Maximizing Security ROI with Reach: Unlocking the Full Potential of Microsoft Security Ecosystem

Adopting the Microsoft security products ecosystem provides a powerful suite of security features, but maximizing ROI across these solutions can be a challenge for customers.

The challenge

Navigating the Complexity of Microsoft's Security Ecosystem

The breadth of capabilities across multiple products is a great benefit to customers. However, the ever-changing productization of these capabilities, including how they integrate, when to best use them, and where they are located, can overwhelm security teams.

Reach integrates with Microsoft's security tooling through Microsoft services and APIs, programmatically identifying new features and options from Microsoft. Customers benefit with optimized and tailored configurations, based on their unique threat profile across the Microsoft suite.

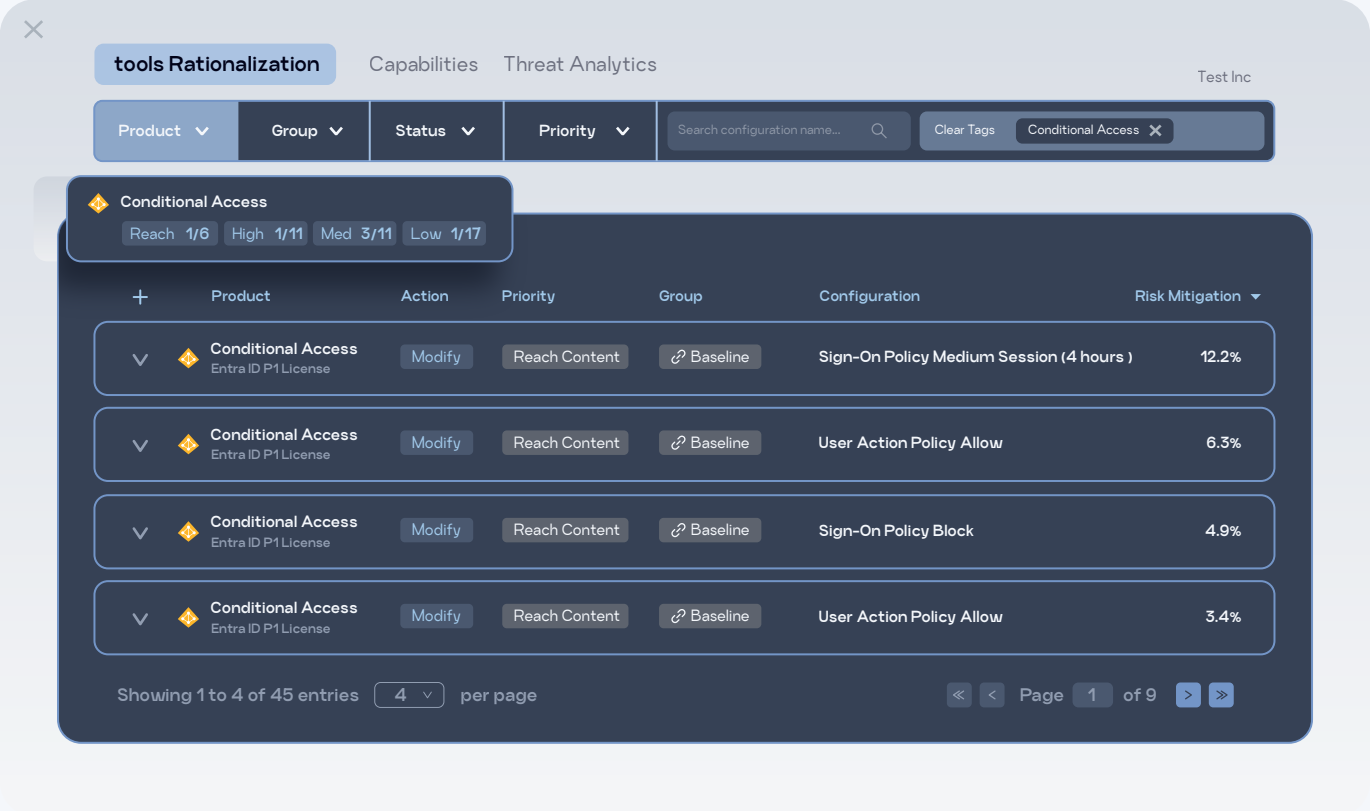
Reach provides cross-product configuration telemetry, enabling seamless configuration across different tools. These configurations are mapped to specific attack types and stages, such as phishing or ransomware, ensuring comprehensive protection. With Reach, users no longer need to stay on top of release notes, feature enhancements, or complex API connection issues which helps to save time and reduce operational overhead.

Overcoming Configuration Challenges for Maximum Security

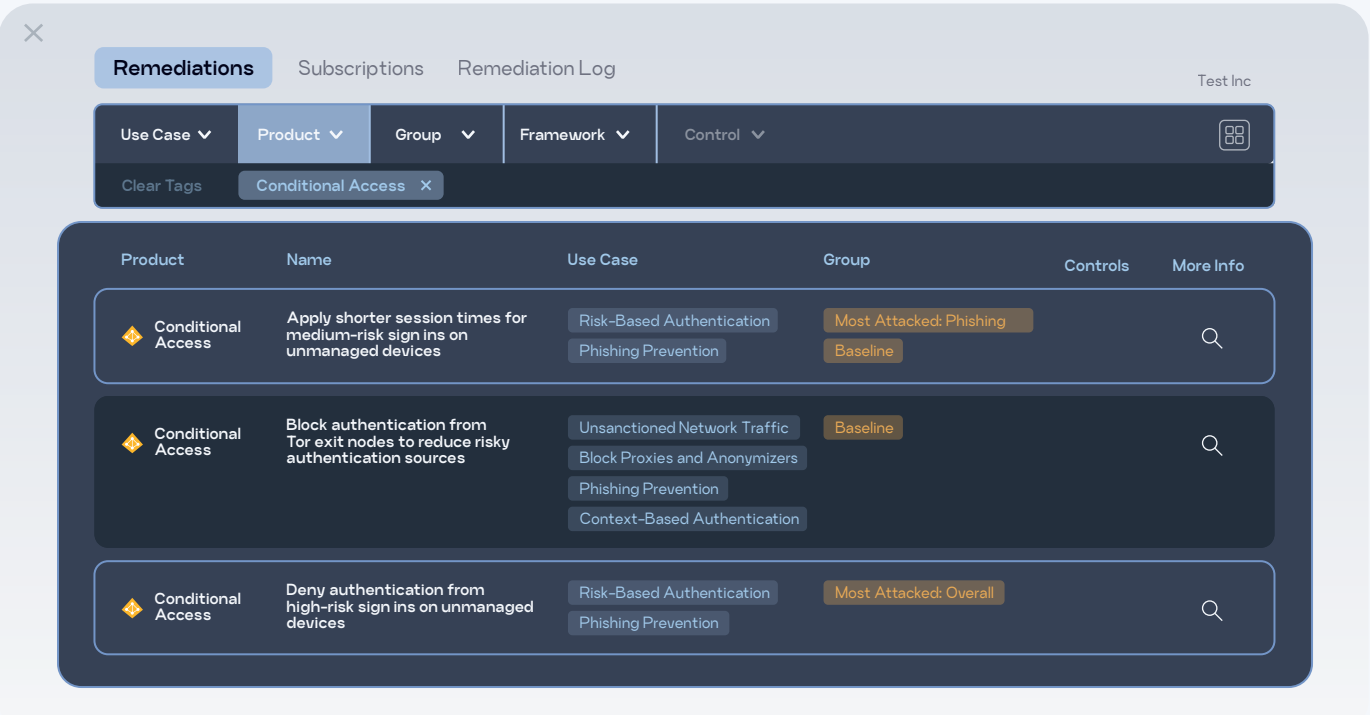
Features like Conditional Access, and Defender for Endpoint require fine-tuned configurations across multiple solutions. Effective prioritization of capabilities can be difficult for teams to create as it requires deep understanding of products.

reach.security
562. 348. 5984
sales@reach.security

Reach simplifies the creation of complex policies within the Microsoft suite by eliminating guesswork. By analyzing real customer attack data and existing product configurations, Reach identifies each organization's unique threat profile and recommends the best configuration options.



It goes further by handling the "last mile," automating remediation, fine-tuning configurations, and deploying them seamlessly which saves time and ensures optimal protection.



Maximizing Value from E3/E5 Licensing ina Dynamic Threat Landscape

The extensive capabilities of both E3 and E5 licenses make it difficult for organizations to assess the security benefits specific to their threat landscape. Without a clear view into current risks and how existing capabilities address them, companies struggle to determine if upgrading to E5 will enhance their security posture.

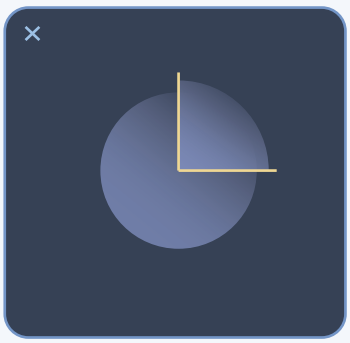
Reach empowers organizations to make the most of their Microsoft licensing by providing actionable insights and tailored recommendations:

Interrogation of Current Capabilities:

Reach evaluates the current capabilities of the existing E3/E5 environment, analyzes how the current licenses are being utilized, and identifies opportunities to leverage E5 features to enhance the organization's security posture.

Optimization of Existing Licenses:

Reach provides continuous insights to help organizations maximize the ROI of their E3 and E5 licenses. For example, it can identify and recommend deploying specific E5 capabilities to the most frequently targeted users, ensuring the upgrade achieves maximum impact.



Data-Driven Upgrade Justification:

Reach translates attacks targeting specific users and assets into actionable insights, demonstrating the value of E5 features like advanced Conditional Access policies. This empowers organizations to make informed upgrade decisions grounded in real, measurable security needs.

Getting Started with Reach

To join the community of customers enjoying the benefits of Reach and learn more about how it can transform your security posture, visit:

Reach.Security/try-reach.

reach.security | 562. 348. 5984 | sales@reach.security