Barracuda Identity Resilience

Protect, detect, respond to, and recover from identity-based attacks, without adding needless complexity

Identity has become the primary attack surface for modern organizations. As businesses adopt cloud services, remote work and SaaS applications, attackers increasingly bypass traditional perimeter defenses by abusing valid credentials, misconfigurations and identity infrastructure. A single compromised identity can lead to privilege escalation, lateral movement, ransomware, and prolonged business disruption.

Barracuda Identity Resilience addresses this reality with a layered, outcome-driven approach. By combining identity risk visibility, Zero Trust access enforcement, continuous threat detection and response, and rapid identity recovery into a single, integrated solution, Barracuda helps businesses reduce the likelihood, impact and downtime of identity-based attacks, without requiring large security teams or complex tooling.

Why identity resilience matters now

Identity attacks are no longer rare or isolated events; they are the dominant breach vector:

- **Compromised credentials are the initial entry point in most data breaches**, making stolen identities the most common way attackers gain access.
- **Cloud identity attacks have surged dramatically**, with billions of password-based attacks targeting cloud identity systems every month.

For mid-market and enterprise organizations that rely heavily on Microsoft Entra ID, these trends create a clear mandate: protecting identities is no longer just about authentication, it's about resilience. When prevention fails, organizations must be able to detect misuse quickly, contain the blast radius and restore identity services quickly, to keep the business running.

Common identity security challenges

Security leaders and IT teams face persistent identity-related challenges, including:

Limited visibility into identity risk

Misconfigurations, excessive privileges and risky identity settings often go unnoticed until exploited.

Overreliance on perimeter and MFA controls

Attackers increasingly bypass MFA or use valid credentials, rendering traditional controls insufficient.

Slow detection of identity misuse

Identity-based attacks often blend in as legitimate activity, increasing dwell time and impact.

High operational impact of identity incidents

Accidental deletions, malicious changes or directory compromise can halt access to applications and disrupt business operations.

Resource constraints

Many organizations lack the time, staff or expertise to manage complex identity security stacks or operate a 24/7 SOC.

Barracuda Identity Resilience: Overview

Barracuda Identity Resilience delivers end-to-end protection for Microsoft Entra ID environments by unifying prevention, protection, detection, response, and recovery within the BarracudaONE platform.

Instead of stitching together disconnected tools, organizations gain a single, integrated solution that helps them understand identity risk, limit exposure, detect threats early, respond decisively, and recover quickly when incidents occur.

How the bundled solutions work together

Barracuda Identity Resilience aligns security capabilities across the full identity-attack lifecycle:

Identify: Reduce exposure before attackers strike

Identity Security Posture Management continuously analyzes Microsoft Entra ID configurations to uncover misconfigurations, weak controls and risky settings. Security teams receive clear, prioritized insights and remediation guidance, helping them address the most critical risks first and reduce the likelihood of compromise.

Protect: Enforce least-privilege access everywhere

SecureEdge Private Access applies Zero Trust Network Access (ZTNA) principles to identity-driven access. Even when credentials are valid, access is restricted to only approved applications and resources, reducing lateral movement and preventing attackers from freely navigating the environment.

Detect: Identify identity-based threats in real time

Barracuda Cloud XDR continuously monitors authentication activity, identity behavior and cloud signals to detect suspicious logins, privilege abuse and anomalous behavior that traditional tools often miss. Threats are correlated across signals to surface high-confidence incidents quickly.

Respond: Contain threats and reduce dwell time

Cloud XDR delivers guided and automated response actions, supported by Barracuda's 24/7 security operations expertise. This helps security teams respond faster, contain compromised identities and limit business impact, without adding operational burden.

Recover: Restore identity services with confidence

Entra ID Backup Premium ensures organizations can recover quickly from accidental deletions, misconfigurations or malicious changes. Granular, point-in-time recovery of Entra ID objects and configurations enables rapid restoration of access and minimizes downtime.

Key customer benefits and outcomes

With Barracuda Identity Resilience, organizations can:

Reduce identity risk proactively

Identify and remediate misconfigurations and excessive privileges before they are exploited.

Limit the blast radius of compromise

Enforce least-privilege access and Zero Trust controls that contain attackers—even when credentials are stolen.

Detect and respond faster to identity misuse

Gain continuous visibility and expert-backed response to identity-based threats.

Recover quickly and maintain business continuity

Restore critical identity services rapidly after incidents, errors or attacks.

Simplify identity security operations

Replace fragmented tools with a unified, easy-to-use platform designed for resource-constrained IT and security teams.

Take the next step

Identity compromise is inevitable, but business disruption doesn't have to be.

See how Barracuda Identity Resilience helps businesses protect Microsoft identities from end-to-end and stay operational when it matters most.

Talk to a Barracuda expert right now.