



2021

ARE YOU SAFE?

Introducing Advanced Threat Detection –
Early warning of cyber attacks for Office 365
& Azure

For the last 20 years, organisations have relied on firewall and anti-virus products as their main defence against hackers. These technologies still play an important role in an organisation's network security defences today, but with most businesses now capitalising on the many benefits of remote working and the Cloud, the fight against cyber-crime has shifted away from the office network and into the Cloud.



Are you safe?

Your new IT security team – your staff

“Are you safe from cyber-crime?” – a simple question yet worryingly most SMEs (and some larger enterprises) are unable to answer this question. And it's fair to assume, if a business does not know the answer they are not.

For the last 20 years organisations have relied on a firewall and anti-virus products as their main defence against hackers. These technologies still play an important role in an organisation's network security defences today, but with most businesses now capitalising on the many benefits of remote working and the Cloud, the fight against cyber-crime has shifted away from the office network and into the Cloud.

The Cloud offers many advantages over legacy server infrastructure – greater accessibility, reduced cost, flexibility,

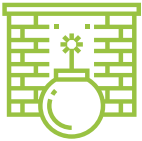
scalability, and higher-availability. But there are risks too. And one of the greatest benefits is also the biggest risk – accessibility. You can access it from anywhere – but so can a hacker.

► **Hackers of yesteryear focused their energies on cracking firewalls and devices, however today, your staff and your data represent the major targets and this fight is invisibly occurring in the Cloud, therefore out of sight and for some organisations, out of mind until the damage is done.**



▶ According to Keepnet's latest Phishing Statistics, 1 in every 8 employees shares information on a phishing site

Old threats (Device centric)



Firewall attacks



Viruses



Spam

Modern threats (User centric)



User exploitation



Office 365



Bring-your-own-device (BYOD)



Securing distributed workforce



Cloud web apps (multiple logins)



Vulnerability exploits



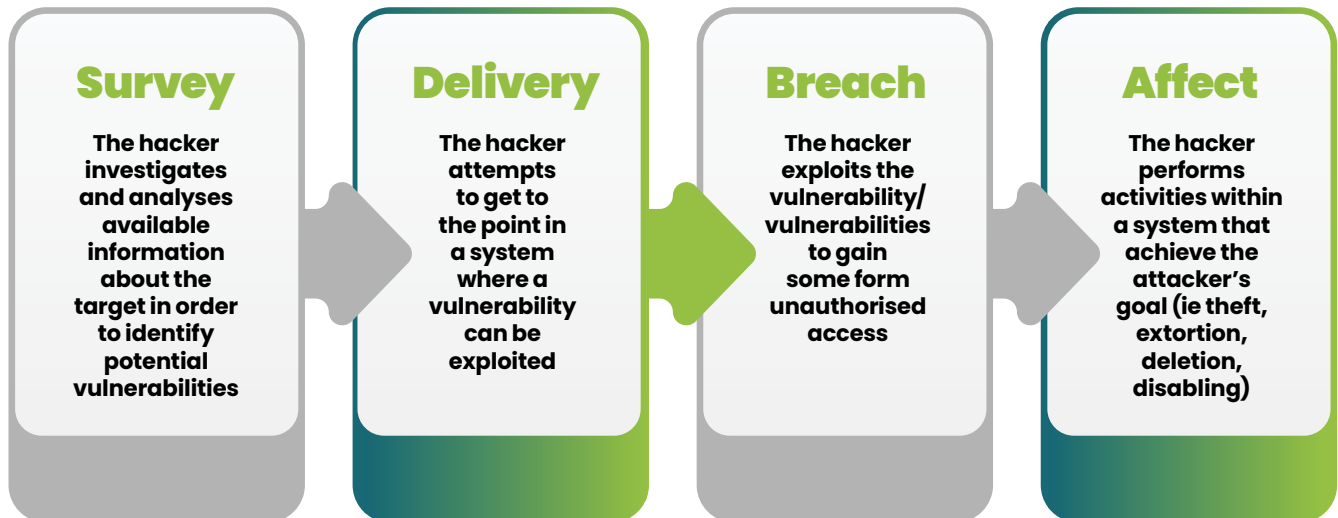
Zero-day threats



Grey IT (unmanaged tech)

Cyber-Crime

The Government's National Cyber Security Centre (NCSC) states there are four main stages to a typical cyber-attack*.



*<https://www.ncsc.gov.uk/information/how-cyber-attacks-work>

The early stages of the attack may be automated, as the hacker scans or emails your staff (and millions of other organisations) in order to find weaknesses.

Identifying a target is relatively straightforward – this could be a member of staff clicking a link, or entering credentials, or visiting a fraudulent web page, or simply someone using their work password to login to a 3rd party website. Eventually, most of us will innocently make a mistake. Many weeks or months may pass while the hacker attempts various strategies to gain access.

However, many hackers have more subtle and nefarious intentions which may not be immediately obvious. In the olden days (10+ years ago) many hacks were purely automated – one of your staff would click a link and a virus would encrypt their data.

The only time a real-human hacker would get involved is processing the transaction (if at all). But after years of being paid bitcoins for crime, and the huge rise in the value of bitcoins, hackers have money and money buys them resources.

Nowadays hackers are no longer kids in bedrooms, but criminal organisations with staff who now spend more time reviewing your data and considering the best angle to extort maximum value. You are no longer dealing with an automated bot, but a real criminal.

► **Over 60,000 phishing websites reported in March 2020 alone. 96% of all targeted attacks are developed for intelligence-gathering.**

► **Nowadays hackers are no longer kids in bedrooms, but criminal organisations with staff who now spend more time reviewing your data and considering the best angle to extort maximum value.**


Because most organisations have several gigabytes (or more) of data, it can take time for a hacker to review this looking for a dataset to extort payments (normally bitcoins). They will often try to copy your data to a remote server which they can readily access should you detect their presence and lock them out of your systems. This way they can continue to review the data in order to extort money.


Most data has some value, however certain types of data are generally more sensitive than others. Personal identifiable information (PII) is often attractive to hackers who know this can normally be found in HR folders. However, Information about clients and suppliers is also valuable.





Why is information about clients and suppliers valuable?

A hacker knows most organisations would:

 not want to have to tell clients data has been stolen, and

 an organisation is likely to have data-protection clauses or non-disclosure agreements in place, so any theft puts them in breach of contract, and

 not want their competitors to find out about the client relationships – contractual and commercial, and

 know they will have to flag the crime with the ICO, and for GDPR breaches, pay a fine of up to £18 million or 4% of annual global turnover.

It's fair to assume when considering the risk that one hack is one too many.

And as the hack progresses, its damage increases dramatically, therefore catching it early becomes vital.

Early Warning – Advanced Threat Detection

Organisations need an early warning while the attacker is performing their “survey” activities.

Organisations have a number of options at their disposal. Many companies have a vulnerability management service, like APEX™Secure, which helps them assess all their technology from a risk perspective – this helps to reduce the points of entry a hacker may exploit but it does not eliminate all risks.

A SOC (Security Operations Centre) service is another common security service. This involves aggregating events and logs from across your network and cloud services. These are reviewed by security professionals who look for unusual patterns, assess

the risks, and take action to protect an organisation.

However, these services are expensive and are therefore, rarely used by SMEs (organisations with under 500 staff) and despite their cost, they still have a major drawback – they lack the knowledge of your staff.

Yet, the majority of cyber-crime is focused at your staff – phishing emails, spoof website, brute force attacks, are some of the forms an attack can take. And once hackers get access to your systems, they use them in a similar way to your staff – they read documents, delete files, copy files. So how can you separate a member of staff from a hacker?



How can you separate a member of staff from a hacker?

Should an attacker gain access there are a number of possible indicators, a few of them are:-



Login from a malicious IP address –

has the same IP address been associated with suspicious behaviour



Atypical travel –

someone attempting to access an account from a location far from the member of staff's locations (ie a member of staff log in from a London IP address, then 40 minutes later, logs in from Russia)



Anonymous IP address –

someone trying to obscure their IP address



Malware linked IP address –

an IP address that has been associated with prior attacks



Password spray –

attempting multiple passwords to gain access



Leaked Credentials –

someone using login details which have been leaked



Suspicious inbox forwarding & redirects –

forwards of email or another provider (a typical activity performed by hackers to continue to monitor emails)



New country –

attempts from a different country the member of staff has never visited



Suspicious User Agent detected –

using a suspicious web client to access resources



Suspicious email deletion activity –

deleting emails after intercepting email dialogue



An event log was cleared –

a hacker attempting to hide their activity by clearing the event logs



Login from a principal user not seen in 60 days –

login after a long period of inactivity



Data deletion –

large deletions of data



Vulnerability scanner detected –

attempts to scan for exploitable vulnerabilities



Data copied –

large copies of data



Unfamiliar sign-in properties –

unusual sign-in attempts

Am I being hacked?

Many of these indicators may genuinely be staff – so how do you tell the difference?

APEX®ATD looks for many of the indicators of cyber-crime while possessing the knowledge of your staff.

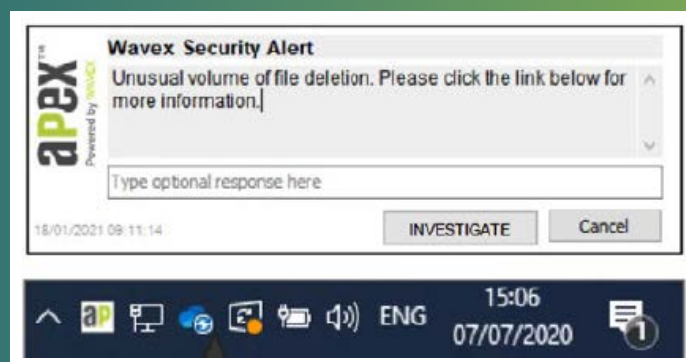
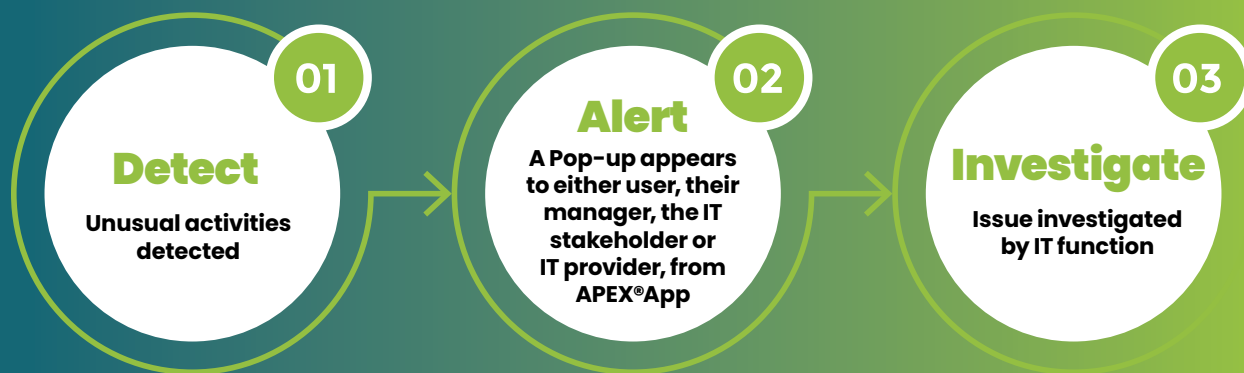
If a lot of data is deleted by a specific user and you know that specific user did not delete the data, you are being hacked.

Similar to a SOC (security operations centre), however, the **security professionals are your staff.**



APEX™ ATD continually monitors activity on Azure, Office 365 (and a number of other web services). The second it detects possible cyber-crime activity it contacts specific individuals. For instance, if your email is forwarded to a gmail or Hotmail account (a common activity performed by

hackers), it will ask you if you meant to do this. If you did – nothing happens. If you didn't – you click "investigate" and IT investigates the issue and locks out the hacker, so the hacker no longer has weeks to covertly read your emails. A simple process of "Detection", "Alert" and "Investigate".



ATD provides the following advantages:

- ✓ Early indication of cyber-crime.
- ✓ Enhanced security over a traditional (and expensive) SoC service which are acting without the knowledge of your staff.
- ✓ Cost-effective solution as it augments your IT function and your staff.
- ✓ Simple deployment without the need of any “bedding in” which normally plagues many complex cyber-security solutions.

Security should be an organisation-wide pursuit – with Advanced Threat Detection like APEX™ ATD, you can dramatically reduce the risk of cyber-crime while you continue to benefit from the advantages of the Cloud.

Stay safe.
Wavex Team.

About Wavex

Founded in 1998, Wavex offers industry leading managed IT and security services, professional IT project delivery and expert IT advice to London-based SMEs. Wavex helps clients improve organisational and individual performance by leveraging well-managed IT infrastructure, backed up by expert IT support and advice, supporting them on their modernisation journey. As a Microsoft Gold partner, we utilise the best of Microsoft, complemented by our IT managed services and a range of unique systems we have built in-house which all seamlessly come together to significantly enhance the overall quality of our IT service offering. The professionalism of our people,

combined with the unique functionality of the Wavex platform, ensures that we deliver a fast, exceptionally reliable and unusually accountable service to our clients. Ours is a flexible approach. We can act as a client's IT department or supplement an in-house IT function. In both cases, we aim to create long-term partnerships that add value through a combination of high-quality day-to-day support, expert project delivery and well considered strategic advice. Our focus is on providing businesses with the tools to improve efficiency while minimising risks and underpinning growth. We pride ourselves on enhancing user experience which is the driving force in all of our developments.

Multiple Awards



Affiliations & Certifications



Call us on **020 7030 3210** for a free consultation to discuss your specific organisational requirements today

Wavex Architect



wavex

Wavex Technology Limited



www.wavex.co.uk



20 7030 3210



tellmemore@wavex.co.uk