Office 365 reduces threats, and enhances visibility and compliance

Microsoft IT is taking advantage of new capabilities in Office 365 Enterprise E5 and the Microsoft security platform. They deliver compelling results and value when it comes to visibility and events, zero-day threat reductions, and data discovery and compliance. Office 365 Enterprise E5 fits into our Microsoft IT platform security strategy—it helps keep our assets safe. With its new intelligence features, we can quickly raise the visibility of anomalies and events, get ahead of security threats and protect against zero-day attacks, and protect our corporate IP. We use its in-place intelligent eDiscovery and Advanced eDiscovery features to help us efficiently and quickly find what's most relevant for discovery purposes. We're using all of these capabilities to help our businesses to transform.

Security challenges

The headlines are familiar: "Millions of compromised data records," "hundreds of days between infiltration and detection," and "an average cost to a business of $3,000,000 per breach." There's no doubt that IT is challenged by needing to keep people safe, while at the same time empowering businesses and people to take risks and grasp new opportunities. IT faces very turbulent times in protecting corporate assets. Here are some common enterprise challenges:

- Keep your users safe, but aggressively drive your business forward.
- Protect, protect, and protect even more—to keep exploding amounts of corporate data safe against increasingly sophisticated advanced threats.
- Manage both the risks and the costs associated with data required for compliance and legal issues.
- Be ready to respond quickly to regulatory requests, internal investigations, and discovery requests for litigation.

Security at Microsoft

At Microsoft, we've always managed security as a centralized IT service. Identity is at its core. We provide our users with a single—hybrid—sign-in credential for multi-factor authentication. The credential works across both cloud and on-premises assets. This straightforward approach provides limited persistent administration rights, and works well with policy controls.

We protect with identity, devices, and apps and data. Our IT teams must balance user convenience and data security. Bring Your Own Device (BYOD) is a reality—our employees use the device of their choice. Microsoft IT uses the Enterprise Mobility Suite, Microsoft Intune, and other Microsoft Azure services to manage identity, devices, and applications.

Our focus on apps and data has expanded from infrastructure to include the behavior of our employees. We categorize data based on the sensitivity to the business and our customers. We also pursue pervasive encryption, including data at rest, data in motion, keys, certificates, and secrets. Like many other organizations, our Finance group depends on Microsoft IT to manage risk and keep our highly sensitive data safe.

We've seen new data security threats occur with greater frequency—and they're more and more sophisticated. The negative effects of these breaches can't be denied as they play out across our industry.

Protect, detect, and respond

Microsoft has made some changes in emphasis to its overall security posture. The core elements—which have not changed—are to:

- **Protect** the enterprise across all devices, in all environments, anywhere in the world.
- **Detect** threats using targeted signals, behavioral monitoring, and machine learning.
- **Respond** quickly, closing the gap between discovery and action.

In our journey to the cloud, we've continued to emphasize the concept of *assume breach*. Traditionally, a large proportion of our resources were dedicated to preventive activities, such as application security, network segmentation, and host hardening. As we move to the cloud we have increased our investment in detection and response activities, using advanced intelligence capabilities—provided by Office 365—as part of our overall security strategy.

Security and Office 365 Enterprise E5

The estimated cost of cybercrime to the global economy is $500 billion. The number of security threats increases exponentially every year. Without a doubt, IT needs visibility and control over what our users are doing in Office 365 apps and services.

We focus on security and our secure and trusted technologies—using Office 365 Enterprise E5 capabilities—to create a digital-driven enterprise, and to help us compensate for decreasing levels of IT applications and support that are inherent in a cloud-based environment. Here's a quick look at some of the new security capabilities that we're using, and how they bring value to Microsoft:

- **Enhanced control and discovery.** We monitor Office 365 usage and the cloud services that our users connect to—this helps us to identify anomalies and potentially risky behavior.
- **Safeguarding against threats.** We address zero-day threats and malware in attachments and unsafe links, to detect and remediate breaches in real time.
- **Intelligent data discovery.** We take advantage of machine learning and automated de-duplication to streamline the delivery of unique and relevant content for discovery purposes.

Advanced Security Management

Advanced Security Management capabilities in Office 365 Enterprise E5 give enhanced visibility and control over the service. They surface anomalies, and provide a better window into Office 365 and shadow IT consumption.

At a high level, Advanced Security Management provides:

- **Threat detection.** Using Microsoft threat intelligence and machine learning, it identifies high-risk and abnormal usage, security incidents, and threats.
- **Enhanced control.** Leveraging granular controls and security policies to shape the Office 365 environment, it helps stop questionable activities, and lower risk.
- **Discovery and insights.** Without installing an endpoint agent, it generates enhanced visibility into Office 365 consumption and shadow IT.

Threat detection

Advanced Security Management provides robust policy and threat alerting through anomaly detection policies for Office 365. Anomalies are detected by understanding user activity and evaluating its risk. Additionally, behavioral analytics help assess risk. It learns how the user interacts with Office 365 on a daily basis. With the baseline it creates

when you enable the service, it can then detect suspicious user activity, and assign a risk score to help you if you decide to take further action.

Advanced Security Management benefits from the vast amount of threat intelligence information that Microsoft has. Microsoft has deep insights into the threat landscape—informed by trillions of signals from billions of sources—and is uniquely positioned to better protect organizations and their data.

Enhanced control

Advanced Security Management provides enhanced controls through a set of activity alerts, policies, and filters. Customizable policies can track specific activities that you might be interested in. Policies help you see when your users are doing things, such as:

- Downloading a lot of data.
- Failing to sign in multiple times.
- Signing in from a new IP address.

Activity filters help scope the policies to detect specific information such as location, device type, or if a user has administrator rights. Based on activities happening within a specific timeframe, you can create an alert, or follow up directly.

Advanced Security Management generates alerts that make it easy for you to see the activities that you want monitored, and start your investigations. Some alerts—like a user signing in from a new location—might be a non-issue. However, you might want to check to see if the user is accessing sensitive documents, or failing to sign in multiple times. Advanced Security Management gives you the power to drill down and get additional details around what else the user was doing, or the IP address being used, because it might have logged additional activities. If you decide a behavior is risky, you can stop them directly from the alert. If you consider some activities inherently risky, you can configure a policy so that an account is automatically suspended if the activity takes place.

Apps frequently plug in to Office 365. However, users don't always closely read the permissions that an app requests, or they may simply not realize when an app isn't in compliance with their organization's policies. They're just trying to be more productive. To help you get better control, visibility, and context, the app permissions feature gives you a way to see those apps, to know which users are using them, and the permissions they have. Based on this information, you can choose to approve the app or revoke its access to Office 365 for all users.

Discovery and insights

Advanced Security Management helps you discover usage information about Office 365 and other cloud services. This helps resolve shadow IT problems. Advanced Security Management can discover about 1,000 applications. You can determine if shadow IT is happening in your organization, and see details around the top apps in each category. For example, you can see how much data is being sent to cloud storage services, like OneDrive for Business, Box, or Dropbox.

To load the data into the dashboard, all you have to do is upload logs from your network devices, like firewalls or proxies. There is nothing to install on the user endpoints to collect this data, which is an advantage in a BYOD environment.

Cloud App Security for SaaS infrastructure

We've seen that Advanced Security Management—which is powered by Microsoft Cloud App Security—is a powerful management tool for Office 365. At Microsoft, we're managing Office 365—and at the same time, we need to manage critical data across our large, cross-cloud software as a service (SaaS) infrastructure. That's where Cloud App Security comes in.

Cloud App Security gives us the threat discovery and control functions of Advanced Security Management—and it also gives us critical visibility and control into our complex cloud services environment. Cloud App Security is a critical component of the Microsoft security platform. It works with Microsoft identity and security solutions—including

Azure Active Directory, Microsoft Advanced Threat Analytics, and Azure Information Protection—to deliver an innovative approach to SaaS security.

Monitoring at Microsoft

Cloud App Security activity logs immediately revealed detailed information about how our users were consuming Office 365 services. Having activity log data allowed us to change our investigative mechanisms in a powerful way. The signals are invaluable and critical for our security team—and probably yours—to use during security investigations.

The activity log information has reduced our dependency on other product teams. For example, prior to Cloud App Security, if we had an issue with SharePoint Online that we couldn't resolve ourselves, we had to reach out to the SharePoint Online Security team and ask them to help us. Because events are recorded across SharePoint Online, we can now investigate many SharePoint Online issues ourselves.

Cloud App Security activity logs give us rich signal data across Office 365, Exchange Online, and SharePoint Online. The deep integration allows Microsoft IT to investigate security issues across all platforms, at the same time.

Advanced Threat Protection for attachments and links

The vast majority of advanced threats come through email. Preventing those threats in the first place is a top priority. Microsoft IT needed to go beyond traditional technologies to stop advanced threats like zero-day attacks and phishing.

We're using Office 365 Advanced Threat Protection to identify and block potential issues. We're gaining advanced protection against unknown and sophisticated threats in end-user email, attachments, and URLs. By using Advanced Threat Protection, we gain visibility and control over what our employees are doing in Office 365. These features are policy-based and can be applied to specific groups of users.

Safe attachments detect malicious behavior

We use the safe attachments policy in Advanced Threat Protection to protect against advanced zero-day attacks. Documents and other files attached to emails are opened in cordoned-off virtual environments to detect malicious behavior. Machine learning—as well as dynamic and static analysis techniques—further build on known threats, and isolate and destroy the very latest attacks.

The safe attachments policy is cloud-based, so all users are protected when a threat is registered, and the service is constantly learning. The safe attachments policy is a configuration option that is simply turned on, and it gives us a huge benefit of scale. When a threat detection is registered, all users get the benefit in real time.

The safe attachments process adds to our security posture. At Microsoft, we've phased in safe attachments by organization, and noticed no loss in email service.

Safe links protect against malicious URLs

We use the safe links policy to dynamically protect against malicious URLs that are embedded in email messages. It wraps external links in special URLs, and then checks the link destinations for threats before opening them. When a malicious site is detected, it effectively blocks other users from being exposed to the same threat. Similar to the safe attachments policy, it acts like a crowdsourced security function, where all users are protected as the service learns about threats.

The safe links policy allows us to significantly increase our defense against malicious websites—by protecting users on all devices, across all networks.

Click trace provides rich reporting and URL trace capabilities by keeping a record of every user who has clicked on a safe link-wrapped URL. Logs record data such as the users who received the link, the users who clicked, and whether the service blocked the link.

In-place intelligent eDiscovery

To continue to meet legal, business, and regulatory compliance challenges, businesses must be able to keep and protect important information and quickly find what's relevant. Spending days, if not weeks, manually sifting through millions of files to find the small number that are relevant isn't just expensive, it isn't an option.

Office 365 eDiscovery capabilities can help you quickly and cost-effectively locate, identify, and retrieve relevant information— and preserve it in place. No need to move content to a separate archive to store, index, and process. And the Office 365 eDiscovery solution is available globally to use in any locale or situation where you need to respond to legal and compliance needs or to an internal investigation. Complementing Office 365 eDiscovery, Office 365 Advanced eDiscovery analytics creates further efficiencies—threading email conversations, removing duplicates, finding near-duplicates, and identifying themes. This lets us give each reviewer a structured batch of unique files, eliminating redundant effort and saving review time.

Office 365 eDiscovery

When you need to respond to a legal or regulatory information request, the search and analytics tools in Office 365 eDiscovery can cut your costs and streamline your responses. eDiscovery search finds text and metadata in content across all of your Office 365 assets—SharePoint Online, OneDrive for Business, Skype for Business Online, and Exchange Online. Office 365 Advanced eDiscovery further organizes and filters your content. It groups content into categories, removes duplicates, and uses machine learning to filter for relevance, reducing the amount that must be sent to review. You'll find relevant content faster—while keeping your organization's information more secure.

At Microsoft, we know how demanding and complex compliance it can be. As you might imagine, being a large enterprise operating at a global scale, we're subject to many discovery requests every year. Our legal department uses the eDiscovery features of Office 365 to improve the accuracy and usefulness of our discovery results and save time and money.

Before Office 365 eDiscovery was available, we had to manually collect content from various sources. Gathering a large volume of content and loading it into an offline processing tool took time. Then we had to reprocess it. With collection, processing, and remediation, it could take between two and three weeks to give outside counsel the documents they requested. Today, we do most of this work in hours, not days or weeks. We start to export content on the fly and have it ready for counsel to load into their review tool by the end of the day.

When we need to find specific content to respond to discovery requests, we first use eDiscovery search in the Office 365 Security & Compliance Center. We run searches right away, across the relevant Office 365 assets, without requiring the preliminary step of collecting content and moving it to a separate location to index and search.

We also preserve relevant content in place, in Office 365. We associate the relevant content sources with a case that we create in the Security & Compliance Center and then place the content on hold. This hold overrides any other retention policies that might be in force, and preserves the content for the duration of the case. The hold is practically invisible to the people using the sources, so they can continue working on their projects without interruption or loss of productivity.

Advanced eDiscovery

Once we discover potentially relevant content using Office 365 eDiscovery Search, we then use Advanced eDiscovery analytics to thread email conversations, remove duplicates, find near-duplicates, and identify themes. This lets us give each reviewer a structured batch of unique files, eliminating redundant effort and saving review time. In some cases, instead of doing heavy keyword culling, we use the Advanced eDiscovery Relevance feature to identify relevant content. And even if we're using keyword filtering, we always use Advanced eDiscovery to export our content in a format that's immediately usable by our eDiscovery review partner and which requires no reprocessing.

By reducing the amount of manual work required to respond to eDiscovery requests, Office 365 eDiscovery saves our legal department about $4.5 million annually. With eDiscovery search, we typically reduce the amount of content in a case by about 95 percent. However, this still leaves large volumes of data that need to be submitted to the very costly process of legal review. Advanced eDiscovery helps us reduce these costs significantly: we typically see a further

reduction of 30 percent by eliminating duplicate files and grouping near-duplicates, and another 25 percent by consolidating email threads.

Key takeaways

We're taking advantage of new features in Office 365 Enterprise E5 and in our security platform to improve visibility into our Office 365 and SaaS infrastructure. These capabilities go beyond malware to get ahead of zero-day threats and events with policy-based granular controls—and they improve our discovery response process. Advanced Security Management and Cloud App Security give us a clearer view across all of our cloud applications, and let us respond effectively to anomalies, events, and shadow IT. In-place compliance features help us manage ever-increasing amounts of data for discovery purposes—organizing, streamlining, and using machine learning to automatically assign relevance.

For more information

Microsoft IT

microsoft.com/ITShowcase

Office 365 Security & Compliance Center

Learn more about Office 365

Video: Digital Transformation at Microsoft: Achieving more with Office 365