Microsoft

Understand & improve your security posture

Gain deeper visibility into and control of your security

Assessing your security posture is an ongoing challenge

Increasingly sophisticated threats mean that organizations must constantly reassess their security

Security posture refers to the current state of an organization's security—that is, its overall fitness to protect its identities, endpoints, user data, apps and infrastructure. An organization's security posture is not static: it changes constantly in response to emerging new threats and variabilities in the environment. Enabling protections, like multi-factor authentication (MFA) for administrators, strengthens a company's posture. A lack of vigilance, such as failing to update endpoints or use available protections can weaken an organizations security posture.

A major challenge to improving an organization's security posture is its ability to accurately and objectively measure it. It takes considerable time for corporations to compare their security configurations to best practices, known risks, and other organizations in the industry—and that's if the data is available, which isn't guaranteed. Furthermore, for a security assessment to be useful, organizations must assess their security continuously and track results over time.

IT security teams are under constant pressure to improve their organization's security posture. This pressure is steadily growing as IT security becomes a more frequent C-suite topic and senior leaders are held responsible for data breaches that erode customer trust and cause stock prices to plummet.

Progressive chief information security officers (CISOs) are looking to their security providers to help quantify their security posture, provide recommendations for improving it, offer guidance on the level of effort required, and estimate the user impact. This data helps enterprises determine how they will invest in security and set reasonable expectations for their return on investment (ROI).

Communicate your organization's security posture effectively

Meet Evan

Evan is the CISO of a large organization called Contoso, and he continuously worries over its security posture. Does he have a clear picture of the company's posture, or has he left a key attack vector vulnerable? Does his board of directors understand why he needs a larger budget for the next fiscal year? Is his security road map going to strengthen the company's security? What else is he missing?

A lot is riding on Evan's ability to understand and improve Contoso's security posture. He must explain the organization's security standing to other executives to justify his budget and show a return on the time and money spent. In the event of a breach, the company is liable, so Evan must produce reports to explain these instances to the board of directors.

Producing the quarterly security briefing for the company's executives takes a lot of time. His team pulls reports from each system, and then Evan spends the first week of every month merging them into a single view. From there, he reviews the data and provides a top-line assessment and recommendations for improvement. However, he struggles to objectively quantify the results without the ability to compare them with similar companies.

Evan

Chief Information Security Officer

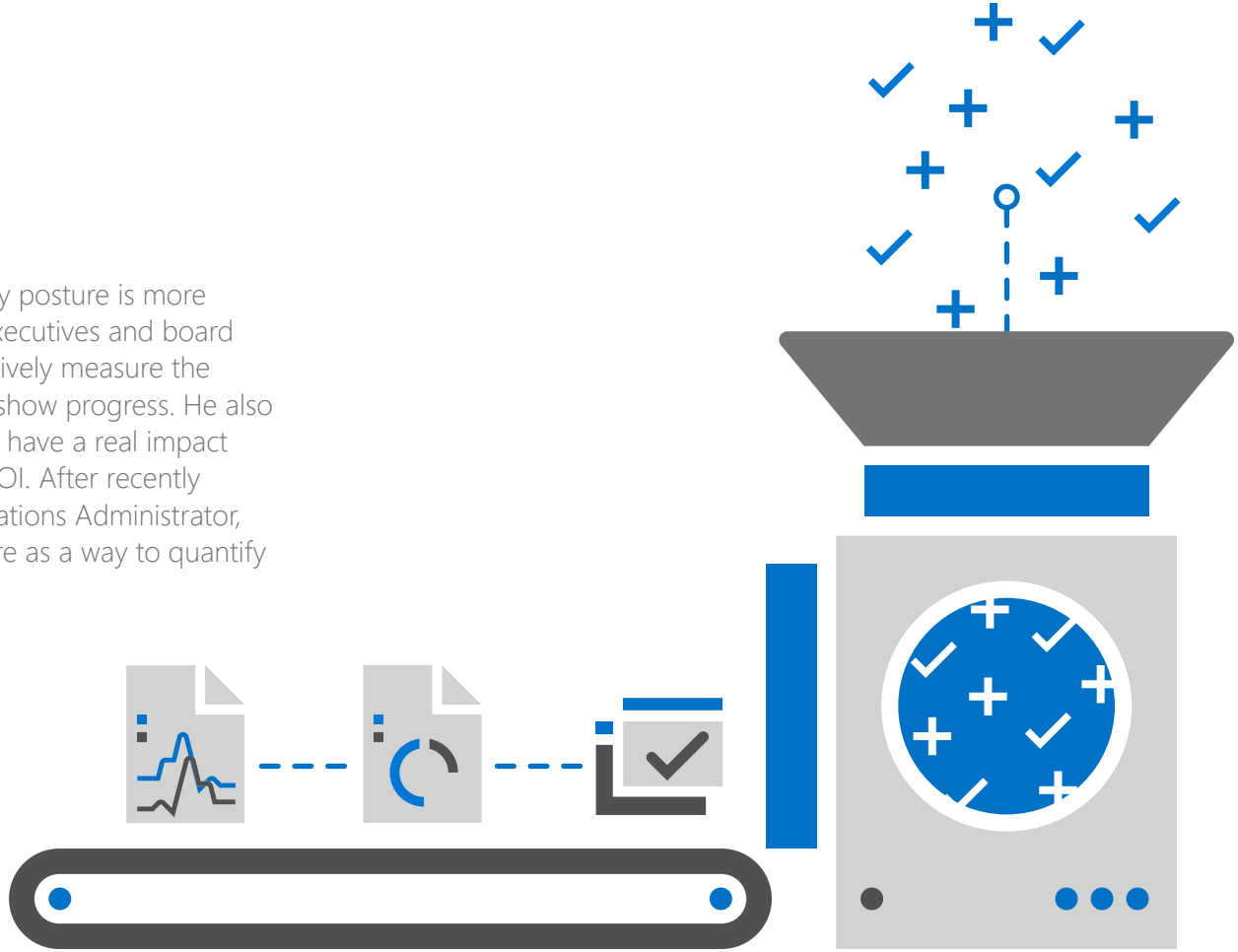
How can Evan understand his current security posture and get recommendations on how to improve?

All characters are fictitious.

Assess and improve your security posture

SCENARIO

Evan is aware that his understanding of Contoso's security posture is more anecdotal than objective, and he knows that the other executives and board members are not convinced. Evan needs a way to objectively measure the company's posture and track it over time so that he can show progress. He also needs a way to identify and prioritize improvements that have a real impact on the company's security so that he can show a great ROI. After recently deploying Microsoft 365 Enterprise E5, his Security Operations Administrator, Cathy, suggested that Evan look at Microsoft Secure Score as a way to quantify the company's security posture.



Quantify your security program

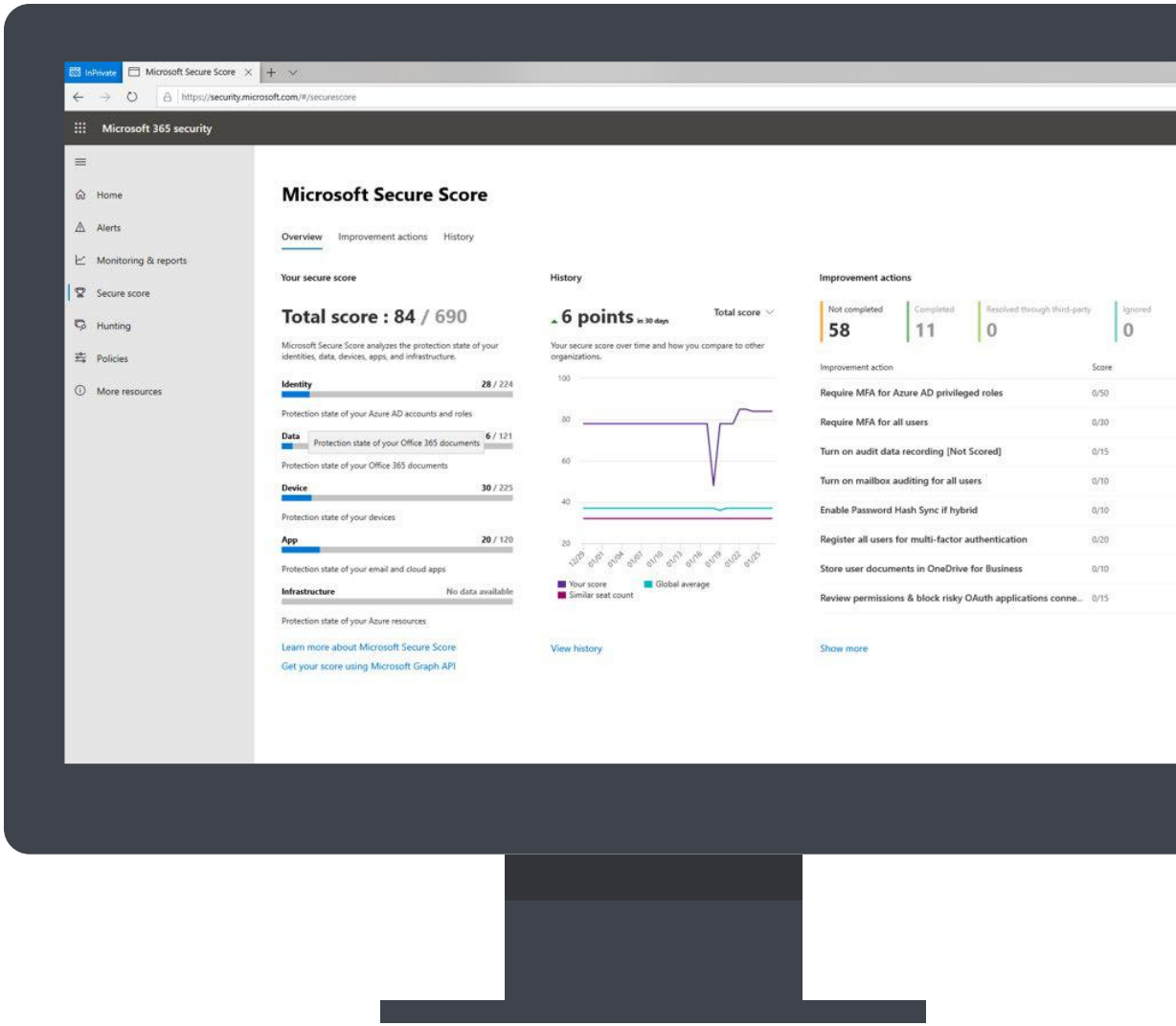
Microsoft Secure Score gives Evan an objective measurement of his organization's security posture. It looks at the Microsoft 365 Enterprise E5 products his company uses, their configurations, and user behaviors, and then compares those with the Microsoft baseline. That baseline comes from the incredible amount of threat intelligence Microsoft gathers, the expertise of its security analysts, and best practices it has developed over time. His organization earns points for each item it completes, and the total number of points possible increases based on the products purchased. For the items that a third-party security provider completes, Evan can mark the control as completed to add the points to his company's score.

Track the progress of your security program over time

Within Microsoft Secure Score, Evan uses the score analyzer to chart his company's progress over time. He exports this data for use in his reports to the board of directors, easily demonstrating his progress, which also encourages confidence in his team. Microsoft Secure Score does not indicate to Evan the likelihood of a breach, but it does give him a good indication of how much risk he has offset for his organization by adopting the security controls that Microsoft recommends.

Benchmark your security score against similar companies

Microsoft Secure Score compares the security score of Evan's organization with similar companies. His company's score is displayed alongside the average score of companies of similar size, companies in the same industry, and the Microsoft customer average. When the company first licensed Microsoft 365 Enterprise E5, its score was low compared with other companies in the same industry, but after adopting many Microsoft Secure Score recommendations, Evan sees that not only is the company's score higher than those of its industry peers, but it also exceeds the Microsoft average by a significant margin. Evan includes this comparison in his reports to the board of directors to get them excited by his team's progress.



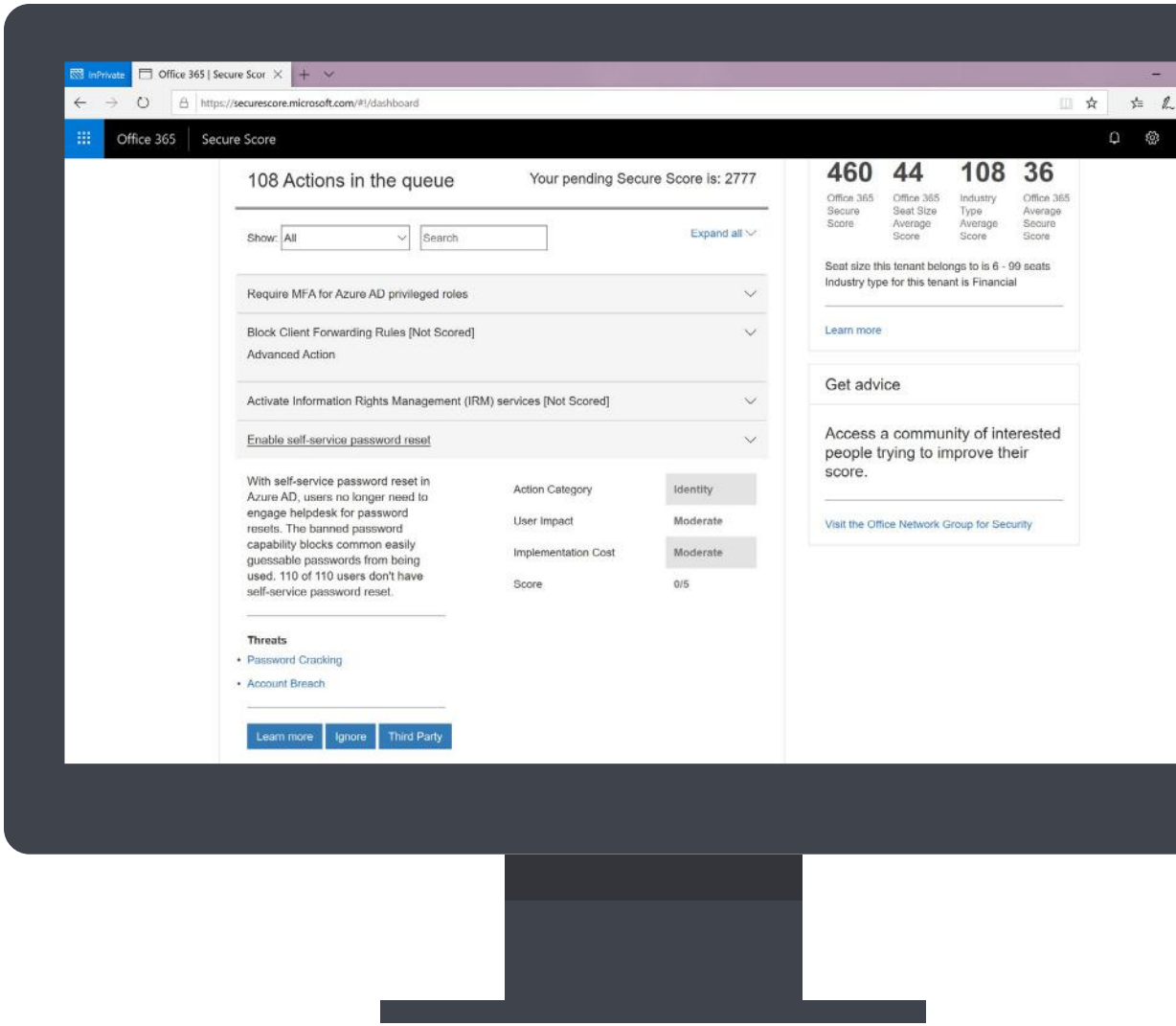
Improve your security posture by taking recommended actions

Evan uses the Microsoft Secure Score modeler to quickly figure out the actions he can take to further improve his organization's score. First, he chooses how aggressive he wants to be by moving the slider left or right to change the target score and reveal the recommendations for each. He selects a target score that balances security with user productivity. Then, he looks through the Secure Score action queue and prioritizes the recommendations he can implement quickly and with minimal impact to his thousands of users. For each action Evan reviews, he learns:

- recommendation details
- points it will add to the company's score
- threats the recommendation addresses
- user impact
- implementation cost

Evan recommends a target score to his security operations (SecOps) team, which takes responsibility for adopting the Secure Score recommendations. The team can drill down to see an overview of each recommendation and then select a link to configure the control or learn more about it. The team can also ignore a recommendation or indicate that a third-party product already addresses it, which adds the points to the score. The Secure Score user interface makes identifying and adopting Microsoft security recommendations easy for the team.

In addition, the recommendations prompt Evan to use security features that his company is already paying for. They guide him in building his security road map for the next six months so that he and his team don't have to guess what to do. Evan can rely on the security experts at Microsoft to advise him on the critical aspects of his security program and what they cost. As he implements these changes, he sees the score improve without increasing cost, and he is happy to report these facts to his company's board and fellow executives.

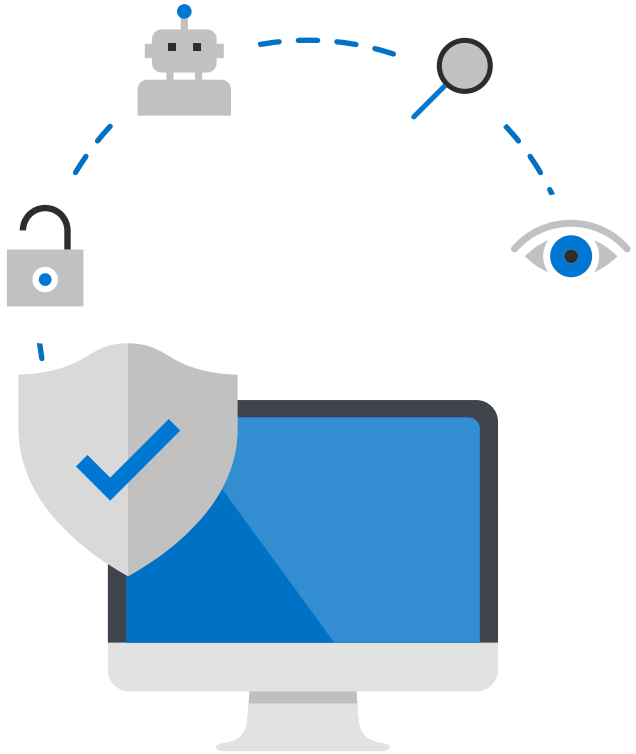


Protect against the latest zero-day threats

SCENARIO

Evan knows that new security threats emerge almost daily. As a result, he is motivated to better understand them so he can quickly evaluate his organization's exposure to specific, complex threats and manage its security controls accordingly. To do that, Evan works tirelessly to educate his SecOps team. He does a lot of online research, gets advice from peers, and encourages his team to share their ideas. Recently, Cathy advised Evan that the security solutions in Microsoft 365 Enterprise E5 can save them effort by providing detailed information about the latest threats that they can act on to prevent the company's security posture from backsliding.

Evan is an experienced CISO and has coached his SecOps team to operate under the assumption of compromise. He needs to know that his SecOps team has the tools necessary to investigate those attacks. Going further, Evan wants to give his SecOps team the ability to investigate how an attack succeeds in the first place so that the team can mitigate the damage and prevent similar attacks in the future. That work includes identifying the security policies, configurations, and user behaviors that allowed an attack to happen in the first place.



Learn about the latest threats through detailed industry reports

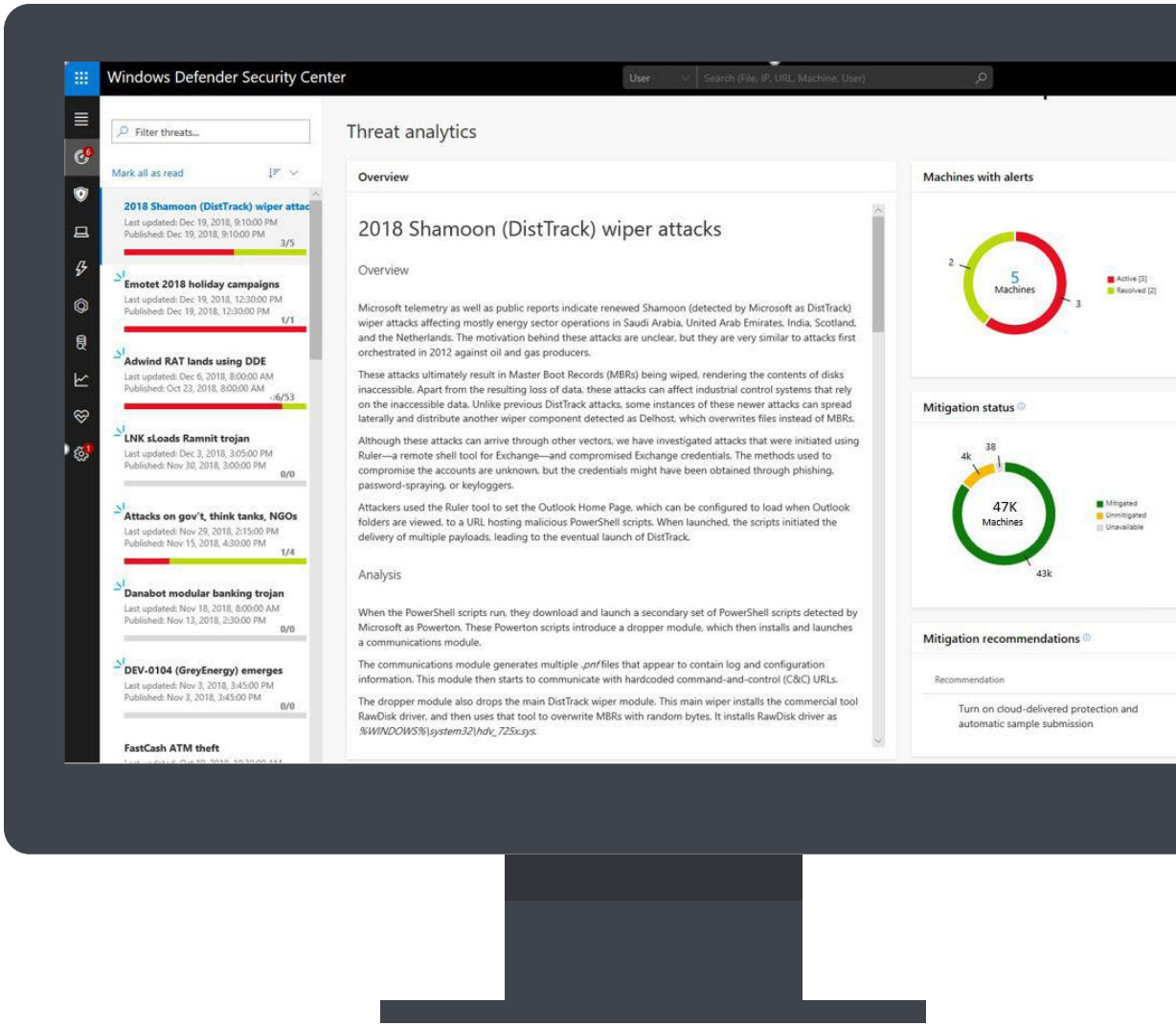
Evan learns about emerging threats by using threat analytics in Windows Defender Security Center—a set of interactive reports that Microsoft publishes as soon as it identifies new threats and outbreaks. Each threat report provides a summary that includes where the threat is coming from, where it has been seen, and the techniques and tools the threat uses. Threat reports also provide a list of mitigations for common vulnerabilities and exposures as well as detection details.

Reports that help answer questions such as, "How well am I protected against the latest attack vectors?"

Threat analytics in Windows Defender Security Center can assess a threat's relevance and current impact to Evan's endpoints. It can also recommend actions he can take to contain an attack, increase endpoint resilience to it, and prevent it.

Evan can quickly determine whether a new threat may be affecting his organization by examining the number of machines in the organization showing alerts related to the threat. The chart shows the number of machines these alerts affect and the number of machines on which the alerts have been resolved. He also looks at the number of affected machines over time. He is looking for a downward trend that shows alerts related to the threat being resolved on all machines within a few days.

To assess his endpoints' resilience to the threat, Evan looks at the recommended mitigations and their statuses, which indicate how many machines have the mitigations applied versus how many do not. As before, he looks at the mitigation status over time for a trend that shows all machines being mitigated within a few days. By applying the recommended mitigations to all his machines, Evan can reduce the risk of a successful attack on his endpoints.



Incident forensic reporting on events, audit logs, and alerts

Azure Advanced Threat Protection (Azure ATP) collects and stores information from configured domain controllers and member servers that it uses to detect known malicious attacks and techniques, security issues, and risks to the network. This information includes:

- Network traffic to and from domain controllers (e.g., authentications and domain name system queries)
- Security logs (e.g., Windows security events)
- Active Directory information (e.g., structure, subnets, sites)
- Entity information (e.g., names, email addresses, phone numbers)

Based on this information, Azure ATP generates an alert timeline that Evan's SecOps team uses to investigate and explore attacks on the network. It links all the alerts, endpoints, related incidents, and users involved with an incident in a live graph that is intuitive to navigate. During incident investigations, the team uses this graph to visualize information about the incident. When they select an item on the graph, Azure ATP displays detailed information about it. For many alerts, these details also include reports that explain the attack and the remediation steps to block it.

In addition, Azure ATP integrates with Windows Defender Advanced Threat Protection (Windows Defender ATP), Office 365 Advanced Threat Protection (Office 365 ATP), and Microsoft Cloud App Security to provide a comprehensive view of events and alerts throughout the company's digital estate, which helps Evan's team better correlate events. From there, they can move between these services while maintaining context, which helps them complete investigations more quickly and with greater insight.

Solve root cause policy and configuration issues

Evan uses the Microsoft Secure Score dashboard in Windows Defender ATP to quickly assess configuration issues in his organization, identifying which machines require attention and the actions he can take to reduce a machine's attack surface. At the top of the dashboard, Windows Defender ATP displays a list of top recommendations and the points that adopting each will add to the company's score. Here, Evan notices that he can add 72 points to the company's score just by installing security updates on his endpoints.

Below that, Evan sees a complete list of improvement opportunities. For each opportunity, Windows Defender ATP displays the current score, the score over the past 30 days, and the number of machines not configured correctly. To see which machines are misconfigured, Evan selects the machine count to reveal a filtered list for that recommendation. To help IT reduce the time to deploy updates to the affected machines, Evan exports that list to a Microsoft Excel file that the deployment team can use to create a target collection for deployment.

Identity Secure Score is a subset of Microsoft Secure Score that recommends actions specific to identity protection. For example, Evan always thought that forcing users to reset their password periodically was good security. Turns out this practice causes users to use weaker passwords that they can remember more easily. By disabling password expiration, Evan was able to increase the company's identity secure score by 10 points.

Identify vulnerable users and educate them about email phishing attacks

To identify vulnerable users in Evan's organization, he uses the Attack Simulator in Office 365 ATP to run a realistic phishing attack. He creates a phishing email with a sender's display name that recipients will trust in order to entice them to click through to the phishing sign-in server. The attack simulator provides email templates Evan can use, or he can create his own. After creating the phishing email, he sends it to everyone in the organization. Attack Simulator tracks users' clicks, so Evan can identify who requires additional training. When Evan presents the results to the other executives, they are surprised by the number of people who fell for the ruse, including members of senior management. By simulating an attack company-wide, Evan is able to educate employees without embarrassing individuals. As a result, they are more receptive to his suggestions and become more mindful of email security.

OTHER ATTACK SIMULATIONS AVAILABLE IN OFFICE 365 ATP:

PASSWORD-SPRAY ATTACK

An attempt to try commonly used passwords against a list of user accounts.

BRUTE-FORCE PASSWORD ATTACK

An automated, trial-and-error method of generating multiple password guesses from a dictionary file against a user's password.

Secure hybrid cloud workloads

SCENARIO

Evan's organization has cloud workloads that run in the Azure cloud and Amazon Web Services. About half of those run Linux. He needs to understand and improve the security posture of these hybrid cloud workloads and would prefer to use only one solution to manage it all because it will be more efficient and keep costs down.

Protect hybrid cloud workloads running Windows Server and Linux

Evan uses Azure Security Center to manage security and threat protection for all his organization's workloads on any cloud platform, whether they are running Windows or Linux. First, he applies security policies to the company's workloads, ensuring compliance with company and regulatory security requirements. He also monitors the security posture of linked machines, networks, storage and data services, and applications to discover potential security issues. Azure Security Center offers Evan recommendations for remediating security vulnerabilities—before attackers can exploit them.

The advanced cloud defenses that Azure Security Center offers caught Evan's attention immediately. For example, adaptive application controls prevent unauthorized applications from running on the company's workloads, but Evan enabled just-in-time virtual machine (VM) access to close management ports until administrators request access to them. When Evan approves access to a VM, he can limit the time administrators have access to them so that the ports close automatically. He thinks of it as a drawbridge that allows VM access to authorized users for only a short time.

Azure Security Center can collect, search, and analyze security data from a variety of sources, including connected partner solutions. This integration gives Evan a more complete view of his security posture across the entire digital estate.

Use security and compliance blueprints to strike a balance between agile development and compliance controls

Evan acts as the cloud custodian overseeing the activities of numerous development teams inside of his organization who use Azure infrastructure as a service (IaaS) and platform as a service (PaaS) to create their offerings. He wants to allow these teams to use agile development processes and make use of all the technical advantages that the cloud has to offer, but he also wants to be sure that these teams' cloud resources are subject to a sufficient level of security and compliance controls to safeguard the needs of his business. To meet the goal of both agility and compliance, Evan uses Azure Policy and Azure Blueprints to establish a set of baseline guardrails that apply to every Azure subscription within his cloud estate. These blueprints include common reference architectures, deployment guidance, responsibility matrices, and threat models that help him quickly and securely implement his solutions. In some cases, blueprint automation is available.

Now, he can mandate that all IaaS and PaaS resources deployed within the organization be tagged with the appropriate application name and cost center, and ensures that "internal-only" resources are configured with mandatory network security groups that do not allow inbound network traffic from the Internet. Using the resource locking capabilities of Azure Blueprints, even subscription owners cannot override or change these mandatory configurations for mission-critical and compliance-sensitive applications.

Data analytics, data warehouse, infrastructure as a service web application, and platform as a service web application security and compliance blueprints are available for the following regulatory requirements:

- ✓ Australia Protected
- ✓ Federal Risk and Authorization Management Program
- ✓ FFIEC
- ✓ General Data Protection Regulation
- ✓ Health Insurance Portability and Accountability Act and Health Information Trust Alliance
- ✓ National Institute of Standards and Technology Special Publication 800-171
- ✓ Payment Card Industry Data Security Standard 3.2
- ✓ Trusted Internet Connections
- ✓ UK National Health Service
- ✓ UK-OFFICIAL

Strengthen your security posture with intelligent insights and recommendations

Microsoft 365 Enterprise E5 enables organizations to continually assess and improve their security posture. Microsoft Secure Score quantifies their security programs and enables them to track their progress over time. It also gives them recommendations for improving their security scores and benchmarks them against other companies of a similar size in the same industry. Organizations governed by compliance regulations can use security and compliance blueprints to set up their cloud for success.

Additional capabilities enable organizations to thoroughly investigate threats and manage security controls. Detailed industry reports help them learn about the latest threats. Windows Defender Security Center shows how well their endpoints are protected against the latest threats. Furthermore, Azure Security Center enables them to find the root causes of security incidents so that they can change security policies and configurations to prevent them. Azure Security Center also gives them visibility and control of workloads running on any cloud platform, whether they are running Windows Server or Linux. Finally, Office 365 ATP can run simulated attacks to help organizations identify vulnerable users who need additional training.

These security products work seamlessly to help improve your company's security posture:

- Microsoft Secure Score
- Microsoft 365 Security and Compliance Center
- Windows Defender Advanced Threat Protection
- Office 365 Advanced Threat Protection
- Azure Advanced Threat Protection
- Azure Security Center

THE INTELLIGENT CLOUD OFFERS AN OPPORTUNITY TO DO SECURITY BETTER

For enterprise customers that embrace the Microsoft productivity suite, there are significant gains to be realized in security. Microsoft 365 Enterprise E5 includes built-in security solutions that integrate easily and share insights from the 6.5 trillion security signals per day seen on the Intelligent Security Graph across the global Microsoft ecosystem. It allows customers to reduce the number of security vendors they manage by unifying security and productivity tools into a single suite that safeguards users, data, devices, and applications—without sacrificing the user experience.

IDENTITY & ACCESS MANAGEMENT

- Azure Active Directory
- Microsoft Cloud App Security
- Windows Hello
- Windows Defender Credential Guard

INFORMATION PROTECTION

- Azure Information Protection
- Windows Information Protection
- Microsoft Cloud App Security
- Advanced Data Governance
- Office 365 Data Loss Prevention
- Microsoft Intune
- Bitlocker

THREAT PROTECTION

- Azure Advanced Threat Protection
- Windows Defender Advanced Threat Protection
- Office 365 Advanced Threat Protection
- Microsoft Cloud App Security

SECURITY MANAGEMENT

- Microsoft 365 Security & Compliance Center
- Windows Defender Security Center
- Microsoft Secure Score
- Microsoft Cloud App Security

Microsoft

GET COMPLETE, INTELLIGENT ENTERPRISE SECURITY

Test it yourself with a free trial, get serious with a proof of concept, or learn more at **aka.ms//M365E5/Security**