Microsoft 365 helps create a secure modern workplace

Enterprises in today’s digital world are onboarding more devices and creating, using, and storing more data in cloud-based services than ever. While this shift to the digital realm brings unprecedented opportunities to the business—allowing employees to be more productive—it also carries security risks if not done properly. Cyberthreats are increasing in sophistication, which requires organizations—including Microsoft—to place greater focus on digital security.

At Microsoft, we’re constantly exploring new technologies and processes to help ensure we have the most productive and secure environment for the company and for our customers and partners. Like many large enterprises, we need to ensure that we are implementing security controls that keep pace with the significant increase we’re seeing in mobile data usage, cloud adoption, digitization, and Bring Your Own Devices (BYODs).

This technical case study describes the multifaced approach that Microsoft is taking to create a secure modern workplace. The key is Microsoft 365, our solution of integrated and intelligent components that includes Office 365, Windows 10, and Enterprise Mobility + Security. We’re using Microsoft 365 to enhance digital security in the following four areas:

- Identity protection
- Information protection
- Threat protection
- Security management

We explore how Microsoft Core Services Engineering and Operations (CSEO), formerly Microsoft IT, is addressing each of these areas in the following sections.

Our approach to security

The Microsoft security team implements Microsoft 365 security technologies to help secure the Microsoft enterprise.

Figure 1 below illustrates the array of security components that are available to enterprise Microsoft 365 subscribers. Although we use many of the technologies listed in the wheel, the larger slices are the focus for this case study. For each security area, we describe some of the challenges and concerns we have had, how we’re implementing specific Microsoft 365 technologies to address those issues, and we highlight the benefits we’re gaining by adopting these technologies.
Microsoft 365 technologies and their associated security areas

Figure 1. The four main aspects of digital security and their integrated Microsoft 365 components. The protruding items represent the specific technologies that we have implemented in CSEO and that we discuss in this case study.
Emphasizing identity-based protection

As organizations continue to move applications and data to cloud services, the effectiveness of the network boundary as a security control is diminished. Today, identity authentication and authorization become the primary security control. The verification we used to perform when someone connected to the network must now be done when the user authenticates to a corporate app or service, regardless of the user’s location, network, or device. In this section, we discuss the challenges and concerns that we’ve had with shifting our authentication strategy to identity protection, and then illustrate how we’re using Microsoft 365 technologies with two-factor authentication and Microsoft Windows Hello to address those issues.

Eliminating passwords and improving productivity with Windows Hello

We’ve been working to eliminate passwords for users who can use alternative authentication methods such as two-factor authentication and Windows Hello. Why is password-based protection such a concern? From a security perspective, attackers are becoming more sophisticated and successful at compromising users’ password-based credentials, primarily through phishing attacks. Industry analysts indicate that 90% of security breaches start from a successful phishing campaign. In addition, the high number of passwords required for daily Internet usage results in 24% of password reuse—meaning that one compromised password can provide access to multiple resources.

Windows Hello is one of the key technologies we’ve employed to not only move away from password-based protection but also boost employee productivity. This technology improves identity protection and enables our employees to save time through single sign-on. Windows Hello biometrics and other nonpassword-based authentication features free employees from having to manage an unwieldy array of passwords. Moreover, Windows Hello utilizes two-factor authentication to generate a strong credential that’s safely stored locally on the PC or device; unlike with passwords, nothing is transmitted across the network.

Expanding two-factor authentication options with Microsoft Authenticator

The transition away from a perimeter mindset requires new methods to ensure that people use strong authentication mechanisms. Microsoft Authenticator is a phone-based authentication tool in Microsoft 365 that we have implemented to increase our employees’ authentication options. Available on Windows, Android, and iOS devices, Microsoft Authenticator allows employees running non-Windows and Windows systems alike to enroll their devices so that they can reach corporate resources securely. For example, a person working on a Mac OS system could use Microsoft Authenticator on a Windows, Android, or iOS device as their second authentication factor.

Employing conditional access with Azure Active Directory and Microsoft Intune

As BYOD becomes more prevalent, organizations incur the risk that personal devices might bring security vulnerabilities and exploits with them when employees and other users connect to the cloud. When devices aren’t patched with updated antivirus signatures, they might be running malware that can infect the network at the first opportunity.

Our approach to ensure device health at Microsoft is to utilize Azure Active Directory (Azure AD) in tandem with Microsoft Intune to implement conditional access. Users enroll their devices with Intune (the unified endpoint management solution in Microsoft 365), which applies appropriate policies to ensure that the device is encrypted by using a strong password, is malware free, and is up to date and running the latest security patches. When the user needs to use the device to access a cloud-based corporate resource, Intune communicates the device’s health compliance status to Azure AD as it processes the user’s authentication.

Conditional access enables Microsoft to require a device health certificate when access is requested to company data or applications. This approach helps ensure that access to company data or applications is only granted after Microsoft validates device health and compliance status, in addition to authorized user credentials. By doing so, we prevent compromised or potentially risky systems from gaining access to other devices or company services and spreading viruses or unknowingly granting access to attackers. This automated approach to ensuring healthy devices has greatly simplified and streamlined our device/identity protection processes. We’re also taking advantage of
additional features in Azure AD that enable us to be more proactive with security responses, such as blocking a user ID whose credentials are likely compromised. With devices running Windows 10, we can detect cases where the full system has been compromised—something difficult to detect on earlier versions or third-party platforms.

From a cultural perspective, some employees were concerned about privacy and allowing CSEO to apply policies to personal devices. This highlighted the need to provide education and awareness training on why this is a critical aspect of helping protect our people, devices, and data.

**Identity-based protection guidelines**

- **Continue your move to the cloud.** The more systems and environments that you transition from legacy, on-premises systems to Azure, the more you’ll be able to utilize Azure AD security capabilities—including identity protection. Your challenge might be in securing legacy apps running in on-premises environments that don’t support the latest authentication protocols. In this case, you might be able to secure legacy apps by enforcing conditional access security at the device level. For legacy apps with a web front-end, you can direct them to open in an Intune-protected Edge browser.

- **Implement automated processes to monitor and manage device health.** Transition your manual device management practices to automated systems to help you stay ahead of the wave of BYODs connecting to corporate resources, and to programatically perform device health checks at scale. At Microsoft, using Azure AD and Intune to automatically manage conditional access for all connected devices not only enhances our security but also streamlines operations.

- **Drive cultural change by communicating the importance of securing personal devices.** Requiring that employees enroll their personal devices in Intune to better secure them can pose a cultural challenge. People are concerned about their privacy, but need to understand the potential impact or threat that bringing their unsecured personal devices to work can have—and why it’s therefore so important to secure all devices—corporate and personal—that connect to work-based environments. At Microsoft, we developed a detailed communication plan with support from our leadership to emphasize the rationale for our drive to secure personal devices. By reiterating the reasons why it’s important and by having executive sponsorship to capture employee attention, we were able to rapidly onboard most of our personal devices into our device-management systems.

**Protecting information wherever it goes**

At Microsoft, data is our business’ currency. We recognize the critical importance of protecting our data and our customers’ data wherever it resides, all the time. As with many enterprises, the sheer amount of data can make data protection appear as an insurmountable challenge. In this section, we discuss the challenges and concerns we’ve encountered with information protection, and then illustrate how we’re using Microsoft 365 technologies to address those issues.

**Detecting and monitoring sensitive data with Office 365 Data Loss Prevention**

Microsoft maintains the world’s largest Office 365 tenant for our employees, and it encompasses multiple petabytes of data, with an additional 350 terabytes of data residing in on-premises systems. The enormous amount of data across this hybrid environment presents a huge challenge for data discovery and protection.

Previously, we relied on a combination of third-party products to try to identify and track sensitive data. Those solutions burdened our security administrators with navigating multiple interfaces and screens, and the different systems frequently produced inconsistent findings. Without having a good understanding of the nature of the data, how could we determine the sensitivity of information in each document? How was the sensitive data being stored? Who was accessing it? Where was it going?

We needed to implement a new, holistic data discovery and protection solution that could seamlessly protect data for Microsoft and our customers, partners, and suppliers. Additionally, the proper protection methods—encryption, permissions, or both—needed to be applied instantly.
Office 365 Data Loss Prevention (DLP) is the tool within Microsoft 365 that we chose for our holistic data protection solution. Instead of having to create multiple classifications in each separate third-party system, classifications in Office 365 DLP can be used everywhere in the cloud—in SharePoint Online, OneDrive for Business, Teams, and more. We can even use the same classifications in our on-premises environment via the Azure Information Protection scanner, another technology available in Microsoft 365. This not only helps secure our data better but also increases our security administrators’ productivity by presenting a single integrated interface.

Office 365 DLP gives us insight into the types of content that are stored, where each data item resides, and how people use and share the data. This information is critical to improving our business practices—for example, we can now identify when sensitive information is being transmitted via insecure email attachments. Our Data Loss Prevention team can immediately notify and raise awareness within the affected department and continue monitoring to confirm that appropriate changes to daily practices which enhance data security have been adopted.

**Simplifying and automating data classification with Azure Information Protection**

Another key aspect of data protection is establishing a data classification system that detection and monitoring technologies can utilize to determine how a certain file should be treated, based on its content’s sensitivity. Classification at Microsoft has traditionally been a manual process in which we relied on each employee to correctly label and classify their own work. With many people interpreting our classification system differently, we saw inconsistencies in labeling, misclassification, or no classification at all.

At Microsoft, we needed to ensure that all documents within the enterprise are properly and consistently classified and labeled—and we needed to automatically tag data as much as possible. One important change we made to improve our data classification was to update our classification taxonomy. We worked with representative stakeholders from numerous departments to achieve consensus on what terminology should be used and what terminology all employees would likely understand and adopt. In addition, we’re implementing unified labels to help us integrate labeling across multiple apps and platforms.

We deployed Azure Information Protection across the enterprise to classify and label employee data. Azure Information Protection is a Microsoft Office 365 plug-in. It is implemented and available within the apps that our employees already use. Word, Excel, and other Office 365 productivity tools feature a new toolbar that visually reminds people to label and protect each document.

We’re seeing Azure Information Protection boost employee productivity by automatically classifying sensitive information and recommending appropriate labels based on the types of data being entered. Additionally, our Data Loss Prevention team benefits from Azure information Protection by utilizing the labeling and document properties that Azure Information Protection places in each file to gauge how sensitive content is used and how it’s shared across the enterprise.

**Information protection guidelines**

- **Plan and fine tune classification rules.** When rolling out your initial information protection deployment, make sure to allocate time for reviewing classification rules and verifying classification actions. As with most deployments, we suggest you start with a small population to work out false positives before deploying to a larger number of users. In our experience, we realized that false positives can also help uncover other sensitive data that may not have otherwise been considered. At Microsoft, we believe that a careful, ongoing analysis of false positives is an effective way to improve data detection and monitoring processes. As we iterate on modifications to classifications and rules, we gain more confidence that the changes made are appropriate when we see the number of false positives trend downward. These improved classifications are then applied across the company.

- **Design intuitive data labels.** If you expect multiple departments and regions to all apply your data sensitivity labels frequently and accurately, you must confirm that your terminology makes sense to everyone; otherwise, you’ll have mislabeled data at best or unlabeled data at worst. Achieving labeling consistency was a more significant challenge than the technical implementation. Because this new taxonomy would be applied across all
our departments and regions, we engaged stakeholders from many teams and spent considerable time building a taxonomy that all parties could understand and accurately apply to their data.

• **Don’t be surprised at the number of faulty business processes found during the discovery and validation phases.** If you haven’t previously had a programmatic means to evaluate whether data is being protected in your business processes, it’s not uncommon to discover a variety of faulty business processes, or even a lack of business process or classification. At Microsoft, we view uncovering business practices that don’t adhere to our security practices early in the data life cycle as a good thing, because it presents an opportunity to educate employees on proper data handling and to encourage corrective behavior. Addressing these issues as they’re identified, then continuing to monitor to ensure adherence, should reduce false-positive rates over time—and that is your best evidence that you’re optimally protecting your corporate information.

• **Educate employees on data protection and why it’s important.** To successfully implement data protection in your organization, focus on the cultural change to the same extent that you focus on deploying Office 365 DLP and Azure Information Protection. Design an education and awareness program to teach employees how to properly classify and label content by using the Azure Information Protection capabilities within their familiar Office 365 apps. At Microsoft, we’ve developed education and awareness training programs that help remind our employees about business processes and proper labeling and storage of sensitive content. This proactive approach helps us remove faulty business practices, which in turn reduces the risk of unauthorized disclosures or inadvertent leaks of sensitive content.

### Detecting and responding to attacks more quickly

There are two main areas of threat protection and response: managing events that raise alerts and using analytics to gain visibility into the underlying data. In this section, we discuss the challenges and concerns we’ve encountered with both these aspects of threat protection, and then illustrate how we’re using Microsoft 365 technologies to address them.

It’s becoming all too common to learn that another large enterprise has been victimized by a hacker and that sensitive data has been accessed. The prevalence and scale of these attacks mandate better protection of internal data and customer data—and the ability to swiftly respond to attacks as soon as they occur.

Technologies such as antivirus and antimalware programs are still an important tool, but as attacks increase in complexity, protecting an enterprise from digital security threats requires a more complete toolkit. Although next generation antivirus solutions like Windows Defender ATP can block clearly malicious PowerShell scripts, such solutions are not designed to block or alert on anomalous or potentially suspicious behaviors. It might or might not notice that a process has been injected, or that someone accessed passwords by using routine system commands that are available to the operating system. So how can your security operations personnel (SecOps) notice these things—how do you notice a single process doing something suspicious to the system? And how do you scale that capability to support the hundreds of thousands of devices that are part of an enterprise?

### Automating threat protection with Windows Defender Advanced Threat Protection

At Microsoft, a key technology that we use to protect employees’ systems is **Windows Defender Advanced Threat Protection** (Windows Defender ATP). Windows Defender ATP is a unified Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) suite for Windows and third-party platforms that brings intelligence to preventative and post-breach protection. Its ability to learn, grow, and adapt through machine learning is enabling our security teams to become more proactive with threat response.

Windows Defender ATP performs automated investigation and response, automatically picking alerts out of the queue and then investigating. It incriminates all entities related to an identified threat, and then remediates the issue. If Windows Defender ATP identifies that malicious code has been injected into a process, it sends an alert to the Windows Defender Security Center web console. Windows Defender ATP delivers instant, detailed visibility into what’s going on in the system or over the network, providing context about the nature of the event. We use Windows Defender ATP to look at that compromised system, examine incidents, and then work back to see where they came from.
from. The depth of the data that the technology provides increases the speed of our response to the threat at the exact moment when time is of the essence—which can be the difference between quarantining malware or blocking an intrusion immediately rather than giving it the opportunity to spread across the enterprise.

Protecting email from phishing attacks with Office 365 Advanced Threat Protection

One of the most frequent vectors that malware takes into an organization is through phishing, in which employees inadvertently reveal sensitive information such as usernames, passwords, or credit card details to a hacker who sends an electronic communication (most commonly email) by masquerading as a trustworthy entity.

At Microsoft, we chose Office 365 Advanced Threat Protection (Office 365 ATP) to programatically address phishing and other email-based malware. Part of the Microsoft 365 suite of technologies, Office 365 ATP does much more than filter spam into the junk mailbox; it allows us to review a suspect email’s header, determine who received it, find out whether the recipient clicked any links within the file, and determine whether the message was forwarded to others. We can then either send the message to the junk folder or delete it. Essentially, Office 365 ATP enables us to qualify the severity of the message’s malware and act accordingly.

Gaining synergy with Office 365 ATP and Windows Defender ATP

The largest benefit we’re seeing, however, is the synergistic effect of combining Office 365 ATP with Windows Defender ATP. The tight integration of these technologies means that we can move seamlessly back and forth between them during investigations, which significantly improves our overall malware remediation capabilities while simultaneously reducing our response time.

For example, if we receive a report of a phishing incident, we can use Office 365 ATP to both examine an email’s header and determine what actions any users have taken within the email (such as clicking links or forwarding the message). With the click of a button, we can then connect into Windows Defender ATP for the same user who received the email to determine whether the malware wrote a file to the device or if it led to a network connection to another site.

The synergy between these products enables our team to respond to alerts much more quickly. Instead of sending emails or calling people who might have been impacted by the malware, we now have a greatly simplified means of analyzing a phishing event, determining precisely what happened, and immediately beginning remediation. In this same scenario, we can use Office 365 ATP and Windows Defender ATP to determine, for example, that 60 people received the message, five people opened it, and two people now have malware in their systems. We can delete the phishing message right from the Office 365 ATP console to ensure that people who haven’t seen it never open it. We can then move straight to the user’s infected systems in Windows Defender ATP to quarantine and remove the malware from infected systems—all without disrupting the employee’s productivity.

These integrated technologies also work from the opposite direction as the situation merits. If, for example, an alert is first raised in Windows Defender ATP, we can start our investigation by examining the system that generated the alert, determine how any malware got onto the system, and identify where it came from in an email. Then we can search for instances of that same email file on other systems, and then quarantine and repair all infected systems. Next, we can link back to Office 365 ATP to get a broader picture of how many users received the message and the scope of the phishing attack, and then delete the message from any inboxes where the message hasn’t been opened.

Our response times have reduced dramatically by using these tools. No matter which investigation direction we take—phishing to system, or system to phishing—Office 365 ATP and Windows Defender ATP together give us all the details we need to properly analyze and respond within minutes. This is a significant improvement from processes that previously could take days or weeks to find and respond to the suspicious activity. Having the right information available at our fingertips enables us to respond immediately. We no longer must contact the owners of the affected systems and then wait for them to respond before we start remediation. Furthermore, our analysts can spend more time investigating true threats instead of sifting through insurmountable mounds of log files, searching for suspicious activity.
Threat detection and response guidelines

- **Invest in your platform and your instrumentation so that you can analyze and respond to threats at scale.** Agility and scalability require forward thinking and building platforms that enable next-generation threat protection. Windows Defender ATP and Office 365 ATP give us an integrated platform that improves our ability to analyze an attack while enhancing our remediation capabilities that don’t disrupt employee productivity. These technologies are key to performing effective, programmatic, and timely remediation of malware attacks. With these tools, we can inventory our assets, monitor system and network health, and then take immediate action to quarantine and repair infected systems and delete phishing emails.

- **Invest in your people.** Although Office 365 DLP and Windows Defender ATP are critical tools that your SecOps and analysts can use to better protect your infrastructure, threat protection starts with your employees. Every person in the enterprise has a part to play in helping keep malware at bay. Educate your employees about their important role as part of the new security perimeter—and what they must do to protect themselves and co-workers about digital threats and security risks. At Microsoft, we’re focusing on streamlining the communication between incident response teams and eliminating persistent admin rights in favor of providing access at the right time. We provide training for our employees on security best practices, risks, and reinforce key concepts through communication campaigns that help keep the proper behaviors foremost in employees’ minds.

**Building intelligent security management**

One of the major security challenges that enterprises face is understanding threats in the context of the organization—and what sort of risk each threat poses. Security teams must be able to work with alerts from multiple siloed products to build a coherent picture of their security landscape. In this section, we illustrate how we’re customizing the Microsoft Graph Security API to bring together all our digital security inputs—both Microsoft and third-party solutions—into a single dashboard and how we’re promoting intelligent security management by supporting the organizational context.

**Bringing security management under one dashboard**

Large enterprises commonly use an assemblage of different security products to better protect their infrastructure. Moreover, each product has its own portal, data model, schema, and API. At Microsoft, this combination of Microsoft and third-party products traditionally has been an obstacle to building a holistic view of our security landscape. Although we’ve been using our Intelligent Security Graph to synthesize the threat intelligence and security signals from our Microsoft products, the third-party security tools we used provided no standardized means of integration.

Until recently, we’ve either had to spend significant development resources to custom code and maintain an interface or rely on our security analysts to manage without any integration. In the latter case, moving back and forth between the Microsoft and third-party portals made it much more challenging to obtain a complete situation awareness. We needed a means to extend our reach into third-party security tools and display their information side by side with our Microsoft technologies.

The release of the Microsoft Graph Security API (Security API) has completely changed our integration efforts. The Security API provides a common interface for all Microsoft 365 products—including the security-oriented technologies we’ve introduced previously in this article, and the other, nonsecurity-related products available in Microsoft 365. The Security API offers a single integration point and fabric for any technology in Microsoft 365 and for any third-party tool that supports the Microsoft Graph API.

Onboarding the Security API is delivering a significant supportability boost, because our developers can switch from maintaining brittle custom code to working with an officially supported API. Maintenance becomes part of standard product support. We’re also unifying the work that is currently being done in multiple applications into a single location. By integrating once with the Security API, we can use that same code to reach all the other products that support the API with no additional effort. In effect, one development effort now returns multiple product integrations.
Inserting organizational context into security risk assessment

Another milestone we’ve achieved by utilizing the Security API is merging organizational context with alert data. Joining these two types of information is critical in helping us quickly ascertain the relative risk of the attack in relation to the role of the targeted person. For example, when a security alert activates or a potential attack is detected, we can determine whether the person under attack is an executive of the company or an executive’s administrative assistant. We might need to treat such an incident very differently based on the person being attacked.

We’re able to gather this information because the Security API is part of the Microsoft Graph API and is therefore able to see into both Azure AD and Office 365 when appropriate permissions have been granted to do so. We can pull the user object from Azure AD, see their picture, and identify their manager and their department to determine whether others in the same department have also been targeted. With approval, we can investigate other email-related details that can help us assess the risk level for each attack accurately and quickly—and then respond accordingly.

Security management guidelines

- **Combine security alert data with organizational context.** Combining information about the nature of a malware attack with details about the targeted user will help you understand a breach’s potential scope. Individuals who hold highly confidential corporate information might require a much more significant response than those who don’t. At Microsoft, using the Security API to connect our security processes with Azure AD and Office 365 gives us this critical insight and helps us adjust our method and level of response for each attack.

- **Transition from custom hacks to a production API.** Shift your security developers (DevSec personnel) from custom coding security interfaces to working with the Security API. This should alleviate much of the resource drain associated with maintaining brittle code, and it enables you to multiply the value of each development effort by coding one integration for one product, and then reusing the same code to integrate with any other product that supports the Security API.

- **Recruit your developers’ and SecOps’ brainpower to integrate security practices within DevOps.** The Security API enables you to reduce the cost, effort, and operational risk associated with custom-code solutions. This helps you better use the skill set that your developers already possess, and it enables them to transition to implementing security practices. At Microsoft, we’re using this strategy to scale our DevSecOps team as needed. Those developers who aren’t as familiar with security aspects can work alongside SecOps team members to streamline their efforts.

Conclusions

Data is the lifeblood of a digital enterprise. As companies continue their digital transformation to cloud-based services, more devices are being used to access these resources in a growing number of locations—not just from within a secure corporate network.

The Microsoft security team has implemented several Microsoft 365 security components to make our environment more productive and secure. We’ve shared how we’re enhancing four aspects of our digital security—identity-based protection, information protection, threat protection, and security management—and explained how the technologies are part of the Microsoft 365 landscape.

Implementing the security technologies available in Microsoft 365 has been key to helping our security team adopt a proactive threat-response strategy while simultaneously supporting the productivity needs of our employees and customers. We’re able to better protect the vast number of devices that need access to corporate resources, and we’re also bringing together our device monitoring and management systems under a single dashboard. This holistic approach that connects solutions and integrates them with alerts and contextual information is delivering the insights we need to better block malware from accessing our systems while improving our threat detection and increasing the speed and efficacy of our incident response the moment any breach occurs.
Our next steps

We're well on our journey to becoming a more secure and productive enterprise that effectively anticipates and responds to security-based risks. We will continue to incorporate more Microsoft 365 security technologies and third-party security solutions, effectively bringing all monitoring and management capabilities—irrespective of product or manufacturer—into one interface.

In the next year we plan to complete our adoption of identity-based protection so that our employees are completely free of passwords and use Multi-Factor Authentication to access corporate resources securely. Furthermore, we’re working to ensure that administrator accounts are fully isolated from regular mail-enabled user accounts, and that no server or service has a persistent administrator.

Finally, we’re evolving our use of machine learning and AI to define intelligent, behavioral-based approaches to threat detection that will help us identify and prevent entirely new threats and methods of attack that we haven’t yet encountered—which is a critical step toward helping our company, customers, and partners remain productive and secure well into the future.

Your next steps

If your organization hasn’t already subscribed to Microsoft 365, review the productivity and security technologies available in Microsoft 365 enterprise.

If you’re already using Microsoft 365, use the links below to learn more about how you can use the full suite of security technologies that are available to you in Microsoft 365 to enhance your digital security.

For more information

Microsoft IT Showcase

microsoft.com/itshowcase

Microsoft 365 Enterprise documentation and resources

Security at Microsoft

IT Expert Roundtable: Information protection at Microsoft

Security expert roundtable: advanced threat protection at Microsoft

Microsoft Graph Security API

IT expert roundtable: Microsoft 365 security

© 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.