Dynamic Workforce Risk and Challenges in Tracking High-Risk Users

Organizations are continually challenged by dynamic risks within their workforce, especially among groups identified as Most Attacked People (MAP). External adversaries specifically target these users, dynamically shifting their tactics and focus based on evolving motivations. This targeting results in a disproportionate amount of end-user risk residing within a small percentage of the workforce—a pattern that is also constantly changing. Reach's analysis reveals that 80-90% of threats relate to just 3%-5% of the organization's population.

With this concentration of risk, there are opportunities to enhance security measures efficiently. By focusing on these high-risk groups, Reach helps organizations streamline their security efforts, delivering significant improvements to their security posture. This targeted approach builds trust and reduces operational complexity, allowing for more effective management of the ever-changing threat landscape.

Common Challenges

Knowing who is being attacked: Continuously identifying and updating the list of high-risk users is a formidable challenge due to the dynamic nature of risk and the practical limitations of existing security infrastructures. On average, about 20% of the users in a company's most attacked group change each month. For example, if a company has 100 users typically in their MAP group, approximately 20 of these users will be different from one month to the next, reflecting the shifting focus of cyber threats.

Knowing how they are being attacked: The challenge for organizations is not only identifying high-risk users but also effectively integrating data from various security tools to track these risks over time. This complexity is compounded by the need to continually update and refine security measures from the enterprise security estate to address dynamic threats.

Knowing what to do about it: Beyond identifying high-risk users, there is a significant challenge in leveraging this information to tailor security controls effectively, conduct targeted training, and run phishing simulations to bolster defenses specifically where they are most needed. This challenge is compounded by the constant flux in threats, users and features available to you from the vendors protecting the organization.

Solving the Challenge is within Reach

Reach leverages comprehensive data integration and sophisticated tracking to address the dynamic risks associated with the most attacked individuals within an organization. This targeted approach not only enhances the accuracy of risk identification but also ensures that security measures for the workforce are continuously updated and effectively deployed.

Reach

Drive Outcomes with Reach

Dynaminc User Risk Monitoring: Reach continuously updates its identification of MAP groups by syncing with the central record of identity (e.g. Active Directory, Azure Active Directory, Google Workspace, Okta), to understand the threats facing your users.

Seamless Integration & Policy Management: Reach seamlessly syncs high-risk user data with the central record of identity and translates user risks into device policies to protect high-risk users with deployable security configurations.

Proactive Threat Management: Reach precisely tracks email threats by analyzing their paths and recipients, enabling faster and more accurate responses to phishing and other email-based attacks.

reach.security/connect
415.828.7475
sales@reach.security

Reach Capability	Description
Continuous Risk Assessment	Reach conducts ongoing assessments of user risk profiles by integrating data from security tools across the enterprise. This continuous monitoring helps identify and track shifts in the threat landscape, ensuring that the most vulnerable users are always under watch. Reach leverages real-time data syncing with AD to keep the MAP groups updated, significantly reducing the window of exposure.
Targeted Threat Management	Reach utilizes advanced data analytics to dissect email traffic and detect targeted threats. By collapsing mailing lists and tracing the final recipient of a potentially harmful email, Reach pinpoints high-risk users more accurately than conventional methods. This unique approach allows for more precise and proactive threat mitigation strategies.
Integrated Security Policy Enforcement	Reach not only identifies high-risk users but also enables direct integration of this data into security policies across platforms like AzureAD and CrowdStrike. By translating user risk into specific device-level policies, Reach applies a holistic security strategy that is both user and device-aware ensuring that protective measures are as personalized and effective as possible.

Reach Security is revolutionizing the cybersecurity landscape by empowering organizations to maximize the ROI of their existing security products. With a focus on optimizing what organizations already own rather than adding complexity with new tools, Reach Security is committed to simplifying cybersecurity, reducing operational costs, and enhancing protection against evolving threats. Founded by cybersecurity experts with venture-backing from leading investors and cybersecurity luminaries, Reach Security is setting a new standard for cybersecurity efficiency and effectiveness. For more information, visit: **Reach.Security**.

Reach

Get Started!

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/connect
415.828.7475
sales@reach.security