Microsoft Security

Una fuerza de trabajo moderna requiere seguridad integrada basada en la identidad

Protección contra el phishing y otros ataques basados en la identidad sin comprometer la productividad de los empleados.

Contents

Introduction

Users accessing enterprise assets via insecure home networks and unmanaged devices have long been attractive targets for cyberattacks. Now, with remote and hybrid work environments becoming common practice at many organizations, **threats are growing more sophisticated**. As a result, security teams are increasingly embracing identity-based security models to deliver secure access to enterprise assets without impacting user experience or productivity.

The right strategy involves a modern, integrated approach that combines strong authentication, adaptive policy-based access control, and proactive detection and remediation of identity compromise and misuse.

The need for strong identity-based security

Even before COVID-19, security leaders were looking for alternatives to traditional perimeter-based security to accommodate an increasingly mobile workforce and the ongoing migration of data, applications, and IT infrastructure to the cloud. The pandemic-driven shift to remote work further broadened the attack surface and made organizations more vulnerable to attacks and breaches.

For cybercriminals, the shift presented new ingress and egress opportunities for accessing and exfiltrating enterprise data. Microsoft's **Digital Defense Report** found that nation-state actors are adopting more sophisticated reconnaissance techniques, along with credential harvesting and virtual private network (VPN) exploits. Traditional security controls and polices that worked behind the network perimeter became harder to enforce as sensitive data transitioned from secure enterprise facilities to weakly protected employee homes, systems, and networks.

Identity-related threat activity has increased significantly since the pandemic began. In March 2020 alone **Microsoft detected** 4.9 billion attacker-driven sign-ins and over 150,000 compromised accounts. There has also been a **sharp increase in attacks** involving brute-force methods and business email compromise (BEC) to harvest enterprise credentials. Twenty-eight percent of organizations in a 2020 **Microsoft survey** reported a successful phishing attack on their organization. Often, compromised credentials have been used to access enterprise data or enable future attacks. For example, cyber adversaries have used stolen identity credentials to **target and to spoof high-value individuals** and initiate fraud including illegitimate payments and wire transfers.

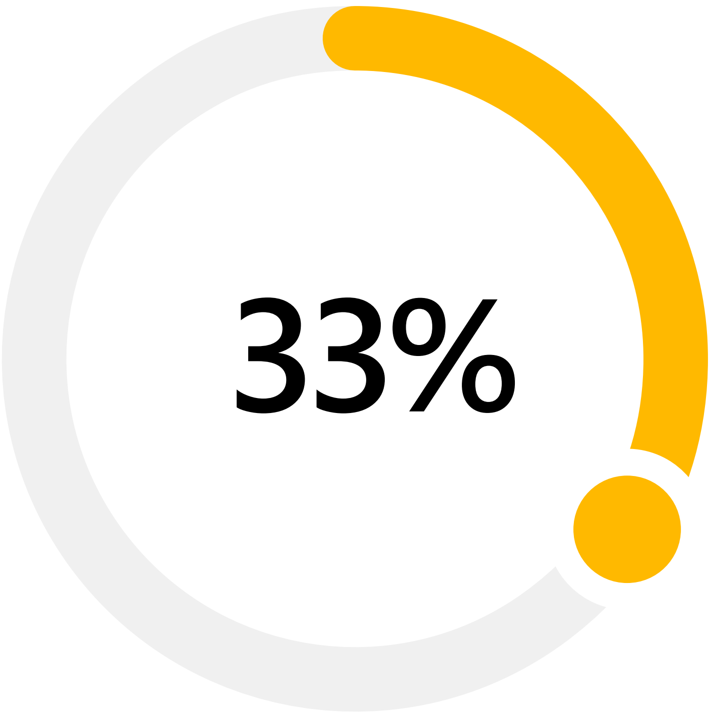
4.9 billion

attacker-driven sign-ins in March 2020 alone

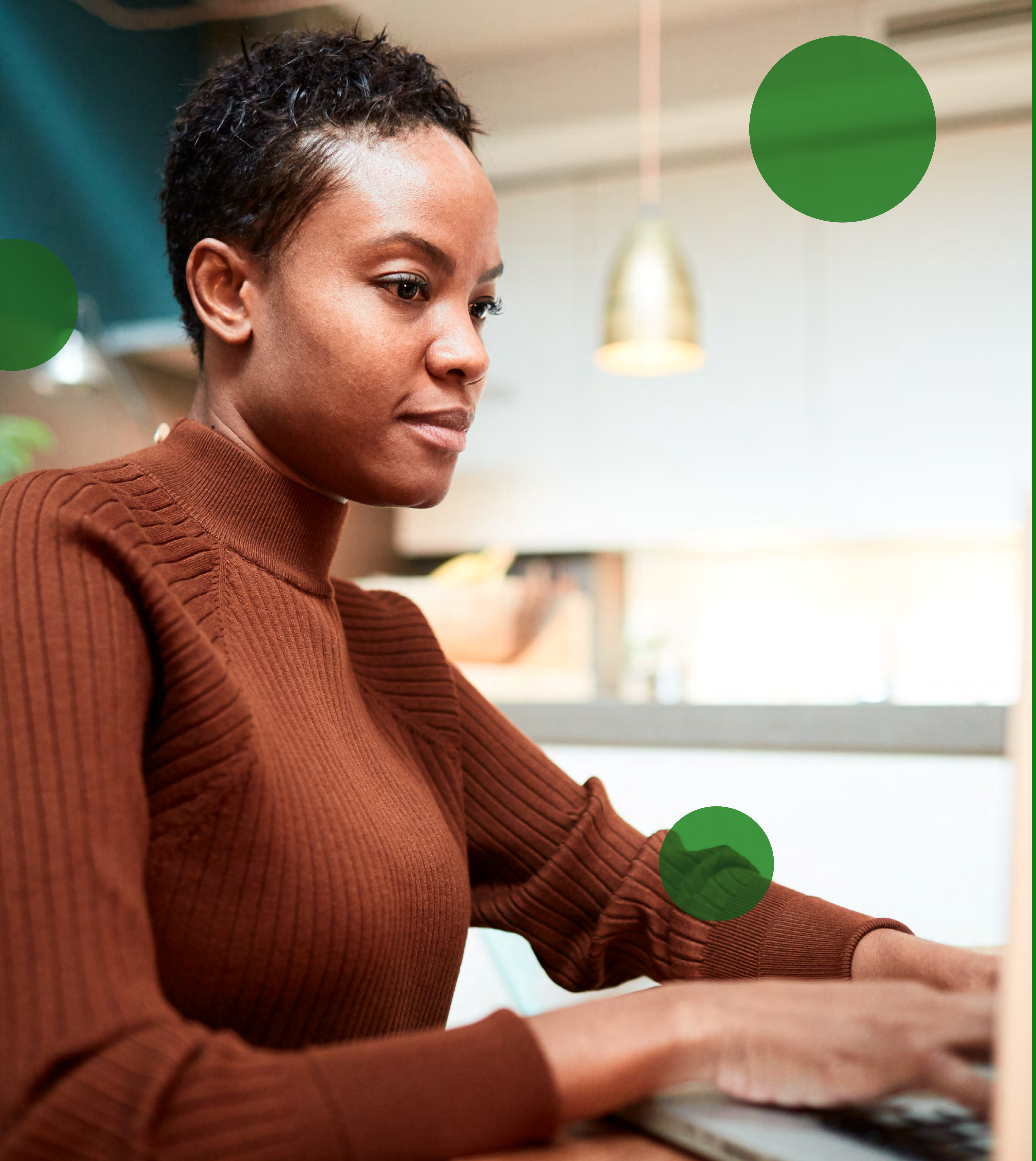
+150,000

compromised accounts

Security managers are aware of the heightened need for stronger access controls and identity protection. They realize that from protecting data behind the enterprise network, security teams now must detect and respond to threats on the extended perimeter of the remote workforce. In IDG's **2020 Security Priorities study**, 33% of security professionals said enhancing identity and access controls was one of their top security priorities in 2021 because of an increase in identity-based attacks targeting remote workers.



33% of security professionals said enhancing identity and access controls was one of their top priorities in 2021



The benefits of integrated, identity-driven security

To give remote workers seamless, secure access to on-premises and cloud-hosted resources, organizations need an integrated, identity-driven security strategy that combines strong authentication with capabilities for proactively protecting against identity misuse.

Critical components include MFA for securing access to enterprise resources, along with support for policies to control what, when, and how a specific user can access information and systems using contextual, real-time information about the user, device, location, and session risk. In addition, the solution should integrate mechanisms for intelligently detecting and responding to compromised accounts and threats using cloud-based AI and automation capabilities.

An integrated approach to security can streamline identity management because it provides administrators with a unified view of data, from multiple sources, through a single console. It gives organizations a way to use both identity-related signals as well as signals across all devices, applications, and networks in an enterprise, enabling consistent policies for access control.

An integrated approach streamlines security across on-premises and multicloud environments, spanning all endpoints, apps, and workloads.

Microsoft’s integrated approach to security: from identity to threat protection

Identity-driven security

Microsoft's identity and access management solution, Azure Active Directory, integrates capabilities for strong authentication and granular access control using real-time adaptive policies and automated identity risk detection and remediation. Microsoft Azure Active Directory helps organizations protect access to resources and data using strong authentication and real-time, risk-based adaptive access policies.

Azure AD helps organizations secure access to resources and data using strong authentication. It enables simpler sign-in via passwordless authentication methods such as Microsoft Authenticator and Windows Hello, which allow users to authenticate securely across mobile devices and the web without requiring a password. Conditional Access in Azure AD enables organizations to control what a user can access, when, and how, depending on factors such as device, location, and real-time risk information.

Azure AD Identity Protection can automatically detect and respond to compromised accounts and other identity-based risks. Azure AD uses advanced machine learning, user and entity behavior analytics (UEBA) capabilities, and connected intelligence on user behavior to monitor continuously for suspicious activity and protect in real-time against breaches from lost or stolen identities.

Integrated threat protection

Interoperation with other Microsoft security products such as Microsoft 365 Defender, Azure Defender and Azure Sentinel can help provide more context for detecting, analyzing, and responding to threats across resources—not just identity—with supporting AI capabilities to help stitch together signals and identify what's most important. The integration enables organizations to compare signals about risky users, sign-ins, and other events with threat data across hybrid environments comprising on-premises and cloud apps.

Integrated threat protection is critical because attackers will use any vulnerability they can find in apps, devices, cloud services, and the users themselves. When a bad actor finds an opening, they will use that initial foothold to escalate privileges and move laterally across a network until they find their target. An integrated, identity-based security system can help detect and respond to such activity—across all endpoints, apps, and workloads, in multiple cloud environments, and on-premises—via a single pane of glass.

Security analysts can use a single dashboard to identify suspicious user activities and correlate data across multiple datasets to detect and respond to multi-stage attacks. Security teams can visualize a breach and gain context on how an attack entered the infrastructure and how it spread, to help prevent future attacks.

Integrated, identity-driven security in action

End-to-end integration, enabled with an identity-driven security model, provides many benefits to organizations across all industries. Here are three examples.

✓ Move beyond simple allow/block decisions to more granular access controls:

Lumen Technologies is leveraging the support for Conditional Access policies in Azure Active Directory to define which apps and what data employees can access from home or while traveling abroad.

✓ Real-time risk assessment and mitigation of identity-based threats:

Bridgewater Associates is using the Identity Protection tool in Microsoft Azure Active Directory to identify unusual and risky sign-in attempts and to block users, reset passwords, or require multi-factor authentication based on signals such as locations and IP addresses.

✓ Build resilience by enabling continuous access evaluation and monitoring:

Global container logistics company Maersk has implemented Azure AD's Identity Protection and Conditional Access tools to flag risky behavior and to take action—such as access revocation—quickly and before it becomes a major problem.

Get started

Close gaps between point solutions and get coverage across your entire multiplatform, multicloud environment.

Learn more

Microsoft