PROTECTING MICROSOFT AZURE AD WITH CROWDSTRIKE IDENTITY PROTECTION

If your organization uses Microsoft Azure Active Directory (Azure AD), these five pointers will help you wrap security around your identities with CrowdStrike Falcon Identity Protection. You will also gain holistic visibility and security control of every human, service and privileged account spread across your on-premises and cloud environment.

1. EXTEND IDENTITY SECURITY BEYOND YOUR PERIMETER

Your regular workforce may be 100% remote, or it may be a mix of on-site and remote workers that may include contractors and vendors. In any case, many are logging into applications from their home and from different locations and devices (that may not be managed by your company) instead of being traditionally bound by your corporate perimeter and NAC.

The CrowdStrike Falcon Identity Protection solution provides full visibility over all application accesses from every user account across both your Azure AD environment and beyond your on-premises Microsoft Active Directory. Falcon Identity Protection can instantly identify risky users that are on-premises but have strong privileges in the cloud.

2. GAIN VISIBILITY INTO ALL CORPORATE APPLICATION ACCESSES

Regardless of where your corporate applications are deployed — on-premises or in the cloud — Falcon Identity Protection provides you with holistic visibility into how these applications are being accessed, based on Azure AD user roles, Azure Groups and Privileges. With Falcon Identity Protection you can continuously assess access behavior, deviations from baselines and user risks from remote locations, gaps in Azure AD authentication protocols, stale users, hybrid users (users on both on-premises AD and Azure AD) and so on.

3. REINFORCE AZURE AD SECURITY POSTURE

With Falcon Identity Protection, you can get a better understanding of your domains' security posture alongside the individual risk scores of every user.

4. BASELINE YOUR REMOTE USER BEHAVIOR ACROSS ON-PREMISES ACTIVE DIRECTORY AND AZURE AD

Falcon Identity Protection helps your Azure AD IAM and security teams to continuously monitor and identify changes in user behavior that are remotely accessing critical resources. Your teams will know which applications are being regularly used by the Azure AD users, and along with their access privileges. Now, you can automatically set a baseline for normal activities that includes regularly accessed destinations and cloud applications.

5. CONTINUOUSLY DETECT THREATS AND INTELLIGENTLY EXTEND AZURE MFA FOR ANY APPLICATION

Falcon Identity Protection continuously tracks and learns access patterns and behavior of every user accessing any application authenticated by Azure AD. When integrated with ADFS, if a user tries to access an application from a blacklisted location, Falcon Identity Protection can enforce conditional access in real time by blocking access or challenging the user with Azure MFA. With Falcon Identity Protection, you can seamlessly extend Azure MFA to any application — including legacy systems, proprietary applications and even on tools like PowerShell. Falcon Identity Protection not only protects on-premises applications and resources, but also works seamlessly with ADFS to protect federated applications.

KEY AZURE AD PROTECTION CAPABILITIES

- Get visibility into both hybrid and cloud-only Azure AD entities — users, groups and privileges
- Automatically analyze Azure AD roles to identify every privileged account
- Understand every user's authentication footprint
- Control access to cloud applications with real-time detection of risks and deviations
- Extend risk-based conditional access capabilities to on-premises resources
- Introduce dynamic conditional access based on continuous risk assessments and baselines for federated applications with Active Directory Federation Service (ADFS) integration
- Ascertain risks from legacy protocol usage to access Azure AD
- Determine Azure logins from endpoints using outdated operating systems
- Get instant alerts for threats across the multiple stages in the attack kill chain including reconnaissance, lateral movement and persistence

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.