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 sign-ins 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 tenant 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 Azure AD Administrative roles, groups, assigned subscriptions, Azure service principals 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) privileged accounts, and so on.

3. REINFORCE AZURE AD SECURITY POSTURE

With Falcon Identity Protection, you can get a better understanding of your tenants' 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 privileges. Automatically set a baseline for normal activities that include 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. Understand Azure service principals' privileges to uncover stealthy privilege paths that could potentially lead to these accounts gaining administrative access to tenants. 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 service principals
- Automatically analyze Azure AD roles to identify every privileged account
- Understand the authentication footprint across 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 sign-ins 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 Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.