Microsoft

Microsoft Entra ID Protection

White paper

Contents

Executive summary

In today's dynamic work environment, cyberattacks are becoming increasingly sophisticated, making it vitally important to safeguard identities. The proliferation of remote work, networks, apps, and devices has exposed vulnerabilities that attackers can exploit. They can use compromised accounts to quickly bypass security protocols and move laterally to gain access to sensitive data and resources.

This white paper serves as a comprehensive guide for IT, security, and identity leaders—including chief information security officers (CISOs), chief information officers (CIOs), and vice presidents (VPs) of IT—seeking effective identity protection solutions to strengthen their cybersecurity posture and proactively mitigate risks.

Here we introduce Microsoft Entra Identity (ID) Protection, a cloud-based identity solution that can safeguard organizations like yours against identity theft. This powerful tool empowers teams to prevent identity takeover in real time by enforcing adaptive

access policies, high-assurance authentication methods, and automated identity threat assessment powered by advanced machine learning (ML). With these capabilities, your organization can prevent identity threats while gaining valuable security insights. Moreover, the solution effectively minimizes the number of alerts you receive and provides easily digestible and actionable insights for your IT and security teams to mitigate risks.

Our objective is to simplify complex identity protection concepts and provide practical insights to empower teams to effectively protect their identities and data assets. By implementing the knowledge and recommendations shared in this white paper, organizations can strengthen their security foundation, minimize vulnerabilities, and confidently navigate the ever-evolving landscape of identity protection.

The evolving landscape of identity security

Today's modern work environment has introduced new complications into the cybersecurity landscape. Hybrid work styles outside of corporate perimeters have increased connectivity and convenience, and organizations are adopting cloud infrastructure, migrating data and apps, and engaging with third-party ecosystems. These advancements, however, create opportunities for threat actors and cyber attackers. The increasing number and sophistication of attacks pose challenges for organizations to protect sensitive information and assets in an expanded digital landscape.

Attackers targeting identities with tactics like password sprays (guessing common passwords) and phishing (convincing someone to disclose personal information in response to a fake website, text message, or email) pose a persistent threat to organizations globally. They take advantage of the growing complexity of these attacks, launching relentless high-volume assaults and exploiting security gaps and permissions. By exploiting compromised identities, attackers gain unauthorized access to valuable corporate resources, enabling lateral movement and causing severe consequences such as data breaches, financial loss, intellectual property theft, and reputational harm.

In addition, attackers have broadened their scope to target all identities within an organization's ecosystem. This encompasses workload identities, system accounts, and other non-human entities with exploitable vulnerabilities. As a result, organizations need to comprehensively understand identity across their entire infrastructure, including user account permissions and potential vulnerabilities within workloads.

→ The number of password attacks has risen to an estimated 921 every second—a 74% increase in just one year

Microsoft Digital Defense Report 2022.

→ The average cost of a data breach in 2022 reached an all-time high of USD4.35 million.

IBM. Cost of a data breach 2022.

→ Microsoft blocked 34.7 billion identity threat attacks in 2021.

Microsoft Security: State of Cybercrime.

Meeting the modern needs of identity protection

Effective identity protection is a complex undertaking that necessitates constant vigilance and a comprehensive understanding of the latest threats, attacks, security tools, and best practices. Organizations must prioritize preventive measures for identity protection to anticipate and remediate potential bad actors who are continually refining their tactics to exploit various kinds of attacks. Cybersecurity threats encompass both pre-authentication and post-authentication attacks, targeting vulnerabilities before and after the authentication process. Traditional approaches that rely solely on passwords and basic authentication methods are insufficient against today's new and sophisticated pre-authentication attacks. Tactics commonly employed include password attacks, phishing, and breach replay (relying on pervasive password reuse to take passwords compromised on one site and try them on others). It's therefore imperative for organizations to recognize the significance of these attacks and act appropriately to mitigate their impact.

Password attacks

Password attacks pose a significant threat to organizations through tactics like password spraying, phishing, and breach replay.

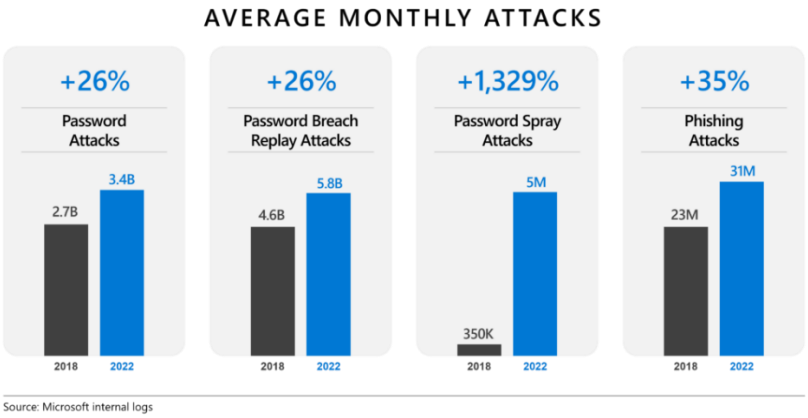


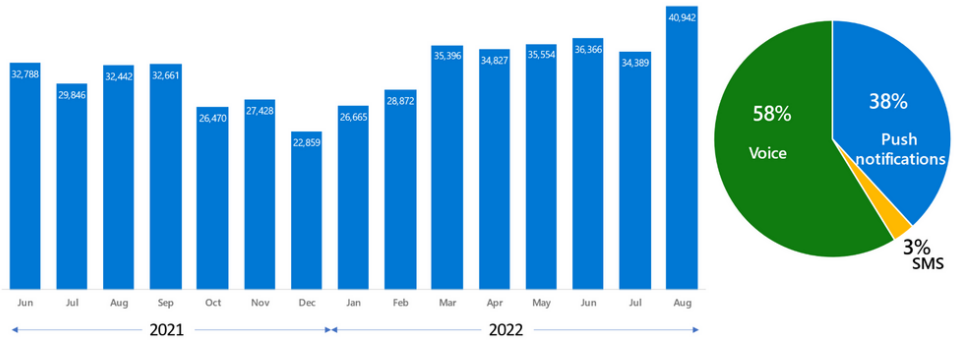
Figure 1: Growth in password-related attacks between 2018 and 2022

Organizations must prioritize strong password management practices to counter these threats, enforce complex password requirements, and implement multifactor authentication (MFA). Modern MFA methods, including apps, tokens, and device-based authentication, provide a seamless and user-friendly experience, adding an extra layer of security to protect against compromised passwords.

→ More than 99.9% of compromised accounts don't have MFA enabled.

MFA attacks

Enabling MFA is a crucial step in deflecting identity attacks. However, not all forms of MFA are equally secure, and sophisticated phishing attacks can bypass MFA. Examples include SIM-jacking and other telephony vulnerabilities, MFA hammering (MFA fatigue attacks), and adversary-in-the-middle attacks (tricking users into completing the MFA interaction). Although these attacks require more effort and investment from attackers, they're still on the rise.



Source: Azure AD Identity Protection sessions at high risk with multiple failed MFA attempts

Figure 2: MFA fatigue attacks from June 2021 to August 2022

To effectively combat phishing attacks, it's crucial to use MFA methods resistant to such threats. These phishing-resistant methods require an interaction between the authentication method and the sign-in surface, eliminating the use of shared codes. Furthermore, phishing-resistant technologies verify the source and destination's validity, ensuring that authentication actions can only occur between the intended site and the user's device. Examples of these methods include Microsoft Authenticator, Windows Hello, Fast Identity Online (FIDO), or certificate-based authentication (CBA) for organizations with Personal Identity Verification (PIV) and Common Access Card (CAC) infrastructure. By adopting this proactive approach, organizations can significantly reduce the risk of unauthorized access and improve usability compared to traditional passwords or telephony-based authentication.

Post-authentication attacks

In addition to the pre-authentication attacks mentioned earlier, organizations also need to be vigilant against post-authentication attacks that occur after a user has successfully authenticated and gained access to a system or network. These attacks focus on exploiting vulnerabilities within the authenticated session to gain unauthorized privileges, escalate privileges, or access sensitive information. Tactics like token protection attacks and OAuth consent phishing are commonly used in post-authentication attacks.

In post-authentication attacks, determined attackers may employ malware to steal tokens from devices, enabling them to exploit valid MFA performed by legitimate users on trusted machines. While tokens can also be compromised through incorrect logging or interception by compromised routing infrastructure, malware on a machine is the most prevalent method. Organizations should implement robust endpoint protection, effective device management, and least privileged access to mitigate these token protection threats. Additionally, monitoring for signs of token theft and enforcing re-authentication for critical scenarios like machine enrollment is crucial.

Another emerging type of post-authentication attack is OAuth consent phishing, where attackers deceive users into granting access permissions to malicious applications. Inspecting and limiting user consent to applications from verified publishers is essential to combat this. The increasing instances of token replay attacks and OAuth consent phishing highlight the importance of robust security measures and user awareness.

Infrastructure compromise

As organizations strengthen their identity security measures, advanced attackers are increasingly targeting the underlying identity infrastructure. Exploiting vulnerabilities in outdated or insecure on-premises networks, they aim to steal sensitive information, compromise federation servers, and undermine the infrastructure. This type of attack is particularly challenging, as attackers can use their access to conceal their actions, making it difficult to remove them altogether.

To counter this kind of threat, you should enhance hybrid and multicloud detections and establish automated protection against indicators of identity infrastructure attacks. It's recommended to reduce reliance on on-premises infrastructure, shifting authority to the cloud and isolating cloud infrastructure from on-premises

environments. Collaboration with the security operations center (SOC) is crucial, with attention given to privileged identity administrators and on-premises servers. Additionally, safeguarding non-human identities and the infrastructure managing them is essential, as adversaries can exploit any potential security gaps.

Key challenges faced by IT leaders in protecting identities and strengthening cybersecurity

IT leaders like CIOs and CISOs face significant challenges in today's dynamic cybersecurity landscape. These challenges encompass various aspects of identity protection and require a multifaceted security approach. However, a critical difficulty lies in integrating multiple security solutions and achieving comprehensive coverage, as the fragmented approach often hampers threat detection and overwhelms security teams with alert fatigue.

Budget constraints further complicate matters, impeding investments in robust security measures and resources. Additionally, the scarcity of cybersecurity talent poses a significant obstacle, as there is a limited supply of skilled professionals proficient in safeguarding critical systems and data. Furthermore, as organizations undergo digital transformation, the expanding network, application, and device landscape creates numerous entry points for potential attackers. To address this expanding attack surface, strategic planning and a proactive security approach are necessary. Moreover, navigating complex legal frameworks and ensuring compliance with regulations adds another layer of complexity for CIOs and CISOs. These regulatory requirements must be considered and met to maintain a secure and compliant environment.

→ Microsoft research shows that large organizations have an average of 75 security solutions.

Microsoft. What's your company's cybersecurity score?

Protect against identity threats using a "defense-in-depth" approach

Protecting user accounts is critical but no longer enough. CIOs and CISOs must protect every layer of the identity ecosystem, including non-human or workload identities, plus the infrastructure that provides, stores, and manages all identities. They need real-time protection of all identities and endpoints, and they need to adopt a Zero Trust strategy, including early detection mechanisms and automated protection. A Zero Trust strategy emphasizes the explicit verification of users, the use of least-privileged access principles, and the assumption of a breach. It focuses on strong user identity, device health verification, validation of application health, and secure, least-privilege access to corporate resources and services. The "defense-in-depth" approach aligns with the principles of Zero Trust and provides a comprehensive framework for identity protection by incorporating multiple layers of security controls to safeguard against evolving threats.

- **High-assurance authentication methods:** High-assurance authentication methods like MFA strengthen identity security. Employing phishing-resistant MFA methods such as Windows Hello, FIDO 2 security keys and passkeys, and CBA can reduce risk even further.
- **Security posture management:** Bad identity system practices can be prevented by monitoring both an organization's infrastructure and, specifically, its identity assets for key risk indicators, bad policies and controls, and system misconfigurations that elevate the organization's risk level.
- **Real-time protection and remediation with identity:** Risk can be reduced by enforcing real-time access policies or Conditional Access policies. Such policies are based on risk aggregated from multiple sources on any identified suspicious activity related to user accounts in the directory.
- **Identity threat detection and investigation:** Finally, analyzing signals from across the organization's digital estate to identify suspicious activity using advanced ML algorithms and behavioral analytics can also help reduce the risk of attack.

Microsoft Entra ID Protection

To strengthen your organization's identity posture, Microsoft offers Entra ID Protection, a cloud-based identity security solution that protects organizations against identity threats at every layer. The solution blocks identity takeover by enforcing real-time adaptive access policies, high-assurance authentication methods, and automated identity threat assessment powered by the strength of advanced ML. Analyzing users and sign-in patterns based on aggregated risk scores protects against identity-based attacks such as password sprays, brute force, phishing, sign-ins from anonymous or suspicious IP addresses, infected devices, and leaked credentials. The solution also allows IT and security teams to easily review security reports and export data to first- and third-party security information and event management (SIEM) and extended detection and response (XDR) tools.

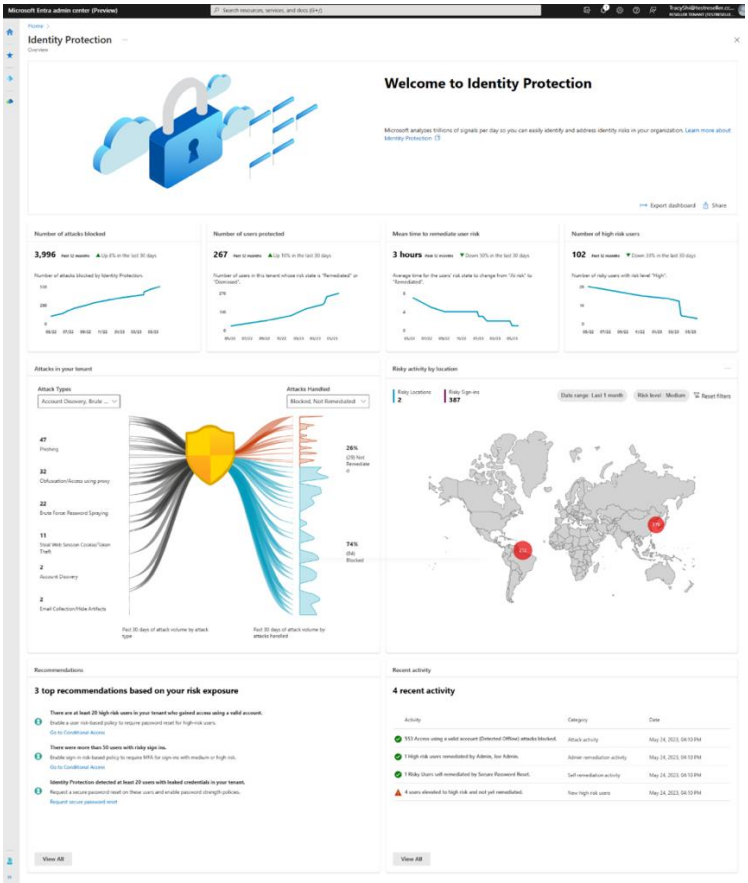


Figure 3: Attacks and recommendations on the Microsoft Entra ID Protection dashboard

→ Microsoft Entra ID Protection uses cloud-based ML to analyze over 200 terabytes of authentication data daily and evaluate sign-in anomalies along 100+ axes in real time.

Enforce risk-based adaptive access policies

In identity protection, identifying suspicious activities or actions taken by users while or after signing in is crucial. These risks are classified as user risks and sign-in risks. Organizations increasingly seek robust authentication and real-time, risk-based adaptive access policies that govern resource and data access to address such scenarios.

→ User risk:
The probability that a user identity is compromised

Microsoft Entra ID Protection can enforce granular policies based on user and sign-in risks, effectively blocking identity attacks in real time. It uses advanced ML and connected intelligence to investigate risky users and sign-ins, addressing vulnerabilities through automated remediation. Cloud intelligence powered by advanced heuristic algorithms and user and entity behavior analytics (UEBA) recognizes anomalous behavior, thus providing a strong defense against identity compromise. Enforcing risk-based adaptive access policies involves enabling user and entity behavior analytics, constantly improving risk assessment techniques, facilitating self-remediation actions, and performing real-time risk analysis.

→ Sign-in risk:
The probability that an authentication was not authorized by the identity owner

Let's delve deeper into these essential action items to better understand their role in enforcing risk-based adaptive access policies

Enable user and entity behavior analytics

Identifying threats and assessing their potential impact, whether they stem from compromised entities or malicious insiders, has traditionally been a time-consuming and labor-intensive process.

However, with Microsoft Entra ID Protection's user and entity behavior analytics (UEBA) capability, security analysts can streamline their workloads, reduce manual efforts, and receive high-fidelity, actionable intelligence. This empowers them to focus on investigation and remediation tasks.

Using cloud intelligence and advanced heuristic algorithms, UEBA recognizes anomalous behavior patterns, effectively blocking identity compromise. By automating remediation based on user and sign-in risk through adaptive access policies, you can extend protection across your entire identity landscape and proactively thwart identity attacks. Furthermore, you can enhance Conditional Access policies by integrating real-time risk detection. Using risk scores, you can make informed decisions on blocking access, allowing access, or allowing access with additional security measures like MFA or password reset. By enabling user and entity behavior analytics, organizations can significantly enhance their ability to detect and

respond to identity threats, freeing up valuable resources for targeted investigation and remediation efforts.

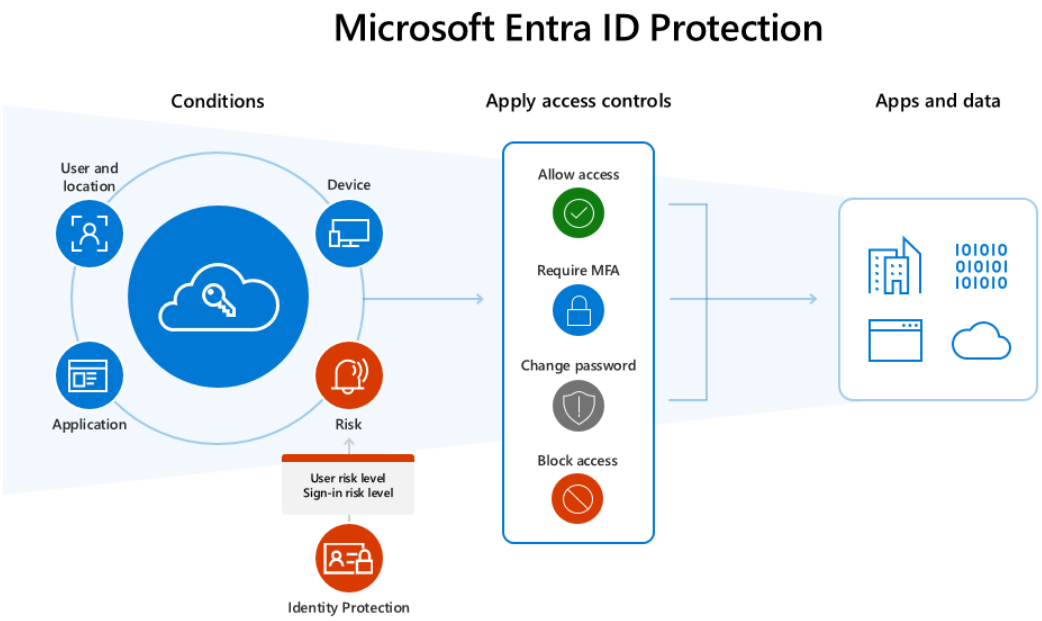


Figure 4: User and sign-in risk and configurable policy

Constantly improve risk assessment

With heuristics and ML-based signals, Microsoft Entra ID Protection performs an identity risk assessment each time a user signs in. To continuously enhance risk assessment, Microsoft's risk engines are designed to incorporate your risk feedback. There are various scenarios in which your feedback can contribute to improving risk assessment, including:

- **Identifying that Microsoft Azure AD's user or sign-in risk assessment is incorrect.** For example, if a sign-in shown in the "Risky sign-ins" report is benign, then all detections on that sign-in are false positives.
- **Verifying that Azure AD's user or sign-in risk assessment is accurate.** For example, if a sign-in shown in the "Risky sign-ins" report is indeed malicious, you want Entra AD to acknowledge that all the associated detections are true positives.
- Mitigating the risk on a user outside of Microsoft Entra ID Protection. For example, you want the user's risk level to be updated.

Microsoft takes your feedback into account to update the risk status of the corresponding user and sign-in to improve the overall accuracy of these events. This feedback mechanism contributes to securing the user more effectively and ensuring accurate risk assessment.

Perform real-time risk analysis and automatic remediation

Microsoft Entra ID Protection provides an easy-to-use, real-time analytics service designed for mission-critical workloads to proactively analyze identity threats. This enhanced solution automatically detects and mitigates identity-based threats using real-time ML systems. The ML model used in real-time risk assessment uses supervised ML and has been improved by expanding the features and processes used to train the model, resulting in significantly enhanced accuracy. The model effectively identifies more malicious activity while reducing false alarms. The real-time ML system incorporates intelligence from various sources, including:

- **User behavior analysis** to assess whether the user is signing in from a known device, location, or network.
- **Threat intelligence** to validate whether the sign-in activity originates from a known suspicious or malicious infrastructure.
- **Network intelligence** to evaluate whether the IP address is associated with a mobile network, proxy, or hosting facility.
- **Device intelligence** to identify whether the device is compliant or managed, or if the request comes from non-compliant devices.

By using multiple intelligence sources, Microsoft's real-time risk analysis gives organizations a comprehensive view of potential threats and enables prompt remediation actions.

Self-remediate with risk-based policy

To empower users in addressing sign-in and user risks, you can implement risk-based adaptive policies that automate the response to detected risks and allow users to self-remediate. These policies are configured based on risk levels, ensuring that they apply only when the risk level of the sign-in or user matches the configured criteria. If a user has registered for self-service password reset (SSPR), they can use this feature to self-remediate their user risk by performing a self-service password reset. Users who successfully pass the required access control measures, such as MFA or secure

password change, will have their risks automatically remediated. By enabling self-remediation through risk-based policies, organizations can streamline the process of addressing risk and empower users to take proactive actions to mitigate potential threats to their identities.

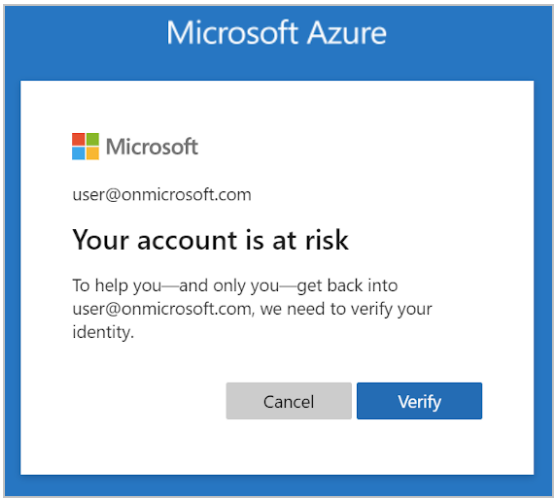


Figure 5: Self-remediation

Safeguard sensitive access

Microsoft Entra ID Protection offers robust measures to safeguard sensitive access. Token protection policies are used to prevent attackers from stealing and replaying tokens, ensuring the integrity and confidentiality of authentication credentials. The implementation of MFA is required to provide additional verification for users accessing services off the corporate network, adding an extra layer of security. It can also block access from specific regions, enabling organizations to enforce access control based on geographical restrictions.

Conditional Access policies can be created to grant or deny access based on the GPS location of the user's phone, allowing for location-based access restrictions and risk mitigation. Additionally, Microsoft Entra extends Conditional Access policies to cover workload identities, providing consistent access controls and security measures for various applications and identities. These capabilities collectively strengthen sensitive access security and safeguard organizations' critical resources. In the following sections, we delve into these capabilities, providing valuable insights into how they contribute to safeguarding sensitive access.

Reduce attacks with token protection

Microsoft Entra ID Protection includes token protection as a crucial security measure to prevent attackers from stealing and replaying tokens. Tokens authenticate and authorize users to access various resources and services. However, if these tokens are compromised, attackers can exploit them to gain unauthorized access. To mitigate this risk, Microsoft Entra ID Protection employs token protection mechanisms. These mechanisms employ various security measures, such as encryption, digital signatures, token lifetime restrictions, and the creation of a cryptographically secure tie between the token and the device it's issued to (a client secret). A cryptographically secure tie between tokens and the devices they're issued to ensures that tokens are usable only from the intended devices, further strengthening the protection against unauthorized access and potential data breaches.

By implementing token protection, Microsoft Entra ID Protection adds an extra layer of security to prevent attackers from intercepting, tampering with, or replaying tokens. Token protection also includes advanced techniques to detect and block token replay attacks. Microsoft Entra ID Protection monitors token usage and compares it against known patterns and behaviors to identify and prevent replay attempts. This ensures that only valid and non-compromised tokens are accepted for authentication and authorization purposes.

Enhance protection with Conditional Access and MFA

One of the powerful features offered by Microsoft Entra ID Protection is the ability to require MFA for users who access a service off the corporate network or to block users from accessing a service from specific regions. This functionality adds an extra layer of security to protect against unauthorized access attempts.

By configuring Conditional Access policies within Microsoft Entra ID Protection, organizations can enforce MFA for users accessing a service outside the corporate network or for sensitive actions, such as modifying access policies. This means that when users attempt to access a service from an external network or perform specific sensitive actions, they will be prompted to provide additional authentication factors beyond their password. Furthermore, organizations can also use Conditional Access policies to block users from accessing a service from specific regions.
This is particularly useful in scenarios with strict data sovereignty or compliance requirements. By setting up policies based on IP ranges or geolocation, organizations can prevent users from accessing the service if they're in restricted regions.
This adds a layer of protection by limiting access to services based on the user's geographic location.

Safeguard access based on GPS location with Conditional Access

Controlling access to sensitive resources is crucial for preventing unauthorized access. With the "location conditions" featured in Conditional Access, you can restrict access based on the user's network location, effectively reducing the risk of unauthorized access. This feature allows organizations to enforce access policies based on the user's physical location. By using the location condition in Conditional Access, you can block access from countries or regions where your organization does not expect legitimate traffic. This helps to prevent unauthorized access attempts from locations that may pose a higher security risk.

Microsoft Entra ID Protection goes beyond traditional IP-based location identification by enabling administrators to create Conditional Access policies that consider the GPS location of the user's phone where the Microsoft Authenticator app is installed. It prompts users for their GPS location before applying policies. GPS location provides a more precise and reliable datapoint than IP address, making it particularly useful when strict requirements exist regarding data access from specific countries. This capability, offered by Microsoft Entra ID Protection, allows administrators to make informed access decisions based on the user's GPS location, enhancing the overall security of your resources.

Enable blocking service principals

A workload identity refers to an identity assigned to a software workload, such as an app, service, script, or container, that's used to authenticate and access various services and resources. While many identity and access management solutions focus primarily on securing human identities, Microsoft Entra Workload Identities addresses the challenges of securing workload identities, including apps, service principals, and managed identities.

One of the key features provided by Microsoft Entra Workload Identities is Conditional Access for workload identities. This feature enables you to implement security measures for workload identities by blocking service principals from accessing resources outside of trusted public IP ranges or based on risk factors detected by Microsoft Entra ID Protection. Using Conditional Access policies, you can define rules and restrictions to prevent service principals from accessing resources from untrusted IP ranges. Using Conditional Access for workload identities, you can block access for specific accounts when Identity Protection marks them as "at risk." This helps mitigate the risk of unauthorized access attempts and strengthens the overall security of your workload identities. Additionally, the risk detection capabilities of Microsoft Entra ID Protection can be used to identify and block access for service principals that exhibit suspicious or risky behavior.

Streamline access with trusted locations

Microsoft Entra ID Protection offers the powerful capability of specifying trusted locations to enhance security and streamline authentication. By configuring trusted locations, organizations can lower a user's sign-in risk score when they authenticate from known good sites. Trusted locations are specific network locations or IP ranges considered safe and trustworthy by the organization. When a user signs in from one of these trusted locations, it indicates a reduced risk of unauthorized access or malicious activity. As a result, the user's sign-in risk score is decreased, reflecting a higher level of trust and eliminating the need for additional authentication measures.

By implementing trusted locations in Microsoft Entra ID Protection, organizations can provide a seamless and efficient user experience by allowing uninterrupted access from trusted sites. This feature improves productivity and maintains strong security measures, ensuring a balance between user convenience and robust identity protection.

Deepen insights into your identity security posture

Unlike many other identity management solutions, Microsoft Entra ID Protection provides intelligence that helps identify and prevent identity attacks and security incidents. By automatically remediating risks based on configured policies, it significantly reduces the number of reports and alerts that are sent out, allowing identity administrators to focus on relevant information. Microsoft Entra ID Protection offers modern reports and customizable notifications, delivering the remaining risk data to identity admins in an easily digestible format. This enables accurate investigations and detailed reporting, empowering security professionals to understand their identity security posture and make informed improvements.

By using the insights gained, IT and security teams can respond to risks more effectively and proactively avoid them in the future. Microsoft Entra ID Protection consolidates informative signals and reports within a single control plane, providing IT teams with a centralized platform to review and investigate alerts and user activity. This streamlines the process of monitoring identity security, enhances the ability to detect and respond to potential threats, and strengthens the organization's overall security posture.

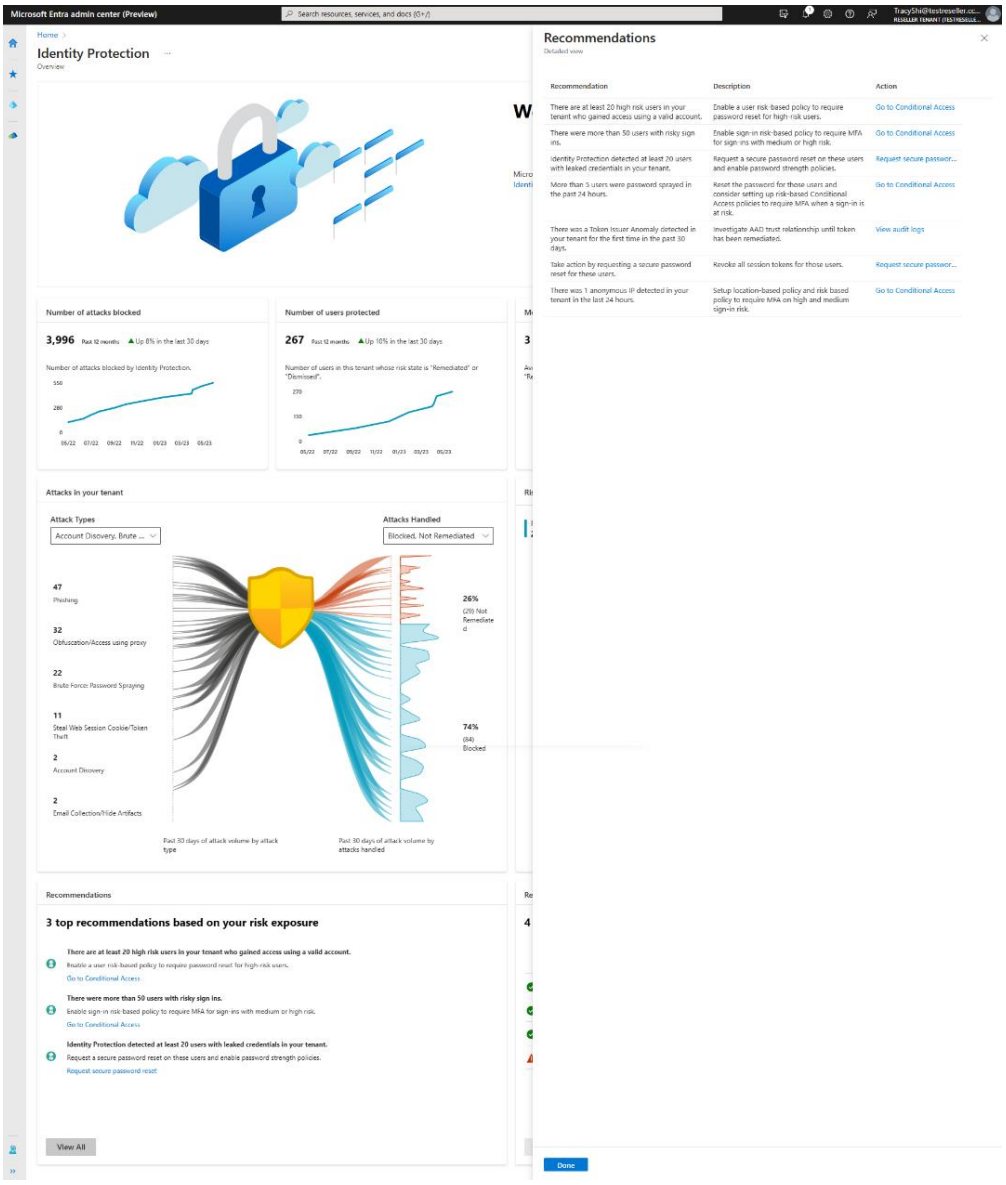


Figure 6: Recommendations and actions based on organizational risk exposure

Proactive and streamlined threat management

Microsoft Entra ID Protection offers a powerful capability to reduce the flood of reports and alerts you'd normally receive by automatically identifying and preventing identity attacks. With the increasing complexity and volume of security threats, organizations often struggle with the overwhelming number of reports and alerts generated by their identity management systems.

Using advanced algorithms and ML capabilities, Microsoft Entra ID Protection analyzes identity-related events and activities to automatically identify potential identity attacks. This proactive approach allows for the early detection and prevention of suspicious activities, minimizing the noise of false alerts and focusing attention on genuine security threats.

The automated identification of identity attacks enables organizations to streamline their security operations and optimize the allocation of resources. Instead of manually sifting through a barrage of reports, security teams can rely on the intelligence provided by Microsoft Entra ID Protection to prioritize their efforts and focus on investigating and mitigating real threats.

Single interfaces for deep visibility

Microsoft Entra ID Protection offers a streamlined user experience with a single control plane to efficiently investigate risk alerts and user activities. A simplified user interface makes it easy to review informative signals and reports to effectively identify high-risk users, sign-ins, risk insights, and key recommendations. Microsoft Entra ID Protection provides organizations with three reports that they can use to investigate identity risks in their environment: risky users, risky sign-ins, and risk detections. Investigating events is critical to better understanding and identifying any weak points in your security strategy. This risk detection report also provides a clickable link to the detection in the Microsoft Defender for Cloud Apps (MDCA) portal, where you can view additional logs and alerts.

A centralized experience to investigate and respond

Microsoft Information Protection, with a centralized experience, helps IT professionals gain greater visibility into sensitive data across the organization. It empowers teams to investigate and respond to alerts across the entire environment—from cloud-based to hybrid. Microsoft Defender for Identity offers a cloud-based security solution that uses your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. It enables SecOps analysts and security professionals struggling to detect advanced attacks in hybrid environments to efficiently monitor users, entity behavior, and activities with learning-based analytics.

Seamless integration with other Microsoft security products

Microsoft Entra ID Protection data can be exported or integrated with other tools for further investigation and correlation. Seamless integration with Microsoft security products such as Microsoft Defender, Microsoft Graph API, and Microsoft Sentinel, as

well as third-party apps, helps correlate alerts and enable unified remediation. You can integrate Microsoft Entra ID Protection alerts with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation. This integration brings a consolidated view of risk users, risk events, and vulnerabilities, with the ability to remediate risk immediately and set policies to auto-remediate future events. The service is built on Microsoft's experience with protecting consumer identities and gains tremendous accuracy from the signal from over 13 billion logins a day.

Conclusion

Safeguarding against compromised identity attacks is crucial as your digital footprint expands and the evolving threat landscape targets identities. Enhance the security of your digital identities with Microsoft Entra ID Protection, a comprehensive cloud-based identity solution that effectively prevents identity compromise and reduces risk exposure in real time. Take immediate action to fortify your cybersecurity defenses by implementing Microsoft Entra ID Protection, empowering your organization with the necessary tools and strategies to protect your first line of defense and ensure ongoing security for your organization's assets.

→ Start with a Microsoft Entra ID P2 Trial today.

→ Visit the Microsoft Entra ID Protection website for more information.