Securing the modern productive enterprise with Microsoft technology

The rise of cybercrime

"Cybercrime costs projected to reach $2 trillion by 2019" [Forbes, 2016][i]

"Cybercriminals collected $209 million in the first three months of 2016 by extorting businesses and institutions to unlock computer servers" [United States Federal Bureau of Investigation, 2016][ii]

Cybercrime is a general term used to describe criminal activity on the Internet. What was once viewed as "kids in basements" is now driven by major organised crime and is a serious issue. The financial motivation behind cybercrime means it's about far more than just technology – and criminals are indiscriminate in their targeting, attacking both individuals and companies. An underworld market of cybercrime-as-a-service provides attackers with the means to become cybercriminals.

The effects of cybercrime are tremendous, impacting a company's financial standing, reputation and ultimately its ability to provide security of employment to its staff.

Nevertheless, organisations can protect themselves. Mitigating the risks of cyber-attack can be achieved by applying people, process and technology to reduce the possibility of attack. To do this, they make themselves unattractive as a target, by increasing the effort involved and ultimately making it unprofitable for a would-be attacker to act against the company or its data.

Perimeter network control

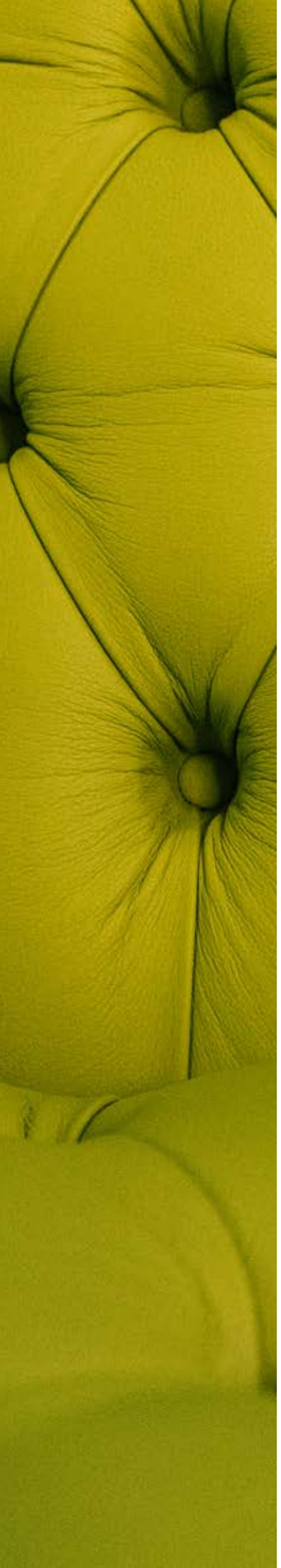
99: The median number of days that attackers reside within a victim's network before detection *[Mandiant/FireEye M-Trends Report, 2017]*[iii]

"The total average cost of a data breach to a company is $3.8 million" [Ponemon Institute study for IBM Corp, 2015][iv]

Enterprises have traditionally built applications and services in siloes, protecting those environments using perimeter network devices. In this traditional operating model, users were largely static and office based. This worked well, with some remote working capabilities possible through secure connectivity solutions such as Virtual Private Networks (VPNs).

The advent of cloud services requires a rethink of this model and a change in mindset. The move of services such as email, file services and other applications into hosted cloud applications means that the traditional perimeter controls are no longer effective. In addition, the ease and availability of cloud applications means employees can quickly and simply start using cloud services without being sanctioned by IT. Enforcing a IT-centric application model has become unsustainable.

With the perimeter network model no longer suitable for use, enterprises are being forced into new access models. These are no longer focused on controlled access and prevention, but focused on detection and response to threats. This has meant many enterprises have moved to a model of "assume breach" – i.e. the corporate network is assumed to be a compromised (or "dirty") environment.



Identity as the control plane

"More than 63% of all network intrusions are due to compromised user credentials" [Microsoft][v]

With the transition away from the perimeter network model and traditional VPN technologies, an alternative model for authentication and access control is needed. Identity has become the control plane and our identities are now very much the "keys to the digital kingdom". The result of this shift in model means that, as an attack vector for cyber criminals, identity has become even more lucrative.

The provides challenges – we can no longer rely on passwords which are often breached and re-used across systems. Meanwhile, the advice provided to generate complex passwords doesn't help if credentials are compromised; such policies lead to users choosing predictable methods to strike a balance between the system controls and usability.

We need a more robust identity management system.

Access control

In the past, organisations focused on securing devices and operating systems. Whilst this is still a valid element of the overall security strategy, the focus must shift to securing data – across any platform.

With the growth in software-as-a-service (SaaS) applications, delivered through a browser, the access control mechanism needs to apply equally to internal and external applications. In addition, it must support standard authentication mechanisms and allow internal applications to be published to remote and external users.

Data security

Securing data is not just about authentication and access though – we need a solution to protect against accidental or deliberate data leakage; provide policies for controlling data as it's shared with colleagues, customers and business partners; and allow organisations to discover and investigate potential issues.

Additionally, in a world where individual departments may procure their own IT services, it's increasingly important to be able to discover and assess the risk of cloud applications that have been adopted by business users without input from the corporate IT organisation (often referred to as "shadow IT").

Multi-vector attacks

Often, a criminal will use multiple vectors to attack. For example:

1. Discovery and analysis: to determine who is who within an organisation, how it is structured, etc. (footprinting)

2. Gain access to credentials.

3. Use credentials to breach organisational security and contact the criminal.

4. Install malware – an advanced persistent threat (APT), offering a means to access the organisation whenever the attacker needs to.

5. Attack, attack, attack:

   a. Inflict damage (e.g. to websites), access sensitive data, etc.

   b. Spear-phishing (e.g. to trick the finance department into making a payment).

   c. Ransomware (encrypting data until payment is made).

   d. (and other forms of attack…)

Potential threat vectors

Cybercriminal attack vectors include botnets and malware, which typically spread by encouraging users to access a malicious website or document, after which a device becomes infected. This doesn't just affect PCs but is prevalent on mobile devices too.

Phishing is a method of tricking a user into giving up their username and password with seemingly-genuine emails directing users to a fraudulent site. Variations of this called smishing (using SMS) and vishing (by voice) have also become commonplace. Sometimes, instead of going directly for access credentials, attackers ask for information around the account recovery process, after which they can assume a user's identity.

Spear-phishing goes further and targets an individual within an organisation (for example a CEO or CFO), who may instruct staff to make a payment to an organisation, assuming it to be genuine. Sometimes the request may be spoofed, making an email appear to come from someone that it doesn't.

Ransomware is becoming more prevalent, with malware being used to encrypt data and payment being demanded to regain access. Attackers use high-pressure techniques such as making data unrecoverable after a certain time; threatening to post captured (potentially sensitive) data publicly; threatening to erase all data and render enterprise computers inoperable; or increasing the ransom payment amount over time.

What may cost an individual a few hundred pounds may cost a company much more, with attackers using IP address information to dynamically price ransoms by geography.

The risks associated with an attack are amplified with mobility – typically infection occurs through one of the following methods:

- Public Wi-Fi (man-in-the-middle attacks).
- Links in email (where the destination may not be immediately apparent, depending on the email client in use).
- Untrusted websites.
- Sharing devices (for example, with family).
- Removeable media (e.g. USB flash drives).

Many security experts advise organisations to take a stance that assumes the network is already insecure, that a breach has been made, and to protect on that basis. Protection is achieved by applying management controls to email, documents, other data and to devices. Over the following paragraphs, we'll discuss some of the methods used, and later in this white paper we'll elaborate and explain how the Microsoft technology stack can be used to enact control.

Protecting email

There are several technical measures that organisations can take to increase email security – the UK Government National Centre for Cybersecurity (NCSC) recommends:

- Encryption, with Transport Layer Security (TLS).
- Certificate-based security.
- Public DNS, ensuring that the required records exist, for example for Sender Policy Framework (SPF) and
- DomainKeys Identified Email (DKIM).
- Anti-spoofing, checking inbound and outbound email using Domain-based Message Authentication, Reporting and Conformance (DMARC).

Protecting documents and data

The primary method to protect documents and data is around authorisation and access. That's why identity is key to controlling data in a secure, productive enterprise. Identity is the control plane around which all services should be designed as organisations grow familiar with working in a multi-vendor, cross-platform environment with increasing levels of SaaS delivery. With access controlled by identity (user rather than device), the ability for a compromised account to access organisation data is constrained to the rights of that user.

After controlling access, we can turn to secondary measures such as backup and digital rights management. If a secondary copy exists, then ransomware is no longer such a challenge – the secondary copy can be restored and business continues. As for digital rights management, controls may be exerted over the way that documents and data are used (or shared), perhaps allowing only read-access; limiting the ability to print, to copy/paste, or to make a new copy; preventing a document from being forwarded, or from being shared externally. Such controls can live with the document so that they still apply, even after it has left the organisation.

Protecting devices

Even with a shift to an identity-driven model, some requirement to protect devices remains. Not only can basic measures such as anti-malware protection limit the likelihood of a successful attack (although zero-day exploits are increasingly common so eradication is unlikely) but advanced technologies can protect against threats that would otherwise be overlooked.

The key to protecting devices is the visibility and capability to respond quickly to potential threats and to deal with them on a device before they spread throughout a network.

Solutions

A plethora of technical solutions exist to mitigate against the threats mentioned in the early part of this paper. Sometimes, it's difficult to keep track of what's what – so we'll describe some of the key technology solutions from Microsoft over the next few pages.
These are all either core features in Enterprise versions of Windows 10, available with selected Office 365 subscriptions, or available as part of an Enterprise Mobility + Security (EM+S) subscription. These complementary technologies are available to Microsoft's Enterprise customers under an agreement known as the Secure, Productive Enterprise (SPE).

Identity and access management

Azure Active Directory is Microsoft's identity-as-a-service (IDaaS) platform. It's a comprehensive identity and access management cloud solution that's central to the "identity as the control plane" approach to managing users and groups. Azure Active Directory provides cloud identity with options to integrate with on-premises Active Directory Domain Services (AD DS) using either a synchronisation engine (Azure AD Connect) or through federation, for example using Active Directory Federation Services (AD FS). Synchronisation keeps on-premises and cloud identities in step with each other (though they are two separate identities). Federation ensures that authentication takes place on-premises, using the existing AD DS functionality.

Azure Active Directory is based on industry-standard protocols and this means that, in addition to Microsoft's own SaaS platforms (Office 365 and Dynamics 365), thousands of third-party SaaS applications are pre-integrated with Azure Active Directory. Because of this, single sign-on is a reality, reducing the reliance on maintaining multiple sets of credentials.

Self-service options for Azure Active Directory mean common service desk tasks can be delegated to users – for example resetting passwords, and creating and managing groups.

Azure Active Directory also has options to integrate with consumer identity systems (Azure AD B2C), or for business partnerships (Azure AD B2B) so that business partners can securely access one another's systems.

Azure Active Directory Identity Protection is a feature that helps organisations to detect potential vulnerabilities and to automatically respond to suspicious incidents (such as multiple logons from geographically-dispersed locations).

Multifactor authentication

Azure Multifactor Authentication (MFA) helps secure environments against compromised passwords, by requiring users to validate their identity either using a smartphone app (directly or using a code), a phone call or an SMS (text) message. In addition to cloud deployments, MFA can also be used to secure on-premises applications.

Certificate based authentication

Certificates provide another authentication option, either as a secondary factor or as the primary authentication mechanism. They are particularly useful for authenticating mobile devices, including Android, iOS and Windows devices.

Microsoft Passport

Built into Windows 10, Microsoft Passport is a key-based authentication mechanism. A private key is stored in the device's Trusted Platform Module (TPM) chip and a user gesture, biometrics or PIN can be used to unlock the device. The private key is then used to provide authentication to Azure Active Directory.

Modern authentication

Modern authentication brings Active Directory Authentication Library (ADAL)-based sign-in to Office client applications across all platforms. With modern authentication, sign-in features such as MFA, smart card and certificate-based authentication, as well as SAML-based third-party identity providers, can be used with Office client applications, removing the need to use basic authentication protocols.

Conditional access

Conditional access comes in two forms: device based and location based. Both can be configured on a per-application basis, for Office 365 applications and applications published via Azure Active Directory.

Device-based conditional access requires that a device is compliant, domain-joined or both before it is granted access to an environment. Compliance policies ensure that devices meet a baseline before being allowed access. Conditional access also requires that a device is registered with Intune/Azure Active Directory.

Location-based conditional access allows applications to be allowed or blocked based on a device's location. This means it is possible to block access for a sensitive application to external users, allowing access from only corporate IP ranges, or to force a requirement for a secondary factor of authentication where a user is outside of the corporate network.

Identity management

With the proliferation of applications across the enterprise, it is important that application access is provisioned in a consistent manner, where possible against a single set of credentials. Microsoft Identity Manager allows synchronisation between directories, databases and applications, with automated provisioning of identities following an organisation's defined business processes.

Privileged identity and access management

Management of privileged access to Azure, Office 365 and on-premises environments is not exempt from the "identity is the control plane" concept. Indeed, identity management is even more critical – and of paramount importance for managing privileged access.

There are two types of management for privileged identities: Privileged Access Management is a feature of Microsoft Identity Manager for managing access to on-premises environments; and Privileged Identity Management is an Azure Active Directory feature for managing cloud based environments.

Both products follow the same concept – rather than becoming permanent administrators, users are granted "eligible administrator" status and need to complete an activation process in order to elevate their credentials for a predetermined time period. Requests are logged and an audit trail is available showing the access granted to individual users. Combined with Office 365 Advanced Security Management or Cloud App Security (discussed later in this paper), a comprehensive solution for securing and auditing administrative credentials and behaviour can be built.

Application publishing

In an enterprise where the workforce needs to be productive and secure whilst on the move, the traditional approach has been to use VPN technology to grant access through perimeter networks. Whilst this is a solution that works, it has often required significant amounts of additional infrastructure and management overhead, leading to the VPN becoming a threat vector itself. Additionally, VPN technology can be a limiting factor where users need to access on multiple devices.

Using Azure Active Directory Application Proxy, web based applications that are hosted internally can be published to mobile users. Applications published in this manner can benefit from the same level of protection as other Azure Active Directory Applications including the use of multifactor authentication and conditional access controls.

Information security and rights management

Advanced Security Management/Cloud App Security Office 365 Advanced Security Management (ASM) and Microsoft Cloud App Security (CAS) provide discovery, detection and control capabilities over the cloud applications in use within the enterprise. Using logs from on-premises network devices and shipping these into the ASM/CAS environment allows an enterprise to discover the extent to which shadow IT exists, giving insight into the type, number of and volume of unsanctioned cloud applications.

Threat detection is used within ASM/CAS to detect anomalies in the environment, analysing and evaluating user risk scenarios against many indicators, including failed login attempts, suspicious administrative activity or geographic access anomalies. Detecting such anomalies is only one part of the puzzle as ASM/CAS also allows policies to be created to give control over the use of cloud applications. For example, should a suspicious activity be detected, ASM/CAS can automatically take an action to suspend the user account or notify a security manager via text or email.

Azure Information Protection and Office 365 Information Rights Management

Office 365 includes Information Rights Management (IRM) capabilities that allow data in Exchange Online, SharePoint Online and OneDrive for Business to have digital rights management assigned. Office 365 IRM makes use of Azure Rights Management Services (RMS), which is now part of the broader EM+S offering in the form of Azure Information Protection (AIP).

AIP focuses on the classification and labelling of data throughout the enterprise. When information is classified, appropriate protections may be added around such data, including data in both email and Office document formats. Appropriate actions may include using Data Loss Prevention (DLP) policies to restrict data with a particular classification level from being shared via email or SharePoint.

For the most sensitive data, AIP offers integration with Azure RMS. This service enables access to restricted documents to be scoped, including the ability to not only restrict access to a set of users, but restricting subsequent behaviour – such as the ability to restrict printing of a document.

This two-pronged approach, firstly to classify and label data appropriately and then to secure and restrict the use of data based on its classification, provides a comprehensive solution for managing and securing data not only within the corporate environment but for those workers using mobile technologies and operating outside of the traditional corporate network.

Protection against threat vectors

Network security: Advanced Threat Analytics

"Only 31% of organisations discover a breach themselves. 69% are notified by a third party" [FireEye M-Trends Report, 2015][vi]

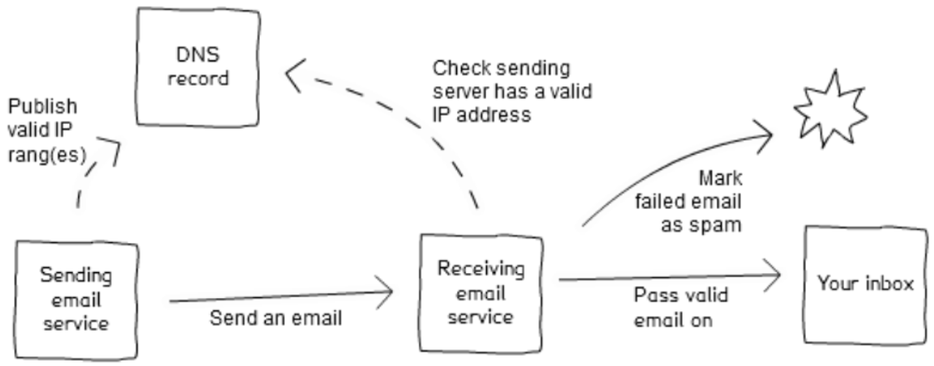
As described earlier, traditional network controls are less effective in a cloud environment and so an approach of "assume breach" is necessary. Establishing and pinpointing an attack through analysis of network logs alone is extremely challenging. Advanced Threat Analytics (ATA) focuses on the identification of suspicious activities making use of information from on-premises environments to detect attacks in a near real-time fashion. In addition to detecting common attacks such as pass-the-hash, ATA also counters against advanced attacks by leveraging behavioural analytics to learn about common user and device behaviour patterns. Departures from these patterns leads to alerts being raised.

Email security: anti-spam

Email sent to Exchange Online (Office 365) customers is received and processed through multiple filters and anti-virus engines within the Exchange Online Protection (EOP) service. EOP is a cloud service that provides anti-spam and anti-malware capabilities as well as filtering options based on email content and organisational policies. EOP is also available as a standalone service for customers who don't use Exchange Online.

Many email providers use the sender policy framework (SPF) as part of their reputation analysis to guard against unsolicited bulk email (spam). Using DNS records, the sending organisation publishes valid IP range(s) for its mail servers and the receiving service can check that the message is from a valid host and act accordingly, for example by quarantining the message as potential spam.

Whilst SPF does not directly filter or identify spam, implementing SPF can assist spam filtering systems to validate messages based on a domain's reputation.



Sender Policy Framework

Email security: links and attachments

Exchange Advanced Threat Protection (ATP) uses machine learning to analyse behaviour and detect anomalies, alerting administrators and providing protection against unknown malware or viruses (i.e. in a zero-day exploit scenario). After passing through EOP, ATP analyses attachments and links to ensure they are safe before delivering the email to the recipient mailbox(es).

With the Safe Attachments features, ATP analyses suspicious attachments in a "detonation chamber" (a form of sandbox), adding a small delay to email delivery but ensuring that only safe attachments are delivered to a user.

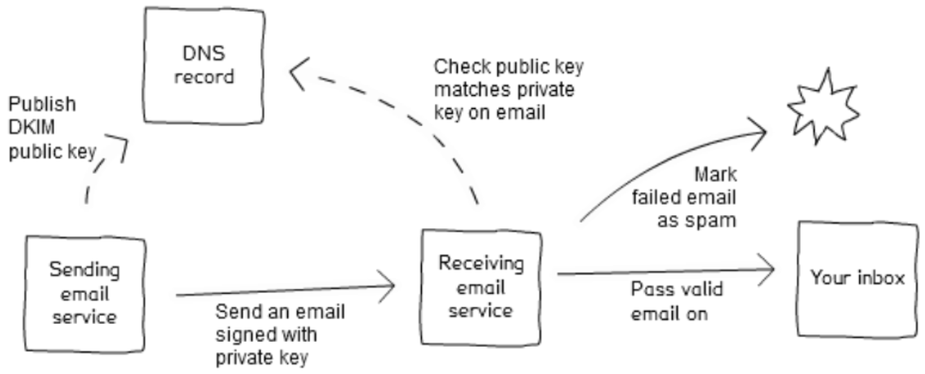
The impact of the delay is reduced using a feature called Dynamic Delivery, which sends the body of the email with a placeholder attachment (which notifies the user that the original attachment is being analysed) whilst the actual, suspicious attachment undergoes a Safe Attachments scan. Recipients can read and respond to the message and, if the real attachment is cleared, it replaces the placeholder. If not, the unwanted and potentially malicious attachment is filtered out.

Safe Links is another ATP technology used to checked links in emails and, if necessary, rewrite them to use a proxy server to provide "time-of-click" protection against a growing list of malicious URLs.

Email security: anti-spoofing

DomainKeys Identified Email (DKIM) builds on the model used for SPF but uses public/private key infrastructure (PKI) to sign email, which avoids publishing server IP addresses. A matching signature shows the message came from that domain and hasn't been altered.

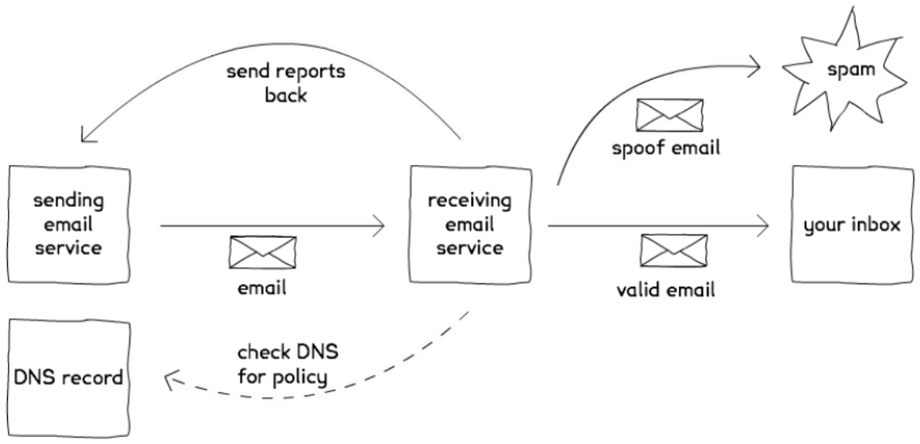
Many email services will check for DKIM signatures on inbound email but if the email service doesn't check for DKIM the message will be delivered. Just as for SPF, DKIM does not directly filter or identify spam but implementation of DKIM makes it much harder for spammers to spoof a domain and implementing DKIM can assist spam filtering systems with assessing a domain's reputation.



DomainKeys Identified Email (DKIM)

Microsoft publishes advice for administrators to enable DKIM in Exchange Online (Office 365) and, for organisations that have not set up DKIM, Office 365 will use its default policy and the keys it creates to enable DKIM for a domain.

Domain-based Message Authentication, Reporting and Conformance (DMARC) checks that inbound emails really do come from where they appear to, using a combination of SPF and DKIM. In addition, DMARC tells recipient email services what to do with messages that fail the check and asks recipient email services to return reports of where email is coming from. In this way, DMARC shares information between mail servers to notify organisations about any attempts to spoof their domain.



Domain-based Message Authentication, Reporting and Conformance (DMARC)

Microsoft automatically enables DMARC in Exchange Online (Office 365) for inbound email and publishes advice for administrators to enable DMARC for outbound email using custom domain names.

Office 365 SecureScore

Office 365 Secure Score is an online tool to provide insights into how securely an organisation has configured their Office 365 tenant. It provides a current and target score as guidance to improve security, together with an exportable action list, based on the features that the organisation has access to. The score may be analysed over time (and compared with the average across all of Office 365) to communicate the security position and show what's being done to improve it.

Device security: Windows BitLocker, Credential Guard and Device Guard

Windows 10 includes several technologies that can be used to secure the device. Not only do encryption technologies like BitLocker Drive Encryption secure data at rest on the device, but Windows Credential Guard isolates and hardens key systems and user secrets against compromise.

Device Guard is another Windows 10 feature that prevents malicious code from running by ensuring that boot files and firmware are signed and have not been tampered with, then running only trusted code from the boot loader onwards.

Device security: Windows Defender and Windows Defender Advanced Threat Protection

Windows Defender provides anti-virus, malware and spyware protection within the Windows 10 operating system. It operates at boot-time, in real-time and in conjunction with cloud services including network inspection and free automatic updates.

Windows Defender Advanced Threat Protection (ATP) should not be confused with Office 365 Advanced Threat Protection, though the two products are complementary. Windows Defender ATP is used in post-breach scenarios for analysis of where a breach occurred, what it did and where it accessed, sending data for analysis. The data is then used to improve detection for future attacks. It's important to note that ATP will work with other anti-malware solutions (not just Windows Defender).

Device security: Intune

For mobile and PC devices alike, Microsoft Intune provides mobile device management, mobile application management and PC management on Android, iOS, Windows 10 Mobile, Windows and MacOS. Corporate data can be secured on user-owned devices and information leakage is prevented by controlling the interaction between applications. As a cloud service, Intune requires no additional infrastructure but it can be integrated with existing System Center investments on-premises.

Summary

The security landscape has changed beyond all recognition. In the past, organisations could rely on the presence of a hardened perimeter but the modern world of mobile and remote working, combined with increased adoption of cloud services requires a much more holistic approach. Identity is key to this approach, described as the "control plane" around which other measures are built. In addition, the rise in cybercrime increases the risks (both reputational and fiscal) associated with a security breach.

Microsoft has a constantly-expanding range of products and services that provide both breadth and depth when improving an organisation's security posture. By combining features from Office 365, Enterprise Mobility + Security and Windows 10 Enterprise a secure, productive enterprise can become a reality.

How risual can help

risual is a customer-first, Microsoft technology company with a proven track record in delivering innovative solutions to meet business needs. Harnessing the capabilities in Microsoft's cloud and on-premises solutions, our consultancy and support teams offer public and commercial customers an end-to-end service, transforming the way businesses operate, reducing cost and enhancing productivity.

With one of the largest cohorts of Microsoft specialists in the UK, risual will tailor a Microsoft solution to support your business needs. The strength of our relationship with Microsoft is demonstrated by our Microsoft Partner of the Year awards – including as Country winner for the United Kingdom in 2015 and worldwide finalist for the Public Sector, Public Safety and National Security award in 2016. risual offer services across the whole of the Microsoft technology stack, which is why we're uniquely positioned to assist your organisation with digital transformation based on our three core transformational propositions: End User Computing; Optimised Service Vision; and Connected Business.

Our Business Group provides advisory services including strategic consulting, architecture and engagement management whilst our six specialised consulting practices focus on implementing technical solutions around:

- Business Productivity
- CRM
- Application Development
- Data Platform
- Unified Communications and Messaging
- Cloud Infrastructure

For full lifecycle support, risual provides fully managed solutions with reactive and proactive support options for both on-premises and cloud-hosted technology.

About the authors

Tim Siddle

Tim is one of risual's Enterprise Architects, helping to lead customers on their digital transformation experiences. Tim has a broad experience in IT having carried out roles in software development, infrastructure and IT Management. He has worked with Microsoft products for 10 years with a focus on mobility strategies and security using the Microsoft stack.

Mark Wilson

With experience in technology leadership, IT strategy and practice management roles, Mark Wilson is one of risual's Enterprise Architects, helping risual's customers to transform their businesses using Microsoft technology. Holding architecture and technical certifications, Mark has been working with Microsoft products for more than twenty years and is a former Microsoft Most Valuable Professional (MVP). Mark maintains a blog at https://markwilson.it/ and can be found on Twitter @markwilsonit.

Resources

The following resources provide additional information supporting the topics discussed in this paper:

- **Microsoft:**
  - Microsoft Secure Productive Enterprise: *http://risu.al/baqhj*
  - Microsoft Protection: *http://risu.al/baqhi*
  - 2016 Trends in Cybersecurity eBook: *http://risu.al/bap84*
  - Understanding Cybercrime: *http://risu.al/bap85*
  - Ransomware in the Microsoft Malware Protection Center: *http://risu.al/baqg2*
  - Credential theft demo: *http://risu.al/baqg3*
- **United Kingdom Government Digital Service (GDS):**
  - Sender Policy Framework (SPF) guidance: *http://risu.al/baqg4*
  - DomainKeys Identified Email (DKIM) guidance: *http://risu.al/baqg5*
  - Domain-based Message Authentication, Reporting and Conformance (DMARC) guidance: *http://risu.al/baqg6*
- **United Kingdom National Cybercrime Security Centre (NCSC):**
  - Protecting your Organisation from Ransomware: *http://risu.al/baqg7*
  - Approaching enterprise technology with cyber security in mind: *http://risu.al/baqg8*
- **United States Department of Homeland Security/Anti-Phishing Working Group (APWG)/United States National Cyber Security Alliance (NCSA):**
  - Stop. Think. Connect: *http://risu.al/baqg9*

Credits

i Cybercrime costs projected to reach $2 trillion by 2019: *http://risu.al/baqha*
ii FBI warning: Ransomware attacks skyrocketing: *http://risu.al/baqhb*
iii Mandiant/FireEye M-Trends Report 2017: *http://risu.al/baqhc*
iv Cost of data breaches increasing to average of $3.8 million, study says: *http://risu.al/baqhd*
v Uncover insider threats, blind spots in your network with Advanced Threat Analytics: *http://risu.al/baqhe*
vi Mandiant/FireEye M-Trends Report 2015: *http://risu.al/baqhf*

risual Ltd

www.risual.com
enquiries@risual.com
0300 303 2044

Securing the modern productive enterprise with Microsoft technology