VECTRA®
SECURITY THAT THINKS

RESEARCH STUDY

Putting a magnifying glass on Microsoft 365 Security in a public setting:

Closing the gap between attackers and defenders

VECTRA
SECURITY THAT THINKS

Table of Contents

Foreword

Microsoft 365 dominates the business productivity landscape today across government, healthcare and education. As the Covid-19 pandemic hit in early 2020, organizations delivering critical public services across the world were able to quickly switch to both remote working and remote service delivery because of the agile and flexible working practices that Microsoft 365 supports. From enabling remote working for government workers, to supporting clinicians in delivering video appointments and teachers to provide online learning, it's clear that use of Microsoft 365 is much broader than ever before.

As public cloud usage increased within organizations that were delivering critical public services, so too did the attack surface that can be exploited by threat actors. Governments, healthcare and education institutions must now ensure that they can defend Microsoft 365 environments from criminals seeking to exploit its valuable data in serious cyber-attacks.

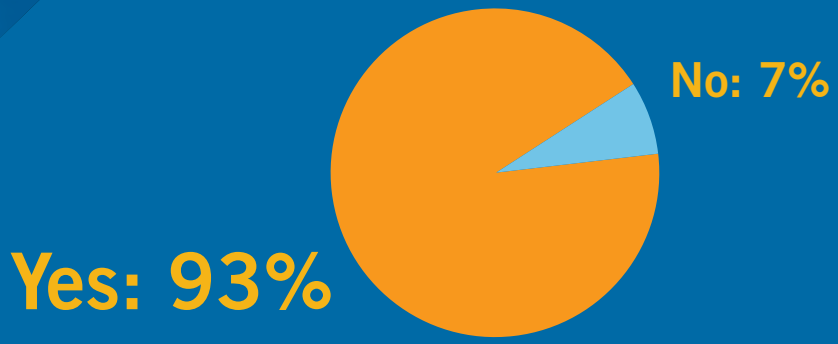
In this eBook, we share fresh insight into the Microsoft 365 landscape. We have conducted a global survey of over 1,100 IT security decision makers, and this eBook zeros in on the responses from the 302 professionals who work for government, healthcare and education organizations and institutions around the world. We have not only gathered their views on the biggest threats facing their Microsoft 365 environments, but also how well they feel they can defend them.

We also share practical actions on how to improve the security of Microsoft 365 infrastructure and Azure Active Directory, including how to identify and stop account takeover attacks in their tracks.

VECTRA
SECURITY THAT THINKS

Cloud usage in pubic service soars during the pandemic

With cloud capabilities swiftly transitioning from strategic advantage to business necessity during the pandemic, public services have raced to extend their use of Microsoft 365. Indeed, in the past year, public services have accelerated their cloud adoption strategy by several years.



93% of IT security decision makers interviewed have extended their use of Microsoft Office 365 as a result of the pandemic.

VECTRA
SECURITY THAT THINKS

As remote operations became the norm, it is perhaps no surprise that we saw an almost unanimous number of organizations extending their use of Microsoft 365. This was witnessed right across the business landscape: Microsoft reported 258 million active users of Microsoft Teams in March 2020, an increase of more than 70 million on the previous year.

"Vectra's solution has reduced the time it takes us to respond to attacks. In the past, it was difficult to know if something was happening because we didn't have an overview. Now, we know it very quickly because we have an overview of what is happening."

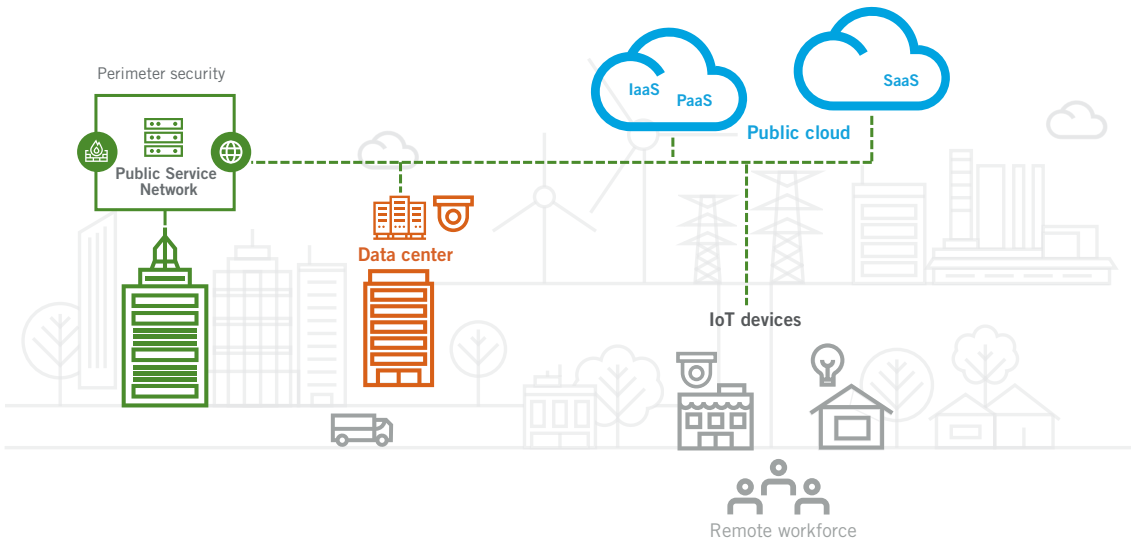
Project manager of a university

This imposed shift has permanently altered the IT landscape. When we asked IT security professionals working in government, healthcare and education organizations about the impact the pandemic has had on operations, more than eight in ten told us they had accelerated their cloud and digital transformation strategies as a result. Remarkably, one in five said it had accelerated by more than two years, and for those working in government organizations, one in four said the same.

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

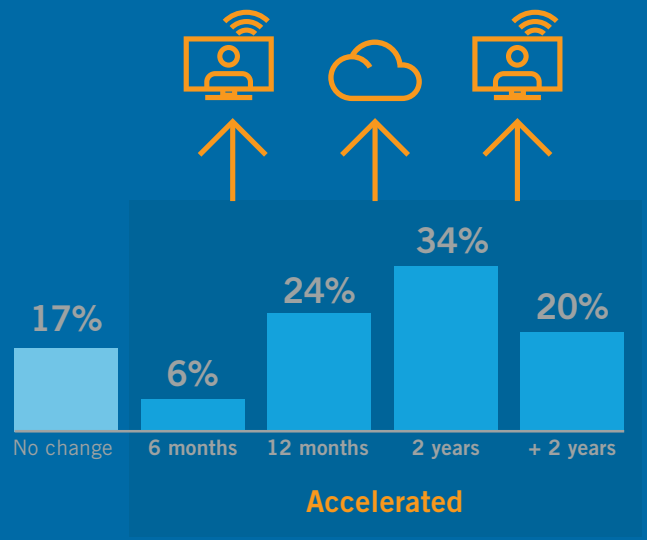
And while the last twelve months has for many been a case of trial-by-fire, this acceleration does appear to have delivered some tangible benefits. Just over 40 percent of our respondents have better job satisfaction and a similar proportion cited improved productivity.

It's clear, however, that the travails of the pandemic also led to a marked spike in stress; just under half of IT security decision makers in the public services organizations we surveyed noted that stress levels had worsened during the pandemic lockdown. Aside from the impact on personnel, the shift in the IT landscape and forced acceleration of cloud migration has also left these organizations more vulnerable to cyber threats.



83%

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

The increase in remote-working and adoption of Microsoft 365 and Azure AD inevitably created a larger attack surface. Many security professionals found themselves on the back foot, fighting to understand and secure this shifting environment. In many cases, existing on-premises security tools and policies were ill-equipped to effectively monitor and protect users. Of course, adversaries wasted no time in capitalizing on this changing landscape and increasing their attacks – by April 2020, Google was reportedly blocking more than 18 million COVID-themed phishing and malware emails globally every day.

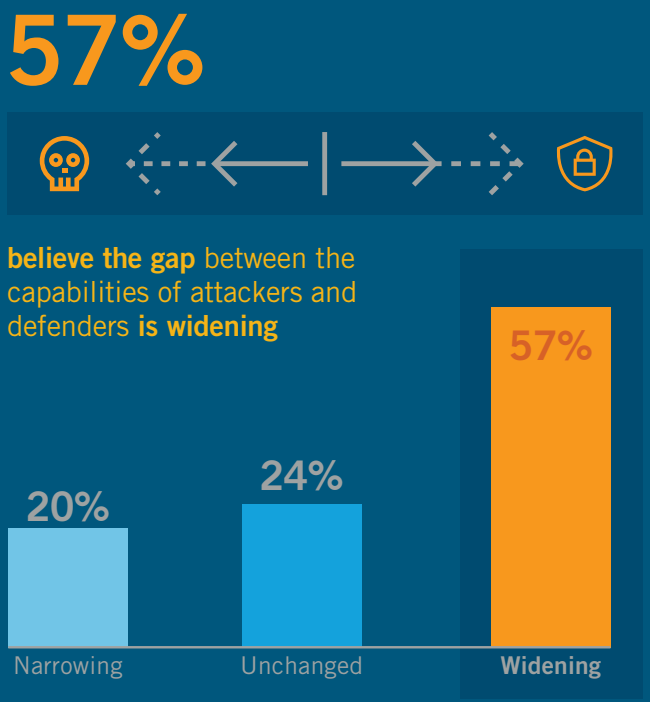
And while the prevalence of COVID-themed phishing attacks may have since declined, the security vulnerabilities of burgeoning cloud deployments will linger on. The majority of security decision makers within government, healthcare and education organizations believe the risks they face have increased over the last 12 months.

Three in five security decision makers believe the gap between the capabilities of attackers and defenders is widening.

Attackers are also getting smarter; applying their experience in navigating and exploiting this new terrain. We have seen a shift from traditional malware-based attacks to those focusing on accounts, credentials, permissions, and roles – an area that traditional security tools are 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 working within public services – almost three in five believe the gap between the capabilities of attackers and defenders is widening.

The majority of security decision makers within government, healthcare and education organizations believe the risks they face have increased over the last 12 months.



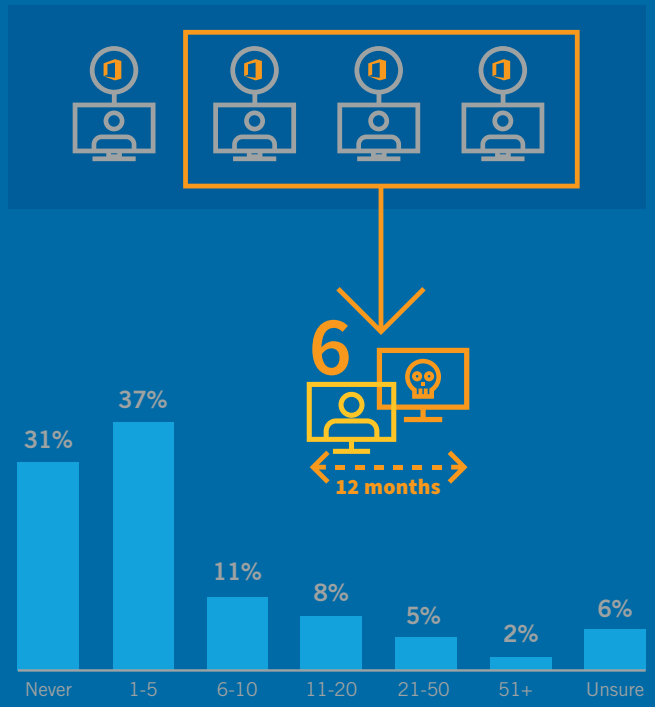
In fact, tools such as threat detection and response (i.e. NDR) and AI-powered analytics mean that the reverse is true. Once attackers have infiltrated an environment, they have traditionally relied on their ability to hide in the noise of normal business operations. Careful adversaries can live off the land by exploiting legitimate business applications and their tools, including those built into the Microsoft 365 suite – such as Power Automate and eDiscovery – to move laterally, hide, and exfiltrate data. AI-powered NDR solutions that integrate with cloud applications and services see straight through this cover and identify the minute clues that suggest an intruder is at work.

AI-powered NDR solutions that integrate with cloud applications and services see straight through this cover and identify the minute clues that suggest an intruder is at work.

Of course, the existence of these tools alone cannot narrow the gap between attackers and defenders. Only those organizations that have invested in these capabilities will be able to detect the subtle signs of malicious activity. Until then, we can unfortunately expect to see attackers continue to take full advantage of unprotected cloud infrastructure. For example, by taking over legitimate users' accounts in order to access sensitive data within. More than three in five of the government, healthcare and education organizations we surveyed had suffered at least one account takeover attack targeting their Microsoft 365 users in the last year.

> We can unfortunately expect to see attackers continue to take full advantage of unprotected cloud infrastructure.

63% of public services organizations have suffered an account takeover of a legitimate user's account **in the last year**



VECTRA
SECURITY THAT THINKS

Securing Microsoft 365 is a top priority

Government, healthcare and education organizations are a prime target for cyber-criminals due to the value of the data they hold and so IT security teams have to stay prepared for a wide variety of cyber-threats. Some of the top concerns amongst government, healthcare and education respondents include threats targeting IoT and connected devices; identity-based threats targeting authorized users; and the growing threat of ransomware.

Half of respondents said their top concern is the risk that data held in Microsoft 365 will be compromised

However, attacks targeting data held within Microsoft 365 emerged as the top worry, followed closely by the risk that hackers can hide their tracks using legitimate Microsoft tools such as Power Automate and eDiscovery. Microsoft 365 has become critical to government, healthcare and education operations; facilitating a significant proportion of data storage and sharing, as well as being the identity provider that brokers access to myriad other SaaS applications. This makes the Microsoft 365 environment a valuable target for threat actors, and with more than 250 million monthly users, there is no shortage of targets. Our recent Spotlight Report on Office 365, which involved the investigation of more than four million accounts, found 96 percent exhibited some sign of lateral movement.

Microsoft 365 has become critical to government, health-care and education operations; facilitating a significant proportion of data storage and sharing, as well as being the identity provider that brokers access to myriad other SaaS applications.

Likewise, many respondents were also concerned about the risk of credential abuse, leading to account take-over by unauthorized users.

The broad scope of capabilities and data afforded to a Microsoft 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 be at the core of cloud security strategies.

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

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

43%

There will be increased attacks through IoT/connected devices

43%

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

40%

Ransomware attacks will become more prevalent

40%

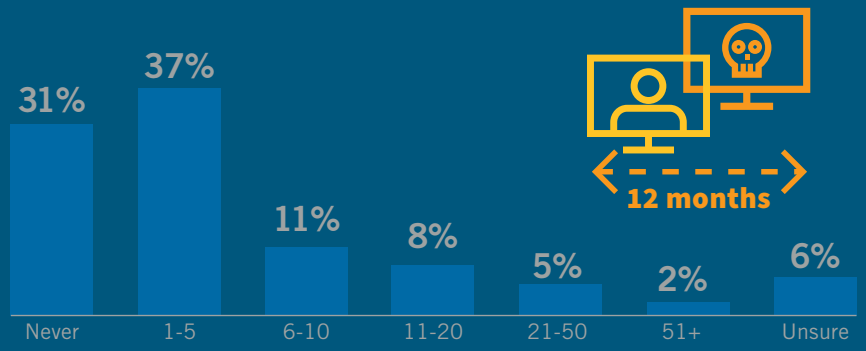
We will see a steep acceleration in cloud-based attacks

VECTRA
SECURITY THAT THINKS

The rising threat of account takeovers

The agility and interconnectivity provided by apps such as those in the Microsoft 365 suite has been a huge boon to the average worker, but the same is true for threat actors. Cloud environments are far more accessible than a traditional application sitting inside the network perimeter. Microsoft 365 attackers know only too well that it is simple to perform reconnaissance on Microsoft 365 and determine customers and their likely naming conventions.

6 **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 organization 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 cybercriminals as it can net huge rewards without the need for a time-and-resource-heavy targeted attack.

Compromised Microsoft 365 accounts can be used to inflict significant harm in a very short space of time.

Cloud environments also enable adversaries to drastically shorten their attack cycle by greatly reducing the time needed for reconnaissance.

Accordingly, IT security decision makers within government, healthcare and education organizations reported suffering an average of six account takeovers of authorized users over the last 12 months.

Strikingly, despite the number of incidents and the risk presented by such a breach, the majority of security decision makers working within the public services organizations we surveyed are confident in their ability to deal with account takeover attacks.

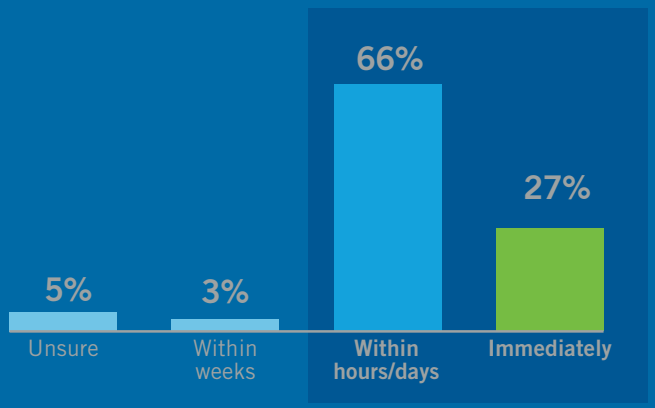
Close to seven in ten respondents estimate their team can identify and stop an account takeover within days, or even hours. Further, almost three in ten believe they could halt such an attack immediately.

Compromised Microsoft 365 accounts can be used to inflict significant harm in a very short space of time, so even taking just a few days to identify a takeover can make an organization extremely vulnerable. It is imperative that security teams can identify suspicious behavior on-premises and in the cloud in real-time, to spot an attacker before any damage is done.

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

almost **27%** say their team could identify and stop account takeovers **immediately**

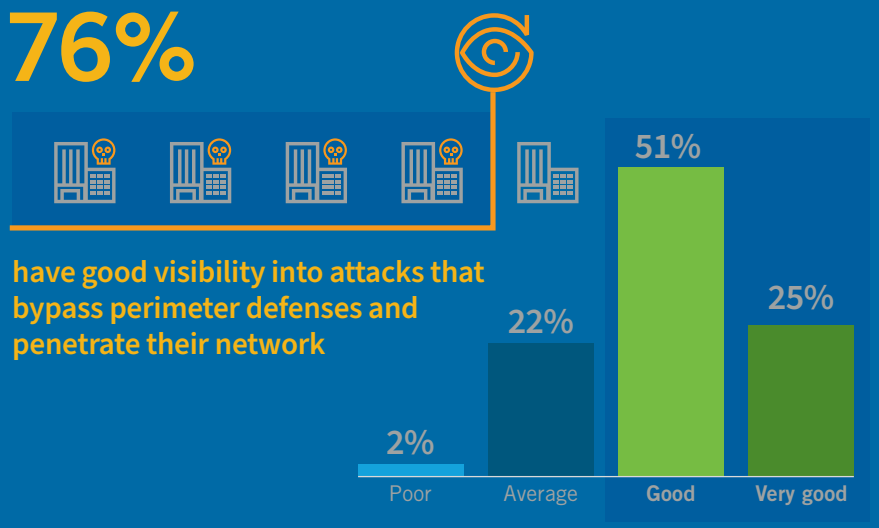
66% say they could stop account takeovers **within hours or days**



VECTRA
SECURITY THAT THINKS

Lack of visibility misleads confidence

The confidence displayed by these IT security decision makers in their ability to prevent account takeover attacks sits in stark contrast to the rising number of attacks and long dwell times reported in the industry at large. The average attack dwell time is estimated to be 43 days – and yet just three percent of respondents told us their team would take weeks to spot and deal with a compromised account.



Respondents were also generally quite confident about their ability 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 365 environments we have investigated display signs of lateral movement.

The average attack dwell time is estimated to be 43 days – and yet just one percent of respondents told us their team would take weeks to spot and deal with a compromised account.

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

Attitudes were more pessimistic from management-level respondents in comparison to owner and C-level executive roles. This suggests that a false sense of confidence may stem from skewed measurement and objectives at higher levels that do not match the reality of frontline security activity.

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

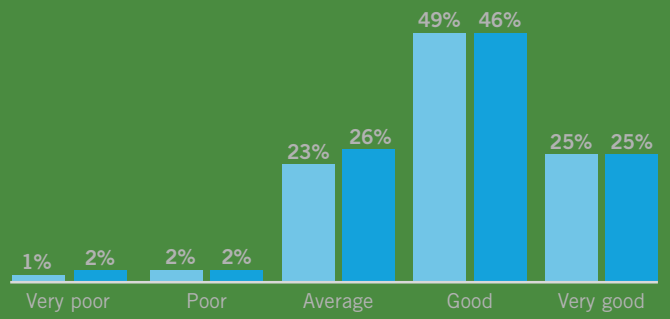
For example, a security operations center (SOC) may be dealing with hundreds of threats a day. If you set the number of thwarted incidents as a leading indicator of success, this is fantastic. However, this approach lacks real context – how long were threats present before being detected and closed? How many were repeated issues? 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.

74%

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

71%

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



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

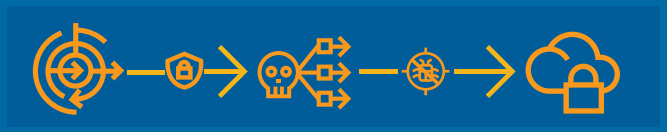
The reality is that threat actors are constantly evolving their tactics to overcome any barriers placed in their way.

Finally, this misled 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.

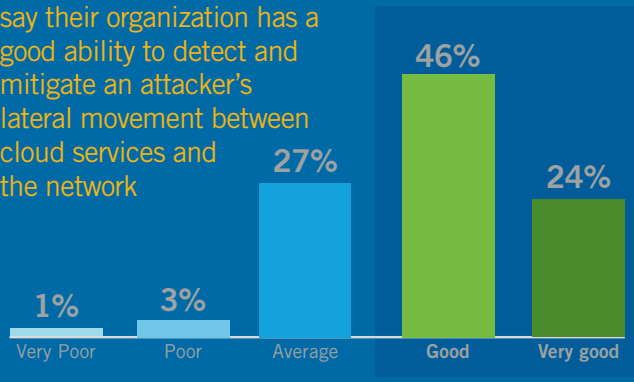
Multi-factor authentication has for example, become near ubiquitous and many will believe it impervious against attempted account hijacking. Nevertheless, Microsoft has recently warned about flaws in relying on SMS and call-based MFA. In the US, the Cybersecurity and Infrastructure Security Agency (CISA) 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.

70%



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



96%

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

* Vectra 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

Analyzing these three factors will provide important context for how well the organization's security capabilities are performing. Attacks that achieve long dwell times represent the biggest threat, particularly if they involve a compromised Microsoft 365 account with access to a range of data and applications where mere seconds is enough to cause an extensive headache for the 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 activities such as penetration testing and red team exercises. This will make it readily apparent where the security strategy has gaps, and how effective defenses actually are.

Aside from the measurement aspect, this is an essential skill for the SOC team – 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.

"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 in government, healthcare and education organizations have adopted a fairly forward-thinking approach to improving their security postures in 2021. Not only are close to three in five planning to invest more in technology and people, but also there is a strong preference to adopt solutions that can be effective in securing Microsoft 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 close to 40 percent of respondents cited NDR as one of the two top priority tools for their SOC teams.

The deployment of more AI and automation solutions is a popular choice for investment 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-premises and cloud networks as a unified whole. AI-powered threat detection and response delivers this capability.

Finally, increased use of threat intelligence and investment in threat hunting and other proactive measures were also popular areas of focus and will help security teams in public services 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:

59%
plan to invest more money in technology and people to improve their security posture in 2021.

49%
aim to deploy more automation and AI.

45%
want to make greater use of threat intelligence.

41%
will move to proactive threat hunting.

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

With Microsoft 365 continuing to play an essential role in underpinning operations, public services organizations must ensure that they have the capabilities to secure their cloud environments. This is a particularly pressing challenge for those government, healthcare and education institutions that have had to adapt their operations quickly over the last year and who may struggle to adapt perimeter-based defenses to the more insubstantial borders presented by the cloud. Guarding against account takeovers should be the lead priority.

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

Understand your privileged accounts. You need to have a solid understanding of which accounts can access sensitive data or use powerful Microsoft 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.

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.

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.

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 ensure 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 365 tools like eDiscovery and Power Automate are devastating in the wrong hands. You need to gain context of how these tools are being used and build an accurate picture of what normal behavior for these tools looks 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 behaviors across your IT network, SaaS cloud environment, data center, 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 defenses may be triggered by false positives. AI-powered threat detection will ensure that downstream response orchestration is accurate and reliable as well as fast.

VECTRA
SECURITY THAT THINKS

How Vectra protects Microsoft 365 and Azure AD

Vectra's AI-driven threat detection and response solution, Cognito, can identify and stop attackers operating in your Microsoft 365 environment and any federated SaaS application using Azure AD. We know that attackers do not operate in siloes, and we can track signs of attacker behavior across enterprise, hybrid, data center, 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 prioritized 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 365, Azure AD, and your local IT 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. The overall study surveyed 1,112 IT security decision makers in organizations using Microsoft 365 with more than 1,000 employees. A subset of 302 respondents was used to produce the statistics within this eBook; all these respondents identified as working within the Government, Healthcare or Education industry verticals.

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 **071521**