Understanding Microsoft Cloud Services and Security

April 2018

Authored by Liam Cleary
Research conducted by CollabTalk LLC
and the Marriott School of Management at Brigham Young University

Sponsored by

Microsoft AvePoint® Rencore solliance your solution experts.

Contents

Introduction

Historically, storing all assets such as hardware, servers, applications and data behind the corporate firewall was the most secure. That was until there were high profile security and data breaches, using often known vulnerabilities as well as very complicated hacking tools and techniques. This led to many organizations coming to the realization that their security strategies were nowhere near where they should be. The answer to this for many organizations has been to spend obscene amounts of money buying the latest security appliances and software, as well as trying to apply broad and not-always-applicable security policies to all employees. This often leads to the battle between Security, IT and End Users for usability and sharing capabilities. Add to this the prevalent struggle in many organizations between security practices for on-premises environments versus those in the cloud.

Coming to the rescue for this internal battle, leading platform providers such as Amazon, Google and Microsoft have started to heavily promote their cloud offerings. Many other vendors, most of them self-install software providers, have also joined this new trend of converting their applications to Software-as-a-Service (SaaS) solutions, making it even easier for customers to access and utilize the products no matter where they are in the world. These individual-focused vendors have been marketing what seem like secure services, oftentimes offering better capabilities than anything an organization could build for themselves. However, even with the big push from the platform providers and the countless single-app vendors, many organizations are reluctant to move to the cloud. The number one concern is security. The issue is not the services (functionality) itself, but a lack of understanding of the implications of moving to the cloud, as well as knowing how security is handles -- and fear of the unknowns that come with change.

Each software or service provider has spent time researching, investing, and often acquiring solutions to bolster their security. The reason is simple: each vendor wants to offer the most secure platform. Some have added security at every level, others have added it to specific features only, and some have made securing their solutions so complex that their services never get fully enabled or configured. In some cases, these services require synchronization between on-premises authentication directories, allowing them to offer a single-sign-on experience with existing accounts, touting this approach as more secure since they use your existing directory of accounts, whereas others offer federation or separate accounts, all of which get wrapped by some sort of multi-factor authentication service.

Even with these innovations and services, organizations still struggle with the move to the cloud because of real or perceived security fears. For example, the fear that hackers are going to simply steal all their data, or somehow manage to break into the cloud, and then back into the corporate environment where they will steal everything. Organizations need to educate themselves on the realities of modern cloud security, identifying the actual risks – and then take the necessary steps to mitigate those risks.

This research-based document will help you identify the real issues around security within the Microsoft Cloud (primarily Office 365 and Azure services) and allow you to better mitigate the risks – and help your organization move to the cloud when ready.

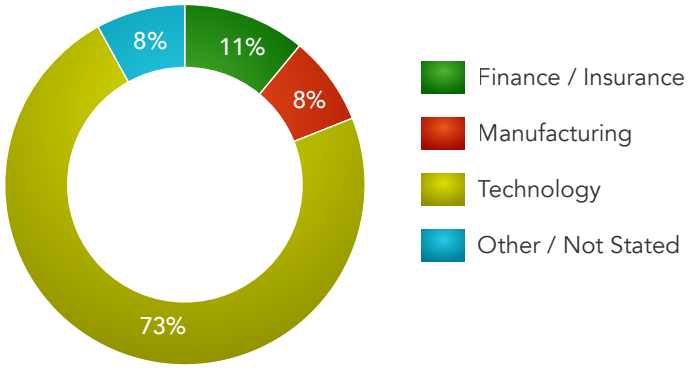
Cloud Services and Security

As you look at the overall security landscape, there are some key trends that are changing how an organization addresses security. There is, however, a lot of work that needs to be done to either achieve better security or ensure that an organization is not part of the $3.62 million average cost of a security or data breach, according to the Poneman Institute. The average cost for each lost or stolen record containing sensitive and confidential information significantly decreased from $158 in 2016 to $141 in 2017. However, despite the decline in the overall cost of breached records, organizations in 2017 were found to have larger data breaches than previously recorded. The average size of data breaches increased 1.8 percent to more than 24,000 records. https://www.ibm.com/security/data-breach

On average, a data breach in 2017 was estimated at 24,000 data records.

Latest Cloud Security Trends, Challenges and Threats

Some of the latest security trends, challenges and threats are explained below. The basis for this information comes from a 2018 study conducted by CollabTalk LLC and BYU Marriott School, as well as other primary and secondary surveys.



General Data Protection Regulation (GDPR)

A major new European Union regulation that will go into effect on May 25, 2018, GDPR rulings and guidelines can and will have an impact on many organizations – inside and outside of the EU. This will force many organizations to implement new security features from required consent to secure storage. It will also, however, open potential security issues as organizations struggle to define policies and meet the GDPR obligations.

Artificial Intelligence / Machine-Learning and Behavioral Learning Defense

Artificial intelligence and machine-learning will become the norm within the Cyber-Security space. With cyber-criminals moving so quickly, machine-learning models that can predict and accurately identify attacks swiftly would benefit most organizations. There is also a risk that AI and machine-learning may be exploited by attackers.

Proactive Monitoring and Protecting of Ransomware and Cryptoware

With the increase of Ransomware and Cryptoware, organizations need to either manually, or automatically with tools, monitor and protect from these types of attacks. This attack is often very hard to mitigate, and is most often based around email and phishing types of attacks.

Breach Notifications and Resolution

Identifying security and data breaches takes an average of 206 days, which often leaves many organizations with further risk. This risk does not change at all, and has always been a problem in the event of a breach.

Implementation of Internet-of-Things (IoT) Devices

With the proliferation IoT devices, both in the business and consumer spaces, being able to secure them has historically been complicated as most devices have not been able to support the required security. As these are added into organizations, or devices are connected to services owned by the organization, this will become a core risk.

Each of these devices bring their own problems, whether with compliance, implementation, or management – no matter what the solution or service selection.

New Security Features

For the past few years, the security landscape has changed tremendously. In the past, vendors have touted the "Next Generation" appliances that can inspect everything and protect from all things malicious. To some extent, this has fueled the industry. However, the services and appliances have often not lived up to the selling points. Organizations have purchased these solutions, but when vulnerabilities are found, many often quickly swap vendors in the search for a better solution, leaving them constantly moving between vendors, chasing the promise of a better and more secure solution.

In the past year, this has changed. The latest trend is Artificial Intelligence (AI) and machine-learning that can identify and mitigate all security problems and issues before we even realize they have happened. With these new intelligent capabilities, these advanced services are now common place with almost all vendors, offering a more powerful solution that can auto-protect, as if you had your own personal security team working 24 x 7 to defend your networks.

To support this type of security, these new "smart platforms" must create a baseline, building a picture of all end users and administrators, so that they can recognize normal behavior versus abnormal behavior. These services and appliances are sold as having behavioral analysis as well as intelligence, helping them to identify threats before they happen.

The Growing Security Concerns with Digital Transformation

I am sure by now that you have heard the phrase "Digital Transformation". When you hear that phase, a few questions probably come to mind: What does it mean? How do you do it? Is it something new?

What it really means is to assess and transform your business processes, data storage, and management, creating automated processes that utilize the full capability of your software and services to streamline processes, making your organization more efficient -- and ultimately, saving you money.

Though all of that may be true, a side effect of many business transformation efforts is that organizations fail to thoroughly understand the security controls of their new solutions and capabilities, focusing instead on features and capabilities. Organizations often get tied up in the transformation piece, allowing business users and services to share data and content easily, to the point where the security "blanket" that should be applied over the top is either completely shut off, or is added as an afterthought. This normally leads to a system being left open by design, with the idea that a more open environment will encourage more open and easy sharing and collaboration.

Speaking with many organizations, specifically security and internal IT teams, this is often their number one priority and issue that they battle with end users and departments. The balance between ease-of-use and security is an age-old battle that isn't easily solved. Luckily, cloud providers have spent a lot of time creating systems that help with "Digital Transformation" but also wrap the necessary security tools and services over the top. However, based on the latest research, organizations don't always implement these features, and don't know what their cloud providers even offer. This education gap, combined with a lack of incident response planning, means that in the event of an issue, the organization has no plan of how to overcome it, or even remediate the security problem.

Based on a study performed by ISACA, ***"More than 3 in 4 (76 percent) of respondents believe security is bought in too late to digital transformation initiatives."***

http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

Common Weakness and Attacks

As you look at the latest cyber-attacks highlighted in the media, there are a few common weaknesses that are attacked, no matter what the technology being used, or the size of organization. The weakest links in any cyber-security strategy are the end users and administrators. Techniques such as social-engineering, which is a non-technical strategy using real human interaction to pressure or trick someone into breaking security protocols, have been around for many years and are still very effective. This attack is successful because end users put complete trust in the systems that have been deployed to protect.

There are, however, many other weaknesses that can be the root cause of a security or data breach. These weaknesses are normally isolated to specific applications or services that do not have the correct security implemented to protect. Most of these weaknesses can be found within the OWASP Top 10:

1. **Injection**
2. **Authentication**
3. **Cross-Site Scripting**
4. **Insecure Direct Object References**
5. **Security Misconfiguration**
6. **Sensitive Data Exposure**
7. **Missing function level Access Control**
8. **Cross Site Request Forgery (CSRF)**
9. **Using components with existing Vulnerabilities**
10. **Un-validated redirects and forwards**

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

These techniques are used in most types of attacks, whether initiated through social engineering or through brute force attacks against physical or virtual infrastructure.

When looking at the Microsoft Cloud services, the most common weakness is always the end user and the associated security account. Many organizations do not enable any type of Multi-Factor Authentication (MFA) services, which increases risk. There is limited risk inherent due to a service being hosted in the cloud because they are hosted within data centers that are potentially under constant cyber-attack.

Over half (53%) of the respondents use Multi-Factor-Authentication, but it was still the most commonly used product

Common Weakness and Attacks

Incident Types

There are many different types of security incidents that can happen within an organization. Incident management is a key tool to help you protect your organization from future issues. Many organizations do not have any kind of incident response mechanisms in place, which means that in the event of a breach, nothing will be detected until the damage is done, and the organization has experienced detrimental consequences. The first task should be to understand the various incident types, followed by incident categorization, followed by response procedure, and finally resolution.
Using the NIST Framework (https://www.nist.gov/cyberframework) there are six core categories that are recommended for incident types.

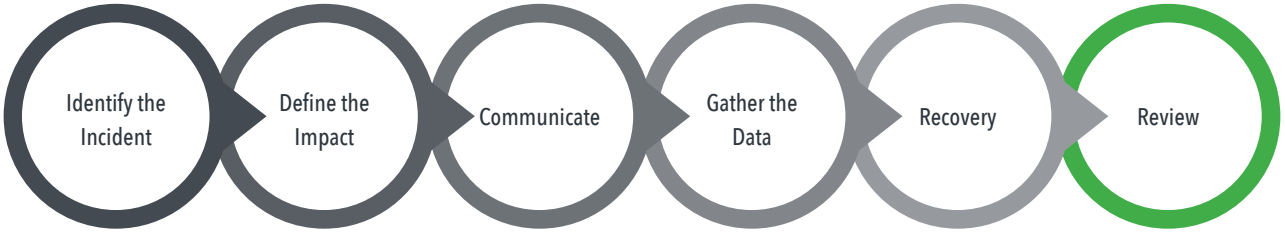
1. **CAT 1 - Unauthorized Access, compromised machine, Compromised Asset, Data Theft, Espionage etc.**
2. **CAT 2 - Denial of Service (DoS/DDoS)**
3. **CAT 3 - Malware or Malicious Code**
4. **CAT 4 - Reconnaissance, Scans or Probes**
5. **CAT 5 - Policy Violations or Improper Usage**
6. **CAT 6 - Others and Uncategorized**

For each security incident that is identified, the next task is to assign a severity rating that will help an organization identify how to proceed and which resources should be tasked with the resolution, as well as used to secure budget support from the management and executive team. An example rating system is outlined below:

Business Impact	Possibility of Attack				
	Rare	**Unlikely**	**Possible**	**Likely**	**Certain**
Catastrophic	Medium	Medium	High	Critical	Critical
Major	Low	Medium	Medium	High	Critical
Moderate	Low	Medium	Medium	Medium	High
Minor	Very Low	Low	Medium	Medium	Medium
Insignificant	Very Low	Very Low	Low	Low	Medium

More details from the NIST Framework that relates to incident response can be found here: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Almost every day we hear of another business that has suffered from a security breach. According to the National Crime Agency in the UK, there were 2,500,000 cyber-attacks in 2017 in the UK alone. With statistics like this, organizations need to change their attitude toward the threat of cyber-attacks. The best way for businesses to protect themselves is by creating and adopting an incident response plan. There are six steps to any incident response plan that will make it effective:



These six steps, when followed, will help an organization ensure that they are prepared for any security incident, as well as help with the remediation process.

Perceived-versus-Real Security Cloud Concerns

Many of the reasons organizations have not moved to the cloud is because of the perceived threat. For most organizations, there is the safety and comfort of hosting all infrastructure and services themselves. The ability for the Security and IT teams to see the servers, and update, monitor and control all devices, brings with it the comfort that most management and executive teams require.

Though cloud may seem new, many organizations have been outsourcing services and technology for many years. Providers deliver hosted technology offerings that are located offsite with client access via private or public connections. However, the thought of moving everything into a public cloud service such as Microsoft's Office 365, for some reason ,raises these perceived concerns.

In a survey completed in 2015, the top perceived security threats with cloud services were:

Unauthorized Access

Hijacking of Accounts

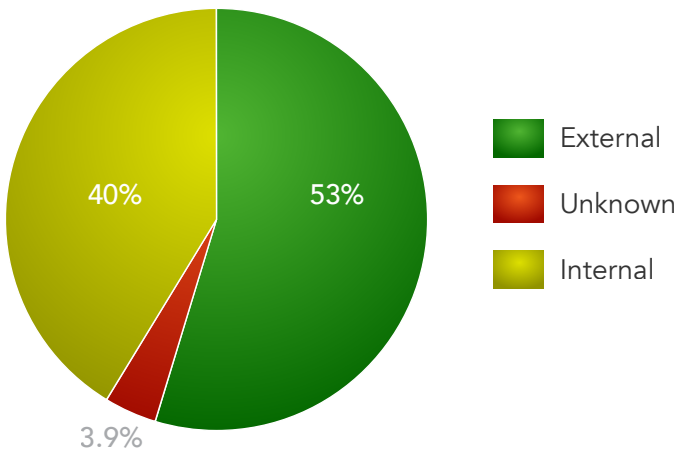
Malicious Insiders

Interestingly, the most common security breaches, such as malware and denial of service attacks, were not in the top perceived security threats.

Actual Cloud Security Risks and Concerns

The top perceived security fears may be justified, considering that more organizations have experienced a security or data breach within their public cloud service, rather than their on-premises applications. On this main issue, when comparing percentage of breaches within cloud applications versus on-premises applications, the cloud has a higher rate of security breaches. However, digging deeper into the breach data, often the attack within the cloud was not an actual brute-force attack on the service, but more of an attack on the end user and their account to gain access. Breaches that took place on-premises were a mix of the same account attack, as well as a higher percentage of core infrastructure attacks. When dealing with a security or data breach, the follow up actions and events performed by Security and IT teams can have a great impact on the potential damage caused.

Breach Type



Based on the 2018 CollabTalk survey, we saw that most organizations were able to identify where the security or data breach originated, however, only 68% ran any kind of security checks to ensure systems were protected correctly. For organizations that did not experience a breach, 32% did not run any security checks on their systems at all.

Actual Cloud Security Risks and Concerns

So, What are the Real Risks and Concerns?

In speaking with Chris Givens, a Microsoft MVP and Sr Cloud Architect at Solliance, he stated *"Office 365 has the possibility of being secure, but not right out of the box. It requires some effort. The customer must choose to take the right security precautions".* From our research, most organizations responded that they had not put the effort into their security configuration, and often did not even own the correct licenses required to implement the services.

The fact is that the real security concerns come from a misunderstanding that an organization loses some level of security and control by going to the cloud. In fact, according to Eric Raff, a Cloud Solutions Architect at JourneyTeam, *"Office 365 doesn't come out of the box secure, it doesn't have the visibility and tools necessary. To get a comprehensive security solution for Office 365 you really need to add the Microsoft Enterprise Mobility Suite, but this also adds another level of complexity and another stack of things to understand and implement."* He also added *"It is a fine line that Microsoft walks. Office 365 is a collaborative environment where things are meant to be shared, but 'sharing' is the thing one is trying to prevent in terms of cyber security. Sharing is therefore one of the biggest security risks with Office 365 and it is up to the user to ensure that only the right people can access the company's sensitive information".*

Many of the respondents of the CollabTalk survey stated that they had concerns with Microsoft security in the cloud, but at the same time, many respondents also stated they did know about Microsoft's overall security strategy and thought that it was appropriate. For example, understanding that Microsoft have a dedicated Red and Blue Team for both Office 365 Services and Microsoft Azure, respondents agreed that Microsoft is showing a real commitment to security. The discrepancy between concerns over Microsoft's cloud services while acknowledging their industry-leading cloud security programs and efforts highlights an important fact: that the risk and threat comes from a lack of education and understanding, not from Microsoft's failure to provide adequate security measures.

More than 60% of organizations report having too few information security professionals

Second, respondents also stated that they did not want to pay for extra services and licenses that, in fact, would provide the required security to remove the risks and concerns, especially for services that would protect end user accounts, which is the often the primary attack vector. Jeremy Grant, Managing Director at Venable LLP, stated in a congressional hearing "Identity Verification in a Post Breach World" that *"There is no such thing as a 'strong' password in 2017 and we should stop trying to pretend otherwise".*

If there really are no secure passwords, then this is a significant issue for Microsoft. Microsoft has security offerings that are much stronger than a password. Multi-Factor-Authentication comes with an additional cost, leaving many organizations behind who think they are saving money by purchasing less expensive licenses. They don't understand its necessity, and thereby introduce serious security risk to their environments.

Third, we identified that many organizations felt they had inadequate security professionals within their organizations to implement what is needed to create a security infrastructure. From our findings, lack of education and lack of security IT budget will also be a stumbling block for many organizations.

42%
Not aware of Microsoft's Security Strategy

79%
Microsoft Security is Sufficient

45%
Proactively run Security check

However, 42% of respondents were not aware of Microsoft's security strategy, compared with 79% who stated Microsoft's security was sufficient, with 45% of them proactively running security checks.

The Risk to Customizations

The Protections of 'Out-of-the-Box'

I am sure you have heard the phases, "keep it out of the box", "we don't want any customizations", or something along those lines. These examples are valid statements that all organizations should adhere to. Now, I am not saying that customizations are completely bad, but there are certain protections that come from staying out-of-the-box. Using SharePoint as the example, Microsoft have built a core platform that, yes, can be extended and modified to suit the business need. However, I have worked with many organizations since SharePoint 2001 was released, and most perceived or needed customizations could be done out-of-the-box by making slight changes to the business requirements. The platform itself has been designed to accommodate specific functionality and has been tested for performance, usage, and of course security. Using out-of-the-box functions and components for business solutions provides the following benefits and protections:

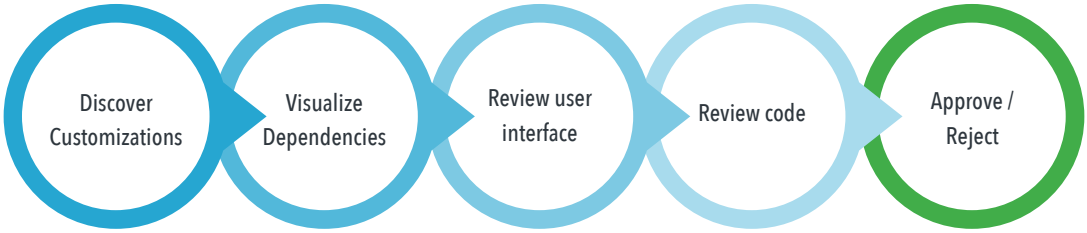
Building a solution that uses out-of-the-box components ensures that you live within the core platform's framework, which makes the task of support and management much easier long-term.

Security Risks of Server-Side Customizations

Over the years, many organizations have spent time and effort in customizing applications on-premises often to meet a perceived or valid business need. For example, as I have performed audits within many SharePoint environments, custom code is deployed that has either been developed by a 3rd Party, an in-house team, or by someone giving away the solution for free. In fact, I am surprised when organizations that are risk-and-security-adverse deploy lots of custom code that has not been thoroughly reviewed and vetted.
During an interview with Tobias Zimmergren from Rencore, who is a Product owner of their Cloud Analysis tool, he stated *"Organizations need to understand their customization. They should 'Know their code' and 'Know what it does'. From our analysis tools, we can see that organizations are aware of the customization they have but not what it really does, as that would require more time and effort".* The real risk is to just accept the code for what it is and deploy with no checks.

> Know your customizations, get an inventory. Understand what the customization is doing.
>
> 

Tobias further recommends the following approach:



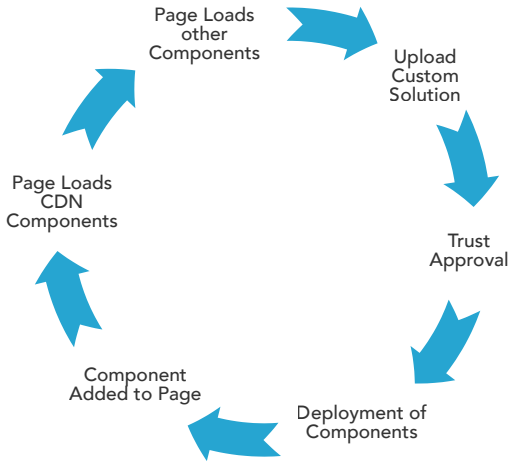
Security Risks of Server-Side Customizations (continued)

Discovering any customizations will allow you to see what has been installed, and more importantly, when and by whom. Next, visualizing the dependencies of the customization will help you understand how it interacts with other systems. From there, the user interface is the entry point for all users, and should be checked and validated to ensure it is not performing an action that should not be performed. The final step should be to review the code, using automated tools or developers to validate exactly what the code is doing, if the code could potentially cause components to fail or simply just not work as expected. Finally, the Approve or Reject step, is exactly that. Rejecting a component does not mean a feature or function will never be on the platform, it simply means that the tests were done and it did not meet the security requirements necessary to be implemented.

Security Risks of Client-Side Customizations

The development stack for Office 365 and SharePoint is now based on modern web technologies, which really is focused on JavaScript. This changes the development type from server-side to client-side code. The code that is developed is isolated to calling existing platform API's that are available, as well as only interacting with the stack through client-side coding.

Though this design seems to limit most of the customization issues, it does raise other security problems. This main issue comes down to the contextual loading of the client-side and what it ultimately has access to during the loading. Microsoft did add some protections, which provided the consent framework, for an IT Administrator to 'Trust' the solution and code that is being deployed. However, after the approval, unless the code has been checked, malicious code could be loaded. The cycle of using a client-side solution is outlined below:



During this cycle, the solution could call out to a potentially malicious script that is not hosted within the core Office 365 Content Delivery Network (CDN). This alone would open the Office 365 site collection and sites and the associated API's to malicious use, as well as data exposure.

Client-side code in any form can perform actions that can have an impact on the system, as well as access other components that it should not. For example, many of the modern applications built today use RESTful API layers to retrieve data, often utilizing the take authentication token, which provides a way to get content and data easily. Too often, the core components are written to accommodate all users by running in context of the current user, allowing the code to easily retrieve all data, inadvertently allowing a malicious component to take that data and transmit it somewhere else, and the user would not realize what was happening.

Unfortunately for Security teams, the ability to build customizations within the Microsoft Cloud has become easy, and now the 'Rise of the Citizen Developer' could potentially cause more problems as customizations are built directly on-top of the stack, without proper checks and balances.

With the rise of citizen developers, greater capabilities can be built–but the risk becomes even greater.

Security for the Masses within the Microsoft Cloud

The Microsoft Cloud has grown over time, and as such, new features, components, and services have been added. Microsoft continues to innovate often, adding new security services to all of its cloud services. As a company, Microsoft was not always known for its security, more specifically related to its Operating System, but this image has now been shaken with these services. For example, the security features now available in the Windows Operating System are as rich and secure as many of the 3rd Party applications that organizations used to need and install within Windows. The Microsoft Cloud is backed by the Microsoft Security Response Center (MSRC), providing real-time intelligence on worldwide security threats. Microsoft also has dedicated teams within each product that ensure that each is adhering to security guidelines.

Microsoft is committed to building more secure software, monitoring and responding to threats as they emerge, and helping others harden their defenses against malicious attacks. The MSRC delivers experience, expertise, and dedication to drive Microsoft's industry-leading, worldwide security response.
This is achieved through the following activities and services:

https://www.microsoft.com/en-US/security/default.aspx

Security for the Masses within the Microsoft Cloud

The benefit to any organization is that Microsoft provides services both within the Microsoft Azure Cloud and Office 365. These services are connected as-needed and can be used in conjunction with each other. Microsoft provides protections for these four pillars across its services:

Each service has its own offerings, but when combined, you get a more powerful security platform.

Core Microsoft Cloud Security Features – Azure

Microsoft core cloud services reside within their Azure Services. As such, most security features are stored within that service, as well as connected to other components, such as Office 365.

Azure Active Directory Premium Services

Azure Active Directory is a comprehensive, highly available identity and access management cloud solution that combines core directory services, advanced identity governance, and application access management. Azure Active Directory also offers a rich, standards-based platform that enables developers to deliver access control to their applications, based on centralized policy and rules.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. The four core features are:

1. **Understand security state across on-premises and cloud workloads**
2. **Find vulnerabilities and remediate quickly**
3. **Limit your exposure to threats**
4. **Detect and respond swiftly to attacks**

This service allows any organization to view and take action on potential security risks across all organizational workloads, whether discovering and adding new Azure resources, or applying consistent security policies across all systems, whether on-prem, hybrid, or cloud, to ensure that compliance standards are being met.

Azure Rights Management Services

Microsoft Azure Rights Management provides a comprehensive policy-based enterprise solution to help protect your valuable information, no matter whom you share it with. Information Rights Management capabilities such as Do Not Forward and Company Confidential, as well as Office 365 Message Encryption, which allows you send encrypted emails to anyone.

Azure Multi-Factor Services

Azure Multi-Factor Authentication helps safeguard access to data and applications. Multi-Factor Authentication helps protect any organization with security monitoring and machine-learning-based reports that identify inconsistent sign-in patterns. To help mitigate potential threats, real-time alerts can notify an IT department of suspicious account credentials.

Advanced Threat Protection

Azure Advanced Threat Protection (ATP) helps protect your enterprise hybrid environments from multiple types of advanced targeted cyber-attacks and insider threats. Azure Advanced Threat Protection technology detects multiple suspicious activities, focusing on several phases of the cyber-attack kill chain including:

1. **Reconnaissance, during which attackers gather information on how the environment is built, what the different assets are, and which entities exist. They generally building their plan for the next phases of the attack.**
2. **Lateral movement cycle, during which an attacker invests time and effort in spreading their attack surface inside your network.**
3. **Domain dominance (persistence), during which an attacker captures the information allowing them to resume their campaign using various sets of entry points, credentials, and techniques.**

Azure Advanced Threat Protection searches for three main types of attacks:

Core Microsoft Cloud Security Features – Office 365

Office 365 as a service, can utilize the security features that reside within Azure. However, it also has its own services and components that specifically control and protect Office 365. These services are accessed through the Security and Compliance Center:

Alerts

Activity alerts can be configured, which will then send email notifications to yourself or other administrators when users perform specific activities in Office 365. Activity alerts are like searching the Office 365 audit log for events, except that you'll be sent an email message when an event that you've created an alert for occurs.

Classifications

Most organizations have different types of content that require different actions taken on them to comply with industry regulations and internal policies. Using labels in Office 365 can help you take the right actions on the right content. With labels, you can classify data across your organization for governance, and enforce retention rules based on that classification.

Reporting

No solution would be useful to an organization if reporting was disabled and unavailable. Office 365 contains reports at all levels of the platform, and within each workload or service. These reports include the following:

- **Data Loss Prevention matches**
- **Data Loss Prevention false positives**
- **Advanced Threat Protection file types**
- **Advanced Threat Protection message disposition**
- **Threat protection status**
- **Malware Detections**
- **Top Malware**
- **Top Senders and Recipients**
- **Spoof Mail**
- **Spam Detections**
- **Sent and Received email**
- **Supervision**

Some of these require other licenses to be available within the Office 365 tenant to work. However, most of them can be viewed either directly in the service, or within the Security and Compliance Center.

Threat Management

In today's digital infrastructure, organizations need to understand common threats, as well what is potentially happening to their systems at any point in time. Threat Management features with the Security and Compliance Center allow for not only certain configurations to mitigate threats, but it also provides a dashboard to instantly see the threat landscape across the organization. The dashboard provides the following information:

- **Weekly threat detections for your tenant**
- **Malware families detected**
- **Malware trends**
- **Catch rate**
- **Security trends**
- **Alert policies you have created**
- **The origin of messages containing malware**
- **Top targeted users within your organization**
- **Global weekly threat detections**

Utilizing Advanced Threat Protection (ATP) combined with information from Microsoft's own Cyber Security division, organizations can become well informed.

Search & Investigation

One of the problems with moving to the cloud is that when issues or problems arise, organizations cannot just log into a server and check the logs. This makes issue resolution complicated and digital forensics almost impossible in the event of a breach. Microsoft, however, has implemented an audit capability, wrapped around its own telemetry solution, that allows organizations to see actions and events taken by both end users and administrators.

The audit log search allows organizations to retrieve historical data of events that took place within any service of Office 365.

Data Loss Prevention

There is a need for most organizations to comply with business standard or industry regulations. Organizations need to protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII), such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy in the Office 365 Security and Compliance Center, you can identify, monitor, and automatically protect sensitive information across Office 365.

By using DLP, organizations can achieve the following:

- **Identify sensitive information across many locations, such as Exchange Online, SharePoint Online, and OneDrive for Business.**
- **Prevent the accidental sharing of sensitive information.**
- **Monitor and protect sensitive information in the desktop versions of Excel 2016, PowerPoint 2016, and Word 2016.**
- **Help users learn how to stay compliant without interrupting their workflow.**
- **View DLP reports showing content that matches your organization's DLP policies.**

These components will not resolve every security issue or risk that an organization may experience, but they are the foundation to a good security posture. The key is to ensure each service and component that can be enabled within the scope of current licensing have the relevant security options turned on, and then to conduct a review of any additional add-on services and components to implement the deeper and more powerful security features.

How the General Data Protection Regulation (GDPR) can Help

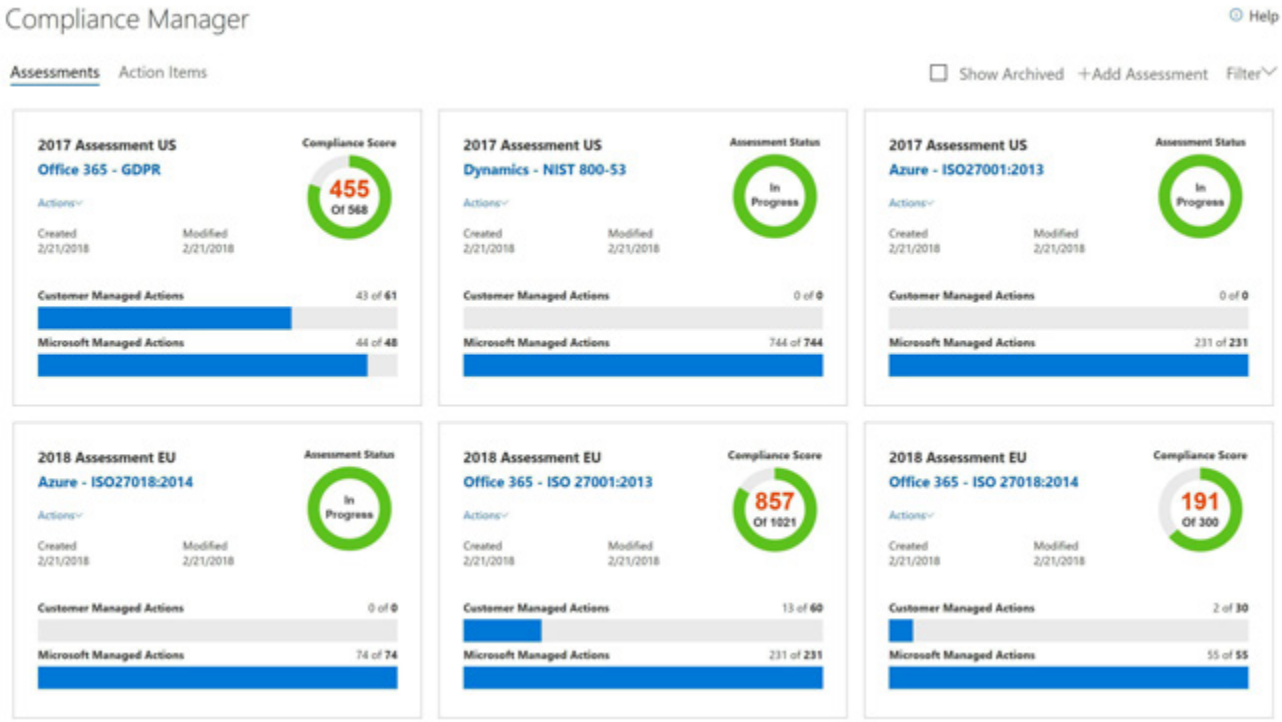
In May 2018, the new General Data Protection Regulations (GDPR) will go into effect. These rulings are about the protection of personal data and an individual's right to privacy. The overarching goal is to better protect the individual's data by assigning a risk level to each data type, and provide security controls and policies that can be used to ensure compliance.

For most organizations, this can make the management of data very complicated due to the specifics within GDPR – but as of May 2018, these rules will be required when tracking or storing data on an citizen within the EU, with protections to be enforced through monetary fines.

Organizations must now manage, control, and implement the following, as required:

- **Understand where "Legitimate Interest" should or should not be used**
- **Provide a mechanism for consent of data use**
- **Provide a notification process, to update individuals of how their data is used**
- **Implement solutions to protect and control the data**
- **Evaluate all personal data, provided updates to individuals of when their data is profiled**
- **Ensure any legacy (existing) data has relevant protections, policies and procedures in place**

As with all organizations, cloud providers like Microsoft must also comply with the GDPR rulings. They have documented their process and learning, and created tools that can help you as an organization to become compliant.



Microsoft's Compliance Manager tool allows any organizations to meet Office 365 GDPR standards by completing various tasks. This is achieved by Microsoft outlining the controls that they are responsible for, and then providing a list of what needs to be completed by the organization.

Using Data Governance to Implement Security Controls

The best approach to implementing security controls within Office 365 is to use a governance process. This comes down to looking at the risk value of the data and content, and then providing a mechanism to protect and control. It is not enough to focus on the products or services a company provides. Companies must create and implement effective procedures for information privacy and security risk management. Companies should employ a layered security approach, or what is commonly called 'security in depth.' This can include perimeter security, intrusion detection systems, egression device monitoring, and the like. With this layered approach, when a single security element fails, there are several others in place to prevent, if not mitigate, the resulting harm. Many companies ignore this approach and relegate information security to an insignificant voice in any debate concerning the best use of company resources. Even for those companies that adopt security in-depth, there is an overreliance on technology. The business leaders may think of data security like infrastructure, attempting to make it work at the lowest cost, but this approach rarely provides the necessary protections for the most critical assets.

When a breach occurs, regulators and law enforcement will have an easier time understanding a company's efforts to properly assess and manage risks to information with written policy and supporting procedures in place. This is especially true in regulated sectors such as healthcare, financial services, and with publicly-held organizations. After a breach occurs, a company's ability to demonstrate that it has current and substantial policies and procedures may help to mitigate, to some degree, potential liability – if the standards and procedures were followed. However, organizations must grasp the idea that written policies are not an end, but only a means to information security.

A data governance plan is a living, documented set of guidelines for ensuring the proper management of a company's digital information. Without a written expression of a company's expectations, including how it will collect, store, and use personally identifiable information, a company cannot reasonably expect its employees and business partners to likewise meet those expectations.

Securing your Business Data using Microsoft Cloud Services

Microsoft's Cloud offerings are built with security features enabled, albeit the core ones that are needed. The underlying data center and network design also provide complex security controls that are enabled by default. Microsoft has ensured that all underlying applications, as well as all modern built applications are done using a security-aware process.

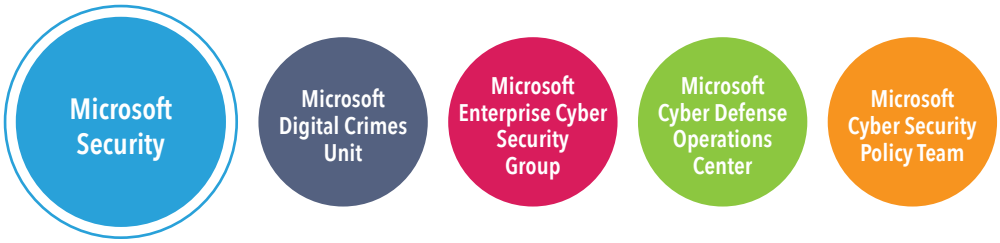
There are seven key areas of investment for security within the Microsoft Cloud, they are:

1. *Auditing and Logging*

Auditing and logging of security-related events, and related alerts, are important components in an effective data protection strategy. Security logs and reports provide you with an electronic record of suspicious activities and help you detect patterns that may indicate attempted or successful external penetration of the network, as well as internal attacks. You can use auditing to monitor user activity, document regulatory compliance, perform forensic analysis, and more. Alerts provide immediate notification when security events occur.

2. *Cyber-Crime*

Like all technical advances, the storage of data and applications in the cloud has attracted an entire criminal ecosystem, from individual hackers to highly organized groups that aim to take down entire networks. Because most companies rely on a third party to administer their cloud services, it's critical that companies that provide cloud services, like Microsoft, are committed to, and capable of, fighting cyber-crime.



The Microsoft Digital Crimes Unit (DCU) mission is to provide a safer digital experience for individuals and organizations worldwide by helping to protect vulnerable populations, fight malware, and reduce digital risk.

The Microsoft Enterprise Cyber Security Group is a team of world-class architects, consultants, and engineers that works with organizations to help move them to the cloud more securely, modernize their IT platforms, and avoid and mitigate breaches.

The Microsoft Cyber Defense Operations Center is a state-of-the-art facility that brings together security response experts from across the company to help protect, detect, and respond to cyber-threats in real-time–all day, every day.

The Microsoft Cyber-Security Policy Team partners with governments and policymakers around the world, blending technical acumen with legal and policy expertise. By identifying strategic issues, assessing the impacts of policies and regulations, leading by example, and driving groundbreaking research, the Cyber-Security Policy team helps promote a more secure online environment.

3. *Design and Operational Security*

Microsoft cloud services and software are built on the same trustworthy technology foundation that applies to all products and services. Microsoft designs its services and software with security in mind to help ensure that its cloud infrastructure is resilient and defended from attacks.

The guiding principle of the Microsoft security strategy is to "assume breach." The global incident response team works continuously to mitigate the effects of any attacks against Microsoft cloud services. These practices are backed by security "centers of excellence" that fight digital crime, combat malware, and respond to security incidents and vulnerabilities in their software and services.

4. *Encryption*

Microsoft business cloud services and products use encryption to safeguard customer data and help you maintain control over it. Encrypting your information renders it unreadable to unauthorized persons, even if they break through your firewalls, infiltrate your network, get physical access to your devices, or bypass the permissions on your local machine. Encryption transforms data so that only someone with the decryption key can access it.

5. *Identity and Access Management*

Securing systems, applications, and data begins with identity-based access controls. The identity and access management features that are built into Microsoft business products and services help protect your organizational and personal information from unauthorized access while making it available to legitimate users whenever and wherever they need it.

These features enable you to manage user identities, credentials, and access rights from creation through retirement, and help automate and centralize the identity lifecycle processes. Microsoft goes beyond the username and password model to provide stronger authentication, while making security more convenient for users with simplified processes and single sign-on (SSO). Robust tools make it easier for administrators to manage identity, and developers to build policy-based identity management into their apps.

6. *Network Security*

Protecting the security and confidentiality of network traffic, whether in the cloud or on-premises, is a critical part of any data protection strategy. Securing the network infrastructure helps prevent attacks, block malware, and protect your data from unauthorized access, interrupted access, or loss.

In the public cloud, the isolation of customer infrastructure is fundamental to maintaining security. Microsoft Azure, on which most Microsoft business cloud services are built, accomplishes this primarily through a distributed virtual firewall, partitioned local area networks (LANs), and physical separation of back-end servers from public-facing interfaces. Customers can deploy multiple logically isolated private networks, and each virtual network is isolated from the other virtual networks.

7. *Threat Management*

Threat management includes protection from both malicious software and attacks against systems and networks. Microsoft products and services have built-in protection features to help defend your data against malware and other types of threats.

Microsoft cloud services help you protect against malware threats in multiple ways. Microsoft Anti-Malware is built for the cloud, and additional antimalware protections are provided in specific services. Denial-of-service (DoS) attacks can deny access to important resources and result in lost productivity, so Microsoft builds its services to defend against such attacks. Windows server and client operating systems include multiple technologies for protecting against these threats at the local level.

You may think that with these areas of control, management and investment by Microsoft, that you are protected within the Microsoft Cloud. Though that may be true to some degree, it is does not guarantee 100% protection. There is still a need for you as the organization to configure, enable and implement the controls and components needed. There are so many features that can be enabled within the Microsoft Cloud, and specifically Office 365.

The core six that will give any organization the base protection needed are as following:

- **Multi-factor Authentication**
- **Mobile Device Management or In-tune**
- **Advanced Threat Protection**
- **Encrypted Email with Data Loss Prevention**
- **Azure Identity Protection**
- **Privileged Identity Management**

Not all these features are enabled in every Office 365 license SKU, so organizations may need to purchase extra services to become as secure as is needed. In fact, one of the findings in the survey, was that some respondents found it unfair that better security features were only available within the more expensive licenses. They felt that this limited them to what could be enabled and the level of protection they could achieve.

> Necessary security features are not part of the standard configuration.

About the Author

Liam Cleary (@helloitsliam) is a Solution Architect for Protiviti in Virginia. His core focus is to ensure that SharePoint can either natively or with minimal customization meet the business requirement. He is also an eleven-time Microsoft MVP focusing on Architecture but also crosses the boundary into Development. His specialty over the past few years has been security in SharePoint and its surrounding platforms. He can often be found at user groups or conferences speaking, offering advice, spending time in the community, teaching his kids how to code, raspberry PI programming, hacking the planet or building Lego robots.

About CollabTalk

CollabTalk is an independent research and technical marketing services company, focused almost entirely on the Microsoft ecosystem. CollabTalk conducts independent research and analysis following our community-focused methodology, and in partnership with the Marriott School of Management at Brigham Young University (BYU). We take a collaborative approach to everything we do, augmenting our capabilities with a deep network of partners and community influencers. www.CollabTalk.com

Research Sponsors

Microsoft develops, manufactures, licenses, supports and sells computer software, consumer electronics, personal computers, and services. Our mission is to empower every person and every organization on the planet to achieve more.
www.microsoft.com

AvePoint accelerates your digital transformation success. Over 16,000 companies and 6 million SharePoint and Office 365 users worldwide trust AvePoint software and services for their data migration, management, and protection needs in the cloud, on-premises and hybrid environments. AvePoint is a Microsoft Global ISV Partner and four-time Microsoft Partner of the Year Award winner.
www.avepoint.com

Rencore is a software company providing industry-leading solutions essential to successfully operating SharePoint on-premises and online and successfully migrating to the cloud. To achieve this, we focus on the three pillars of a healthy SharePoint environment: Governance, Transformation and Risk Prevention.
www.rencore.com

Solliance is an alliance of top experts from across the industry, leveraging partners to put together a team that can handle everything from project inception to product delivery, including architecture, project management, coding, testing, infrastructure management, security and operations.
www.solliance.net

tyGraph provides intelligent tools for better collaboration.
www.tygraph.com

A leading SharePoint, Office 365, and Azure conference with events in Seattle, DC, and Chicago.
www.sharepointfest.com

The authoritative, independent voice of the Microsoft IT community.
www.redmondmag.com

A network of online sites designed to serve the Office 365 community.
www.collab365.community