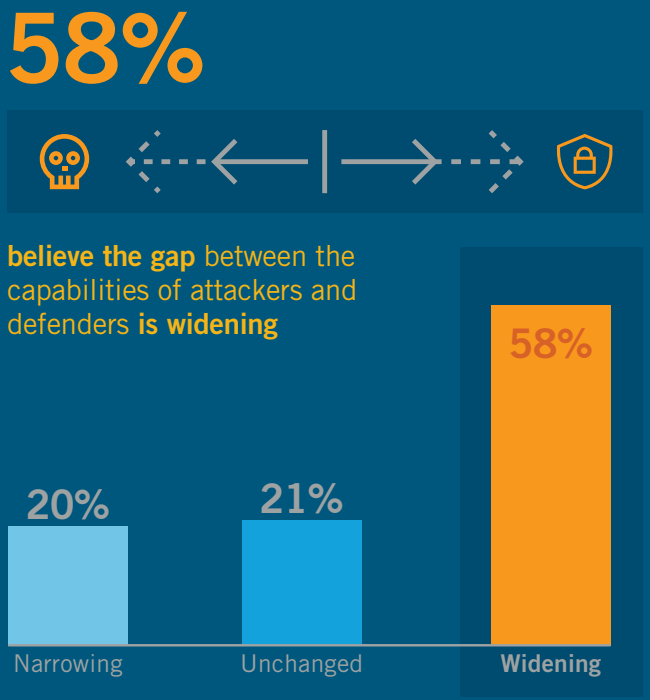
And while the prevalence of COVID-themed phishing attacks may have declined, the security vulnerabilities around burgeoning cloud deployments will linger on. Most security decision makers believed their organisation's security risk had increased over the last 12 months as a result of these factors.

Directors and C-level executives were markedly more likely to see a widening gap than those working at management level.

Attackers are also getting better and are applying their experience in navigating and exploiting this new terrain. We are seeing a shift from traditional malware-based attacks to those focusing on accounts, credentials, permissions, and roles – another area that traditional security tools are completely blind to detect.

With threat actors continuing to increase both the volume and sophistication of their attacks, there is a fairly pessimistic outlook among many security decision makers – almost three in five believe the gap between the capabilities of attackers is widening. Directors and C-level executives were markedly more likely to see a widening gap than those working at management level.

Most security decision makers believed their organisation's security risk had increased over the last 12 months as a result of these factors.



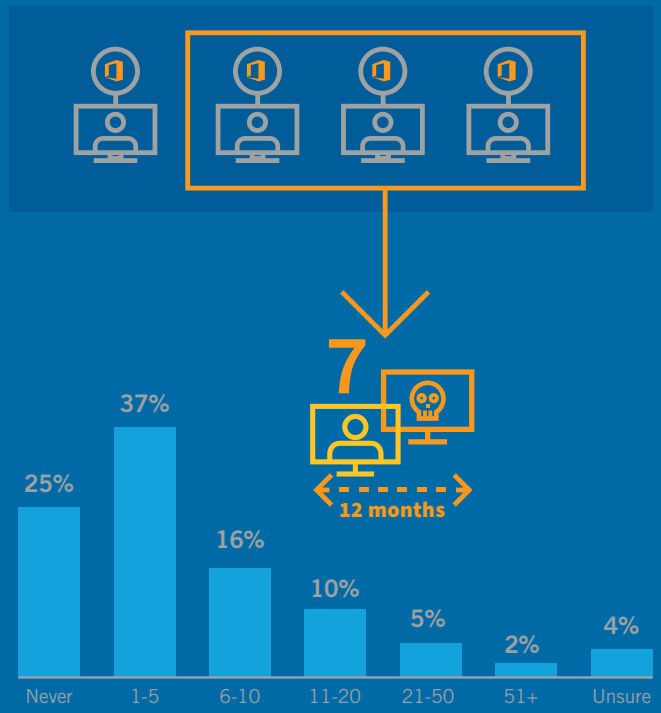
In fact, powerful developments around tools like network detection and response (NDR) and AI-powered analytics mean that the reverse should be true. Once attackers have infiltrated an environment, they have traditionally relied on their ability to hide in the noise of normal business operations. Careful adversaries can live off the land by exploiting legitimate business applications, including those built into the Microsoft O365 suite such as Power Automate and eDiscovery to move laterally, hide in HTTP, HTTPS and DNS traffic, and exfiltrate data. AI-powered NDR solutions that integrate with cloud applications and services are able to cut through this cover and rapidly identify the minute clues that an intruder is at work.

AI-powered NDR solutions that integrate with cloud applications and services are able to cut through this cover and rapidly identify the minute clues that an intruder is at work.

However, while this means that on paper the gap between attacker and defender is narrowing, this is only the case for organisations that have invested in these capabilities. For those that lack the power to detect the subtle signs of malicious activity, the gap will continue to widen as attackers take full advantage of their cloud infrastructure. While the increased use of the cloud is no surprise, we encounter surprising attitudes from security decision makers about the severity of the threat and their ability to manage it.

For those that lack the power to detect the subtle signs of malicious activity, the gap will continue to widen as attackers take full advantage of their cloud infrastructure.

71% of Microsoft Office 365 users have suffered an account takeover of a legitimate user's account on average **7 times in the last year**

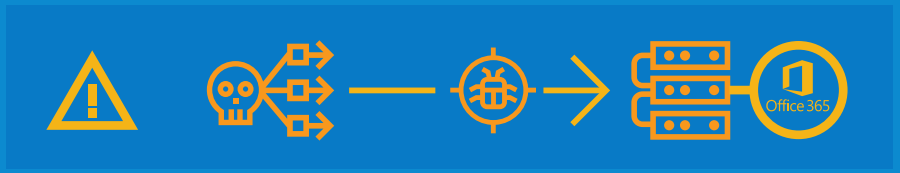


VECTRA
SECURITY THAT THINKS

Microsoft Office 365 is the leading security concern

Security decision makers have to stay prepared for several serious threats. We found ransomware was viewed as a significant issue, along with the increased risk of attacks exploiting various IoT devices as businesses expand their IT estates.

48%



share top concern to be the risk of compromise of data held in Microsoft Office 365

However, attacks targeting data held within Microsoft Office 365 emerged as the leading worry, and with good reason. Microsoft Office 365 often forms the heart of an enterprise's operations, facilitating almost all data storage and sharing as well as being the Identity Provider brokering access to a myriad of other SaaS applications. This makes any Microsoft Office 365 environment a valuable target for threat actors, and with more than 250 million monthly users, there is no shortage of targets. Our 2020 Spotlight Report on Microsoft Office 365, which involved the investigation of more than four million accounts, found 96 percent exhibited some sign of lateral movement.

Microsoft Office 365 often forms the heart of an enterprise's operations, facilitating almost all data storage and sharing as well as being the Identity Provider brokering access to a myriad of other SaaS applications.

Likewise, many respondents were also concerned about the ability for attackers to live off the land using legitimate Microsoft tools such as Power Automate and eDiscovery. Indeed, this was the main issue for respondents based in Singapore, as well as for those in the retail industry globally.

This comes in parallel with the increased threat of identity-based attacks. The broad scope of capabilities and data afforded to a Microsoft Office 365 user means successfully compromising an account can enable an attacker to cause massive harm with ease. Privileged accounts can be exploited to accelerate lateral movement and make systemic changes that will make it easier to gain permanence and remain undetected. Protecting these accounts and detecting and stopping their exploitation needs to form the core of any security strategy in 2021.

> The broad scope of capabilities and data afforded to a Microsoft Office 365 user means compromising an account can enable an attacker to cause massive harm with ease.

When asked about the most worrying threats to enterprise security in 2021, the survey revealed:

44%

There will be an increasing trend towards identity-based attacks on our authorised users

40%

Ransomware attacks will become more prevalent

45%

There will be increased attacks through IoT/connected devices

45%

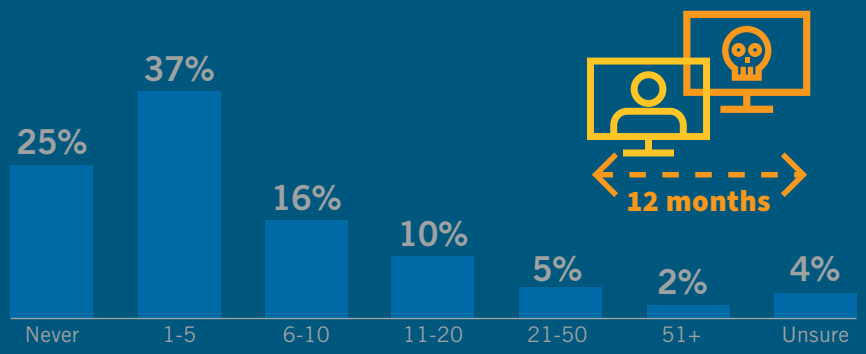
The ability of hackers to hide their tracks using legitimate Microsoft tooks such as Power Automate and e-Discovery

VECTRA
SECURITY THAT THINKS

The rising threat of account takeovers

The agility and interconnectivity provided by public cloud has been a huge boon to the average worker, but the same is true for threat actors. Microsoft Office 365 and other cloud environments are far more accessible than a traditional application sitting behind a perimeter. The attack surface of Microsoft Office 365 has been well publicised. Attackers note it is simple to perform reconnaissance and determine customers and their likely naming conventions.

7 **account takeovers** suffered by IT security decision makers on average of a legitimate user's account during the last 12 months



From here, attackers can deploy highly automated attacks to thousands of accounts with attempted logins. An organisation only needs a single user with poor password management for the attacker to find their way in, with multi factor authentication (MFA) often not posing a challenge to circumvent. This approach is extremely attractive for cyber criminals as it can net huge rewards without the need for a time-and-resource-heavy targeted attack.

Compromised Microsoft Office 365 accounts can be used to inflict massive harm in a very short span of time.

Cloud environments also enable adversaries to drastically shorten their attack cycle by greatly reducing the time needed for reconnaissance. Once a privileged account has been compromised attackers can use the organisation's legitimate APIs to retrieve any information they require.

Accordingly, IT security decision makers reported suffering an average of seven account takeovers of authorised users over the last 12 months.

Strikingly, despite the number of incidents and the huge risk presented by such a breach, the majority of respondents were quite confident in their ability to deal with account takeovers.

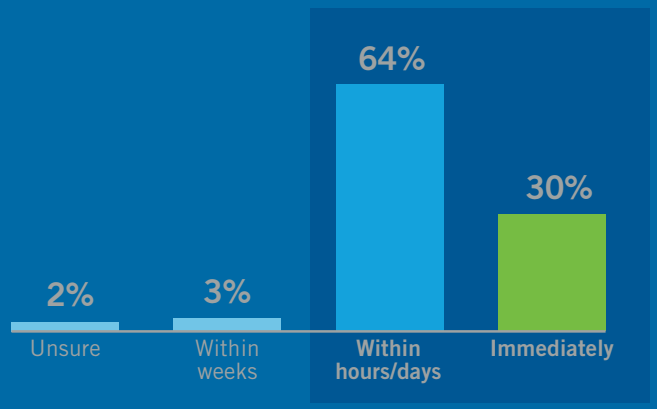
Sixty three percent believed they could identify and stop an account takeover within days, or even hours. Further, 30 percent of respondents believed they could halt such an attack immediately.

Compromised Microsoft Office 365 accounts can be used to inflict massive harm in a very short span of time, so those organisations that believe it will take several days to identify a takeover are still extremely vulnerable. It is imperative that they can identify suspicious behaviour on-prem and in the cloud in real time to spot an attacker before the damage is done.

Those who believe they can spot a compromise immediately must be sure their confidence is well placed – or brace for a rude awakening when a breach occurs.

almost **30%** say their team could identify and stop account takeovers **immediately**

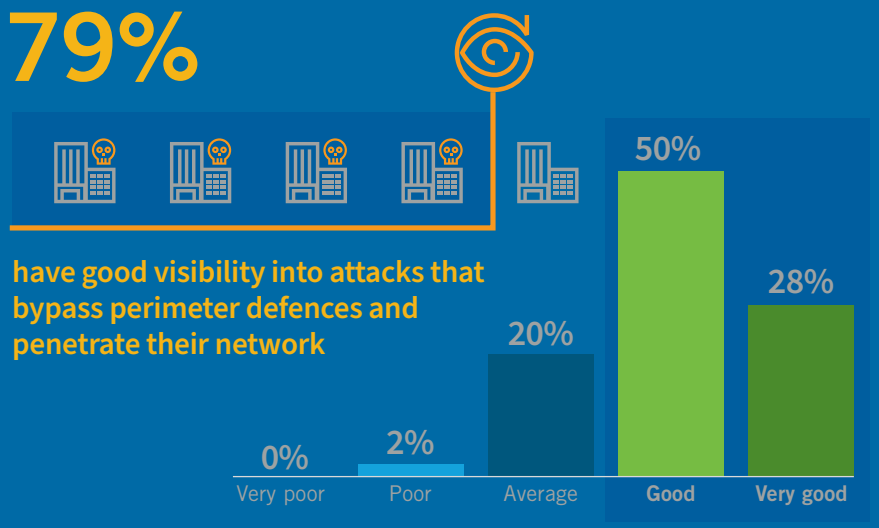
64% say they could stop account takeovers **within hours or days**



VECTRA
SECURITY THAT THINKS

Misplaced confidence?

The confidence displayed by security decision makers in their ability to prevent account takeover attacks is a stark contrast to the rising number of attacks and long dwell times. The average attack dwell time is estimated to be 43 days – and just three percent of respondents told us they would need weeks to deal with a compromised account.



Respondents were also generally quite confident about their abilities to identify and stop other forms of attacks. Most believed they had good visibility of attacks bypassing their perimeter and could detect and mitigate lateral movement. Again, this juxtaposes the fact that 96 percent of the Microsoft Office 365 environments investigated display signs of lateral movement.

The average attack dwell time is estimated to be 43 days – and just three percent of respondents told us they would need weeks to deal with a compromised account.

This positive attitude is disconnected from the reality we encounter when investigating an organisation. While some respondents can no doubt back up their claims, much of this confidence is likely misplaced.

Notably, attitudes were far more pessimistic across the board from management-level respondents in comparison to director and C-level roles. This indicates that a false sense of confidence may stem from skewed measurement and objectives at higher levels that don't match the reality of frontline security activity.

A false sense of confidence may stem from skewed measurement and objectives at higher levels that don't match the reality of frontline security activity.

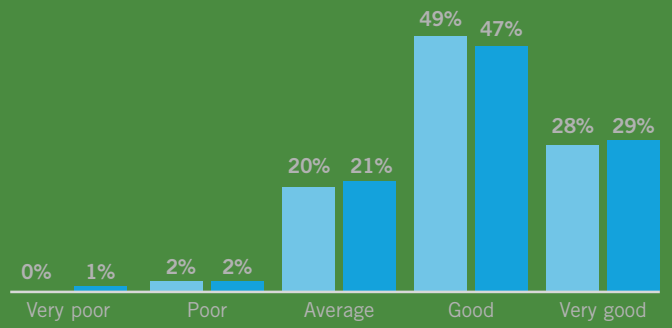
For example, a security operations centre (SOC) may be dealing with hundreds of threats a day. If you set the number of thwarted incidents as a leading indicator of success, this is fantastic. However, this approach lacks real context – how long were threats present before being detected and closed? How many were repeated issue? The ability to stop a large number of high volume, low-level attacks also has almost no bearing on detecting sophisticated threats, especially ones targeting users.

77%

describe their company as good at **detecting attacks**

76%

describe their company as good at **preventing attacks**



When it comes to the most dangerous attacks such as account takeovers, the indicators of compromise have shifted towards behavioural factors that are harder to define and may be spread across multiple environments in a way that is not immediately obvious.

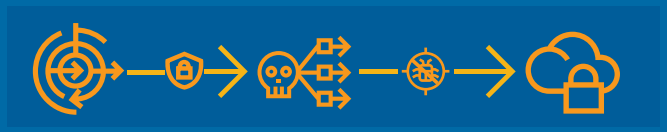
The reality is that threat actors are constantly evolving their tactics to overcome any barriers placed in their way.

Finally, this misplaced confidence may spring from the idea that following best security practice will guarantee protection from attack. However, the reality is that threat actors are constantly evolving their tactics to overcome any barriers placed in their way.

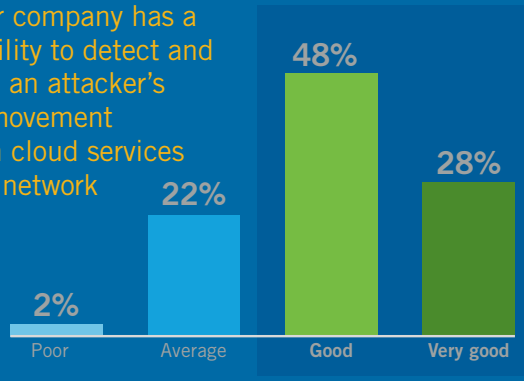
Multifactor authentication has for example, become near ubiquitous and many will believe it impervious against attempted account hijacking. Nevertheless, Microsoft has recently warned about flaws in relying on SMS and call-based MFA. In the US, the Cybersecurity and Infrastructure Security Agency (CISA) has reported a new "pass the cookie" technique that can bypass authentication to access cloud services. Security processes will only slow attackers down, not stop them entirely.

Microsoft has recently warned about flaws in relying on SMS and call-based MFA.

76%



say their company has a good ability to detect and mitigate an attacker's lateral movement between cloud services and the network



96%

of 4m businesses sampled by Vectra exhibited signs of lateral movement*

* Vectra 2020 Spotlight Report

VECTRA
SECURITY THAT THINKS

Ensuring confidence matches reality

Achieving an accurate view of security capabilities begins with the right measurements. The three most important factors to measure are:

1. Mean time to detect a threat (MTTD)
2. Mean time to respond (MTTR)
3. How often the same issues are resurfacing

Analysing these three factors will provide important context for how well the organisation's security capabilities are performing. Attacks that achieve long dwell times represent the biggest threat to the enterprise, particularly if they involve a compromised Microsoft Office 365 account with access to a range of data and applications where mere seconds is enough to cause an extensive headache for an organization. It is also important to note where the same issue is continually being addressed, as this indicates a fundamental change in policy or infrastructure may be required.

Any measurements must be based on a sufficient level of repeatable data.

Any measurements must be based on a sufficient level of repeatable data. Security analysts can create a higher volume of reliable threat data through activity such as penetration testing and red team exercises. This will make it readily apparent where the security strategy has gaps, and how effective defences actually are.

Aside from the measurement aspect, performing this activity is an essential skill for security analysts – locksmiths must be able to break locks as well as repair them.

Attacks that achieve long dwell times represent the biggest threat to the enterprise, particularly if they involve a compromised Microsoft Office 365 account.

"We now have a greater degree of confidence that we can detect and stop credential abuse that has become common in Office 365."

Kevin Orritt
ICT security manager
Greater Manchester Mental Health

VECTRA
SECURITY THAT THINKS

Improving security postures in 2021

Encouragingly, most security decision makers have adopted a fairly forward-thinking approach to improving their security postures in 2021. Not only are most planning to invest more in technology and people, but there is a strong preference for solutions that will be effective in securing Microsoft Office 365 environments against threats such as account takeover.

The deployment of AI solutions and increased automation were two of the most popular choices of focus for investments in 2021. These capabilities are essential for effectively analysing large volumes of threat data and identifying the subtle behavioural signs that point towards compromise. In addition, the use of AI to ease the workload can be attributed to the difficulty in hiring and retaining staff.

It is also noteworthy that 45 percent of respondents cited NDR as one of the two solutions for their SOC teams.

The deployment of AI solutions and increased automation were two of the most popular choices of focus for investments in 2021.

The key to security in a complex cloud environment is the ability to cut through the noise and identify signs of suspicious activity across the entire environment, treating on-prem and cloud networks as a unified whole. AI-powered NDR delivers this capability.

Finally, increased investment in threat hunting and other proactive measures were also popular areas of focus and will also help organisations gain a more accurate understanding of their security posture and identify vulnerabilities and attack paths in advance.

> "Before we deployed Vectra, we had limited visibility into malicious behaviours inside network traffic or Microsoft Office 365. We're impressed by what we can now see."
>
> **Kevin Orritt**
> *ICT security manager*
> *Greater Manchester Mental Health*

Also revealed within the survey:

58%
plan to invest more money in technology and people to improve their security posture in 2021.

52%
Deployment of more automation and AI.

47%
Use of threat intelligence.

45%
A move to proactive threat hunting.

10 steps for defending against identity-based attacks on Microsoft Office 365

With Microsoft Office 365 continuing to play an essential role in holding together business operations, organisations must ensure they have the capabilities to secure their cloud environments. This is a particularly pressing challenge for those organisations that have had to adapt their operations quickly over the last year and may struggle adapting perimeter-based defences to the more insubstantial borders presented by the cloud. Guarding against account take overs should be the lead priority.

Here are the top 10 steps organisations should be taking to secure their Microsoft Office 365 environments against compromised accounts:

1. **Understand your privileged accounts**. You need to have a solid understanding of which accounts can access sensitive data or use powerful Microsoft Office 365 tools such as eDiscovery. These accounts will be the prime target for threat actors. Strictly limiting system and tool access to those required by job roles will limit the damage a compromised account can inflict.

2. **Measure the right metrics**. Any metrics used to measure security effectiveness must pass the "so what?" test – it must drive action, not just inform. Measuring time to acknowledge, time to respond, repeated incidents and reinfection rates will provide a strong indication of how effectively your team is identifying and closing threats.

3. **Implement MFA**. Multi-factor authentication may not be the golden ticket of securing accounts, but it is still a very important tool for slowing attackers down. If you don't already, you should ensure that all accounts are using MFA.

4. **Minimise configuration complexity**. Transitional hybrid cloud environments can deliver the worst of both worlds in security, creating redundancies and blind spots that can be exploited. Lengthy transitions strain your IT and security resources and increase risk, so try to focus on accelerating the process to simplify and streamline your environment.

5. **Conduct regular testing**. Exercises such as penetration testing and red teaming will help assess the foundation of your security confidence by identifying vulnerabilities and attack paths. Tests must be repeated on a regular basis to ensure that fixes are improving your security standing.

6. **Train all your staff – security included**. As you continue to transform your operations, you must ensure your workforce is aware of how to use new tools safely – as well as educating them about threats such as adversaries impersonating the IT team in phishing emails. Greater awareness will reduce the success of initial compromise attempts. You also need to ensue your security personnel are up to speed with your new environment and can switch over from traditional perimeter-based strategies to the more open borders of the cloud.

7. **Understand how tools are being used**. Microsoft Office 365 tools like eDiscovery and Power Automate are devastating in the wrong hands. You need to gain context for how these tools are being used and build an accurate picture of what normal behaviour for these tools look like. Incorrect and malicious activity needs to be identified immediately and stopped before the damage can be done.

8. **Gain a unified view across your environments**. Adversaries will freely move between your traditional and cloud networks in pursuit of their goals, but it is difficult to connect the dots between separate security tools monitoring different environments. You need to be able to identify malicious behaviours across your IT network, SaaS cloud environment, data centre, and anywhere else attackers may exploit. NDR is essential here.

9. **Use AI to accelerate and automate your response times**. You aren't the only one benefiting from the increased speed and scale of the cloud – threat actors are too. The use of well-defined APIs means attackers can drastically shorten the exploration phase and begin executing their attack much faster. AI and machine learning enhanced analytics is key to rapidly identifying signs of malicious activity and automating response activity.

10. **Cut through the noise**. Rapid response capabilities are essential, but only half the story. Without a high-fidelity signal that cuts through the noise, overzealous automated defences may be triggered by false positives. AI-powered NDR will ensure that downstream response orchestration is accurate and reliable as well as fast.

> "Vectra gives all the necessary threat information to our SOC analysts. Cognito for Office 365 is priceless."
>
> **Head of security**
> *Global financial services firm*

VECTRA
SECURITY THAT THINKS

How Vectra protects Microsoft Office 365 and Azure AD

The Vectra AI-driven NDR solution, Cognito can identify and stop attackers operating in your Microsoft Office 365 environment and any federated SaaS application using Azure AD. We know that attackers don't operate in siloes, and can track signs of attacker behaviour across enterprise, hybrid, data centre, IaaS and SaaS, all from a single point of control.

VECTRA
SECURITY THAT THINKS

Vectra Cognito provides high fidelity, prioritized alerts rather than simply adding to the noise of constant security alerts. Critical threats such as the use of privileged access accounts are identified and prioritised so they can be shut down before the intruder has a chance to execute their attack.

Deploy in minutes with a cloud-native approach that quickly starts to monitor, detect and stop attacks.

Regain comprehensive security coverage between Microsoft Office 365, Azure AD, and your local enterprise infrastructure.

Stop unknown and known attacks and account takeovers in real time before they lead to data breaches.

"Vectra enables me to be proactive rather than reactive, which is a big deal for us. Instead of chasing down alerts from irrelevant logs, I spend more time working with our end-user community to create awareness about important security practices."

Kevin Orritt
ICT security manager
Greater Manchester Mental Health

VECTRA
SECURITY THAT THINKS

Appendices

Methodology

The research was commissioned by Vectra and conducted by Sapio Research among 1112 IT security decision makers in businesses using Microsoft Office 365 with more than 1000 employees, in the following industries: Government, Finance, Retail, Manufacturing, Healthcare, Education and Pharmaceutical.

At an overall level results are accurate to ± 2.9% at 95% confidence limits assuming a result of 50%.

The interviews were conducted online by Sapio Research in February 2021 using an email invitation and an online survey.

To find out how Vectra can help secure your Microsoft Office 365 and Azure AD environment against account takeover and other leading threats, get in touch at **info@vectra.ai.**

Email info@vectra.ai vectra.ai

Version **031721**