Microsoft uses threat intelligence to protect, detect, and respond to threats

From a global perspective, the amount of data in organizations is ballooning at 50 percent year over year. The number of threats to this data from cyberattacks and data breaches is mushrooming. Cyberincidents cause organizations to lose money, data, productivity, and consumer trust. In 2016 alone, cybercrime resulted in:

- Companies losing a total of $400 billion from damages from hacking
- Companies losing $3.86 million, on average, per breach

When it comes to malware alone, 1 million new pieces of malware are created each day. According to the 2017 Verizon Data Breach Investigations Report, malware accounts for 51 percent of breaches.

It’s clear that organizations worldwide need rapid-fire protection, detection, and response to threats. Yet, on average, more than 99 days pass between infiltration and detection, which is like leaving the front door wide open for over four months. This is why we need threat intelligence.

At Microsoft, we continue to improve our ability to identify, prioritize, and respond to the biggest threats that target our company and customers. Every six months since 2006, we publish the Microsoft Security Intelligence Report. This report has extensive Microsoft research on software vulnerabilities, vulnerability exploits, and threats like malware—along with guidance to help assess risk and protect against threats.

At Microsoft, security is front and center

Part of what enables this defense is threat intelligence. Threat intelligence gathers indicators—or signals—from a breadth and depth of sources to understand the threat landscape. As a security leader, we build on our vast experience as a global enterprise, ongoing study of the threat landscape, broad scale, strength of signal, and visionary thinking to help understand and mitigate the effects of increasingly sophisticated attacks. These include zero-day attacks, targeted phishing campaigns, and other novel attack methods.

We employ threat researchers and analytics systems across our global network to give a timely, actionable view of the threat landscape. We are in a unique position, with billions of data points that shed light on security issues. For example, each month, we gather intelligence by:

- Processing more than 450 billion authentications.
- Scanning and analyzing 400 billion emails for malware and phishing.
- Updating more than one billion Windows devices.
- Building a rich resource from more than 200 cloud and commercial services worldwide.

This intelligence and signal richness is built into products and services like Office 365, Windows, and Azure to let you know that attacks are happening. Many organizations don’t have threat managers, threat analysts, or a threat intelligence framework. To help organizations worldwide use the framework that we have built, we look at questions like:

- What does threat intelligence mean to Microsoft, and why is it vital for the company and for customers?
- How does Microsoft deliver threat intelligence in services like Windows Defender ATP, Exchange Online Protection, and the newly released Office 365 Threat Intelligence?
- How do security analysts in Core Services Engineering and Operations (CSEO) use threat intelligence capabilities in various Microsoft products and services to investigate threats and take action? How does this lead to faster detection and response time, efficient incident analysis, more relevant indicators of compromise, fewer false positives, and other benefits?
Because Microsoft has infused threat intelligence into its technologies, other companies reap the benefits along with their purchase or subscription, even if they don’t have a formal threat program in place.

Why does threat intelligence matter?

Let’s take a closer look at what the concept of threat intelligence means to us and why having this intelligence is important. Given the number of signals, it’s easy to get lost in a sea of noise. It’s crucial to have context to understand which signals are highest priority, why, and what actions to take.

Threat intelligence at Microsoft includes signals inside and outside the company, related to areas shown in Figure 1, like denial of service, malware, or unauthorized data access. With the right context, this intelligence leads to targeted actions—for example, releasing system updates, enforcing security policies like multi-factor authentication, or applying other security measures.

![Figure 1. Examples of the threat intelligence we get](image)

**Threat intelligence gives context, relevance, and priority**

More than just a buzzword, at Microsoft, true threat intelligence goes beyond lists of bad domains or bad hashes. Instead, it provides the necessary context, relevance, and priority—sometimes called enrichment—for people to make faster, better, and more proactive cybersecurity decisions. For example:

- A security analyst who uses threat intelligence to analyze the highest-priority signals, and takes action.
- An information worker who knows to watch for emails with links that appear suspicious and could be a phishing campaign targeting the company. This awareness could, for example, influence the email recipient to be vigilant, avoid opening files or clicking questionable links, and report the email as suspicious.
- An organization that uses threat intelligence to alert employees that a particular email attachment is associated with ransomware that has affected other companies in the same sector.

Enriched intelligence is built into our technologies that are used worldwide. Where does this enrichment come from? Some of it is from threat intelligence producers. Other enrichment is from intelligence about ourselves and the threats we face. Enrichment gives context on threat detections—for example, whether a threat is related to a group that’s involved in corporate espionage, or whether it involves criminals who are trying to steal credit card numbers.

Having this enrichment and context helps us and our customers who are defending against threats know the priority for mitigating threats and identifying next steps. Threat intelligence producers at Microsoft provide relevance and tell why something’s bad, which is just the type of information that security analysts want.
Threat intelligence helps organizations share knowledge

Security concerns aren’t limited to any sector. All organizations need to defend themselves against cyberthreats, making it a core part of their strategies and operations. Visibility and intelligence into threats are crucial for preparedness—for example, knowing the type of attack, who’s being targeted, how often, and the source of attacks. Through threat intelligence, we give organizations and customers visibility, context, and relevance of security events. Having access to—and sharing this knowledge—helps decision makers both inside and outside security teams prioritize actions and reduce risk.

Threat intelligence is built into Microsoft products and services

How do we at Microsoft enable enterprises to take advantage of shared threat intelligence through products and services like Office 365 and Windows Defender ATP—and offer context, relevance, and priority to help people take action?

We gather, produce, and consume threat intelligence in our security ecosystem through:

- The Microsoft Intelligent Security Graph
- The Microsoft Threat Intelligence Center
- Our large customer base
- Intelligence feeds that we generate, as well as from third parties

We integrate the threat intelligence we gather into products and services like:

- Office 365 Threat Intelligence and Office 365 Advanced Threat Protection
- Exchange Online Protection
- Windows Defender Advanced Threat Protection
- Azure Security Center

The Microsoft Intelligent Security Graph

The **Microsoft Intelligent Security Graph** is foundational for embedding security protection in Office 365, Azure, Windows, and other products. The graph will gather signals from the entire ecosystem of Microsoft and industry-leading commercial and consumer services, security monitoring and operations services and products, Windows devices, Azure, and Office Security and Compliance services. It enriches those signals with threat, customer, industry, and operational context. Signals in the graph generate insights and context that are infused into Office 365, Azure, Windows, and other products and services.

By stitching together and correlating these enriched signals, the Intelligent Security Graph can generate a holistic picture of the threat landscape. This, in turn, helps Microsoft and graph-enabled customers detect threats and share real-time intelligence—and drive rapid and systematic response and remediation action.

In fact, the security analysts in our Cyber Defense Operations Center (CDOC)—a facility that unites security response experts from across the company to protect, detect, and respond to threats—use the Intelligent Security Graph. Faster detection is essential. The Intelligent Security Graph enables faster, more comprehensive threat discovery and response.
Microsoft Threat Intelligence Center

The Microsoft Threat Intelligence Center (MSTIC) team—one of the main producers of threat intelligence at Microsoft—collects the threat intelligence that’s infused into products and services. MSTIC aggregates data from sources such as:

- First-party threat intelligence feeds (honeypots, malicious IP addresses, botnets, malware detonation feeds)
- Third-party sources (threat intelligence feeds, reference/lookup data)
- Analysts/human-based observation and intelligence collection

Microsoft and third-party intelligence feeds

Microsoft gets additional visibility into the security landscape by collecting intelligence feeds. These combined feeds supply data about threats and can be matched against the signals provided in Microsoft products and services.

Integration across Windows 10, Azure, Office 365, and other products

Certain cybersecurity threat intelligence data that’s gathered from different sources is processed and enriched by MSTIC, so that there’s ample context and actionable insight for security analysts. Some of this threat intelligence data is then fed into products and services.

Figure 2 shows examples of built-in security protection and threat intelligence across our products and services bundled into Microsoft 365 Enterprise.

<table>
<thead>
<tr>
<th>Microsoft</th>
<th>Windows</th>
<th>Microsoft Azure</th>
<th>Office 365</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Threat Analytics</td>
<td>Windows Trust Boot</td>
<td>Azure Active Directory</td>
<td>Threat Intelligence</td>
</tr>
<tr>
<td>Cloud App Security</td>
<td>Device Guard</td>
<td>Azure Security Center</td>
<td>Advanced Threat Protection</td>
</tr>
<tr>
<td>Intune</td>
<td>Credential Guard</td>
<td>Azure Key Vault</td>
<td>Anti-spam/anti-malware</td>
</tr>
<tr>
<td>Windows Server 2016</td>
<td>Windows Hello</td>
<td>Exchange Online Protection</td>
<td>Message Encryption</td>
</tr>
<tr>
<td>SQL Server 2016</td>
<td>Windows Defender ATP</td>
<td>in Office 365 for blocking email malware and spam.</td>
<td>Customer Lockbox</td>
</tr>
<tr>
<td></td>
<td>Windows Update for Business</td>
<td></td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td></td>
<td>Windows Information Protection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2. Examples of built-in security protection

To list just a few examples, Microsoft builds threat intelligence into products and services like:

- **Advanced Threat Analytics** for identifying and analyzing normal and suspicious user or device behavior.
- **Windows Defender ATP** for zero-day protection against malware in attachments and links.
- **Azure Security Center** for preventing, detecting, and responding to threats related to Azure resources.
- **Exchange Online Protection** in Office 365 for blocking email malware and spam.
- The **Office 365 Security and Compliance Center** for helping to protecting data and managing compliance.
- **Advanced Security Management** in Office 365 Enterprise E5 or as an add-on subscription.
- **Data Loss Prevention in Office 365** for data protection, risk management, and compliance.
- **Office 365 Advanced Threat Protection**, an email filtering service for protecting against advanced threats and for integrating and sharing threat data.

Office 365 Threat Intelligence

With **Office 365 Threat Intelligence**, we’ve empowered our customers to have their own threat intelligence on the cyberthreat landscape. Office 365 Threat Intelligence integrates with other Office 365 security features like Exchange Online Protection and Advanced Threat Protection. Office 365 Threat Intelligence takes advantage of rich
signals from the Microsoft Intelligent Security Graph, giving our customers access to many of the powerful threat intelligence feeds that Microsoft itself uses.

Office 365 Threat Intelligence consists of the threat dashboard, Threat explorer, incidents, and alerts. The threat dashboard, shown in Figure 3, and Threat explorer are available in the Office 365 Security and Compliance Center.

Figure 3. Office 365 Security and Compliance—managing threats

**What Office 365 Threat Intelligence does**

Available to Office 365 Enterprise E5 subscribers, this service:

- Gives insights on advanced threats, malware, phishing, and other attacks for proactive defense.
- Reports on attacks that are happening in the Office 365 ecosystem. It creates insights on what Office 365 blocks, or stops, for instance—based on signals from the broader Microsoft ecosystem—which includes Office, Windows, Azure, and other sources.
- Shows how many threats were detected on a given day, how many messages were scanned, and how many threats were stopped, blocked, or removed.
- Integrates data from 3,500 Microsoft security specialists, who search data to detect advanced threats.

**How Office 365 Threat Intelligence helps organizations**

By using Office 365 Threat Intelligence to protect, detect, and respond to threats, any size organization can:

- Track and respond to today’s most serious threats, in real-time, in one place.
- Retain high-value data, ensure business continuity, and reduce risk.
- Proactively detect advanced attacks before they reach the organization.
- Gain insights from our broad global presence.
- Systematically help protect the organization with dynamic policy recommendations.
- Take action on malware threats in real time.
- Gain visibility into top targeted users.
• Use dashboard components that range from global trends to investigation starting points.

**Office 365 Threat Intelligence has unique features**

Office 365 is one of the biggest enterprise email services and productivity suites in the world. To help protect information and spot patterns in Office 365, Microsoft has built a vast repository of threat intelligence data. Let’s look at some of the capabilities and features in Office 365 Threat Intelligence:

• Threat dashboard—overall view of threats that were detected and handled; can be used to report to business decision makers and other stakeholders.

• Threat explorer—details about threat families, global threats, and links to security analyst reports on malware families that summarize the threat.

With Threat explorer, organizations can see threat families over time, top threats, and top targeted users. Figure 4 gives a sample view of threat families, top threats, and top targeted users in an organization.

![Threat explorer](image)

*Figure 4. Threat explorer—sample view of threat families, top threats, top targeted users*

**Scenario: Office 365 Threat explorer to investigate a malware threat**

Suppose you want to investigate a malware threat. Here are some examples of how you can use Threat explorer:

• Drill down into the history of a threat. You can filter on options like sender email, recipient email, sender IP address, and the detection technology used to stop a threat—for example, whether an email was blocked by Office 365 ATP or through an Exchange Online Protection filter.

• Get information about malware family behavior, a definition of the threat, technical details (with a link to an associated analyst report), global details (to see how a threat has affected the global Office 365 network, specific nations and industries, and your own organization), and advanced analysis (with more details on how the threat is affecting your organization).

• See each instance where a user in an organization got an attachment with a specific malware threat.

• See if an email was caught and blocked before it reached the user or if it was delivered as spam.
Figure 5 shows an example.

**Figure 5. Threat explorer—sample view of recipients, subject, sender, sender IP, and status**

- Also, in Office 365 Security and Compliance Center, you can remediate emails in real time. Use filters to find the email you want to investigate and then create an incident.
- Once you create the incident, there are options to delete the incident, move it to junk, move it to the user inbox, or keep it but delete any attachment.

In addition to the threat dashboard and Threat explorer, Office 365 Threat Intelligence offers real-time alerts, and through its threat intelligence schema, threat intelligence feeds are made available to the Office 365 Management Activity API. This API gives visibility into user, admin, system, and policy actions and events from Office 365 and Azure Active Directory activity logs. The Management Activity API also connects to a wide variety of security information and event management providers so that you have access to most of the data in Office 365 Threat Intelligence. You can use this information in your investigations to help understand and remediate a suspected breach.

**Scenario: Office 365 threat protection to help prevent a malware attack**

This Microsoft Security, Privacy and Compliance blog post has an example of using threat intelligence and threat protection capabilities in Office 365 to help prevent a specific malware attack from occurring—by using the end-to-end Office 365 Threat Protection stack. Features include:

- **Office 365 Exchange Online Protection.** Anti-virus signatures are updated to block the malware attack, based on known file hashes for this malware.
- **Office 365 Advanced Threat Protection.** ATP can catch new variants of a malware attack if email is the vehicle of attack. If new variants are detected in ATP, the anti-virus signatures are updated in Exchange Online Protection. Also, Office 365 ATP works with Windows Defender ATP to help protect users and systems from attacks.
- **Office 365 Threat Intelligence.** Office 365 Threat Intelligence shows emails that were part of a malware campaign. Search for the malware family, if any emails related to the campaign targeted a tenant:
  1. In the Office 365 Security and Compliance Center, under Threat Management, click Threat explorer.
  2. In Threat explorer, search for the malware family.
3. If an instance of this family entered a tenant through Office 365, a graph will display it.

- **Office 365 Advanced Security Management.** Create an activity policy to detect if a user renames, syncs, or uploads multiple files with a suspicious file extension to Office 365. Automatically suspend the user’s account to help stop other encrypted files from being transferred.

Together, the threat intelligence capabilities in Office 365 Threat Intelligence provide insights to help organizations proactively defend against advanced threats, malware, phishing, zero-day attacks, and other attacks.

Now let's look specifically at how the CSEO organization uses threat intelligence to protect, detect, and respond to threats.

**How Microsoft uses threat intelligence in Office 365**

There are both producers and consumers of threat intelligence. As stated earlier, MSTIC is one of the main **producers** at Microsoft. They work with groups in Microsoft to help build threat intelligence data into solutions like Office 365 and Windows Defender.

Within CSEO, we're primarily threat intelligence **consumers.** We analyze signals that we get and do operational response based on analysis. We process more than 15 billion security events on a given day and manage:

- More than 600,000 devices for more than 150,000 users.
- Devices and users in more than 100 countries and regions.

Within Microsoft, the Digital Security and Risk Engineering (DSRE) team was developed to help ensure that all the company’s information and services are protected, secured, and available for appropriate use through innovation and a robust risk prevention framework. Across CSEO and throughout the company, DSRE is continually evolving the security strategy and taking actions to protect our assets and the data of our customers.

The Office 365 security stack provides insights to help organizations—including CSEO and DSRE—proactively defend against advanced threats, malware, phishing, zero-day attacks, and other attacks. For example, CSEO uses technologies in the Office 365 security stack such as:

- Office 365 Advanced Threat Protection
- Exchange Online Protection in Office 365
- Office 365 Threat Intelligence

All of these technologies have threat intelligence built in.

Let’s look at how the CSEO organization uses Office 365 threat protection capabilities to detect, investigate, and remediate threats.

**How Microsoft uses threat intelligence technologies**

We use a combination of threat intelligence technologies and related processes in Office 365 such as:

- Office 365 Advanced Threat Protection for preventing exposure to unknown threats, together with Exchange Online Protection in Office 365 for preventing signature-based malware. Exchange Online Protection handles the large volume of attacks, and Advanced Threat Protection has extra capabilities built on top of Exchange Online Protection to handle the sophistication of certain types of attacks. Both are tightly integrated with Office 365 Threat Intelligence.
- Office 365 Threat Intelligence and Threat explorer in Office 365 Threat Intelligence for gaining better visibility into the cybersecurity landscape and for context and prioritization, which help us investigate and quickly respond to threats.
How Office 365 Advanced Threat Protection and Exchange Online Protection help us

Ninety-nine percent of our mailboxes are in Exchange Online. We use the entire Office 365 email protection suite including Office 365 Advanced Threat Protection and Exchange Online Protection.

Email that contains unsafe attachments and links can carry many advanced threats like zero-day attacks and advanced phishing campaigns. We need to get ahead of these threats for our employees. To proactively defend against the sophistication and volume of attacks, we use Office 365 Advanced Threat Protection and Exchange Online Protection.

Based on the visibility we get, we apply security policies in organizations across Microsoft. We use ATP and EOP to:

- Enable the Safe Links policy, which gives time-of-click protection against malicious URLs. ATP’s Safe Links feature protects anyone who clicks. Malicious links are dynamically blocked while good links can be accessed.
- Enable the Safe Attachments policy. With ATP’s Safe Attachments, potentially malicious files are opened in an isolated environment to see if they’re malicious. Messages and attachments without a known virus/malware signature are routed to the isolated environment, where behavior analysis and machine learning help detect malicious intent. If no suspicious activity is detected, the message is released for mailbox delivery.
- Reporting and tracing. With reporting and message tracing, we investigate messages that have been blocked because of an unknown virus or malware. The URL trace capability helps us track individual malicious links that have been clicked.

How Threat explorer in Office 365 Threat Intelligence is a game-changer for Microsoft

The recently released Threat explorer in Office 365 Threat Intelligence has transformed how MS detects, investigates, and responds to email threats. It gives us insights into top threat families, top sender domains, protection status, and top targeted users.

Core part of our security investigation

Threat explorer has become critical to our security investigations. As we identify related emails, our security team can quickly group them into an incident and take action.

Easier searches for better visibility of issues that are happening and how to tackle them

Before Threat explorer, two teams were engaged to respond to email threats: the Security Operations Center Team and the Email Service Delivery team. The SOC provided the Email Service Delivery team criteria to search across all mailboxes. After going through the search results, malicious emails were identified and asked to be deleted. If only malicious emails were returned, a blocking rule was added to protect against the same threat in the future. If legitimate emails were also returned, the search criteria had to be modified, a new search had to be performed, and the cycle would continue.

This was time consuming because Microsoft has more than 300,000 mailboxes in Exchange Online. Each email had to be searched to see if there was a match.

Threat explorer drastically simplified this process. The SOC can do targeted searches itself and get results back in a fraction of the time. This dramatically reduces the time to investigate an email and take action.

Self-service response for quicker, more efficient actions without having to rely on other teams

Taking action based on the results of an email search is an important step in our email investigations. Malicious emails left in user mailboxes are like ticking time bombs—at any moment, people can open them and fall victim. The faster those emails can be removed or purged, the better.

Before Threat explorer, response actions against email were limited to high-level user roles on the Email Service Delivery team. Now, the ability to take action is integrated directly into the incident pane. Because of Threat explorer, our security analysts can take direct action against emails to rapidly contain threats.

Integrated products, services, and information for quicker investigation and broader visibility

One example of integration is between Windows Defender ATP and Office 365. Let’s look at a scenario. A security analyst investigates a behavioral alert. Windows Defender ATP identifies a malicious file that has come from email. Integration behind the scenes pulls email information from Office 365, including the date of the email, the sender address, the recipient address, and the email subject. For security analysts in large enterprises like ours, having this
information available inside the Windows Defender ATP portal is invaluable and saves minutes or even hours trying to gather it in other ways. Windows Defender ATP charts the activity in the sequence it happened, making it quick to comprehend an action.

Another example of this deep integration appears on the file metadata page in the Windows Defender ATP portal. If any email across the entire enterprise had that file as an attachment, an indicator and a link appears, which allows the analyst to continue investigating in Threat explorer. From there, the analyst can keep investigating to see if other systems are also compromised—using the email as a link between the two systems. This is one of the big integration points between Windows Defender ATP and Threat explorer.

Benefits summary

The threat protection capabilities in Office 365, Office 365 Threat Intelligence, Exchange Online Protection, and Advanced Threat Protection have allowed CSEO to identify, investigate, and respond to attacks better than ever before. We can:

- Get greater visibility into indicators of compromise and the cyberthreat landscape.
- Rapidly identify email threats using Threat explorer and integration with Windows Defender ATP.
- Perform detailed investigations to precisely target the emails, users, and machines that were affected.
- More quickly detect and investigate threats, and respond with greater speed and efficiency to contain threats—in minutes instead of hours or days.
- Respond more precisely to threats because of the increased visibility into indicators of compromise.

What we’ve learned

Here’s a quick summary of some of the lessons we’ve learned about applying threat intelligence:

- **Give analysts as much context as possible around signals to save time and money.** This helps us make sure we give an operator, analyst, or CISO the most context and prioritization that we can. They want to know what to address first and how, with as few resources and impact as possible.
- **Know what your own capabilities are to thwart attacks.** Sometimes people think threat intelligence is only about understanding an attacker. It’s also important to collect information from internal systems and assets in your own organization and to prioritize security events that affect your key services.
- **Know your trade-offs with each security provider you use.** There are many companies that do threat intelligence and provide a feed of indicators that can be matched against email, network traffic, or indicators on the host. The challenges we’ve found are that:
  - They often use automation that doesn’t provide the context needed to understand the priority and relevance to your organization. We don’t know why an indicator is bad because there’s no context.
  - There usually isn’t a confidence-level rating. People report threats, but today’s threats might not be relevant tomorrow. Or there might not be context, which can affect the quality and accuracy of the results. All these factors affect the confidence level and trustworthiness of the threat indicators.

What’s next for Office 365 Threat Intelligence?

Microsoft is constantly enhancing the ability to identify, prioritize, and respond to the biggest threats to the company and to our customers. For Office 365 Threat Intelligence our roadmap includes new capabilities such as:

- Expand threat intelligence across the Office 365 productivity suite, beyond email.
- Give a more proactive understanding of the threat landscape to drive policy recommendations before an incident happens. These recommendations help organizations adjust and update their policies to align with the evolving threat landscape.
- Create alerts from identified patterns for the security team, threat hunters, and high-level analysts to investigate.
- Detect low-prevalence, new, and targeted campaigns; detect anomalies in account usage.
Microsoft uses threat intelligence to protect, detect, and respond to threats

- Create add to block-list capabilities.
- Understand the most vulnerable points or targets within a tenant to enable better and stronger protection.
- Provide further insight into the attacker origin and location.

Summary

Cyberthreats are ongoing, and protection is paramount. Microsoft has built a security and threat intelligence framework based on billions of signals that it gathers. Threat intelligence is infused into products and services like Office 365, Windows, and Exchange Online Protection—with the context, relevance, and prioritization that help people make proactive decisions. Even organizations without threat managers, threat analysts, or a formal threat intelligence program can use the threat intelligence that’s available in many Microsoft products and services to help protect, detect, and respond to cyberincidents that affect software, people, and organizations worldwide.

For more information

Microsoft IT Showcase
microsoft.com/ITShowcase

Office 365

How to use Office 365 threat protection services to help prevent malware attacks

Security intelligence at Microsoft

Learn more about threat intelligence and start a free trial.

© 2018 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.