Human-centric Exposure Management

Know the threats facing your people. Automatically remediate and reduce their risk exposure using Reach.

The challenge

The most vulnerable asset in an organization is its people. They're also the most sensitive to your security controls.

Organizations have more tools than ever to protect people from attacks and misconfigurations. However, organizations must tailor and deliver dynamic security posture fit for them.

When it comes to exposure management, modern enterprises are struggling with three challenges:

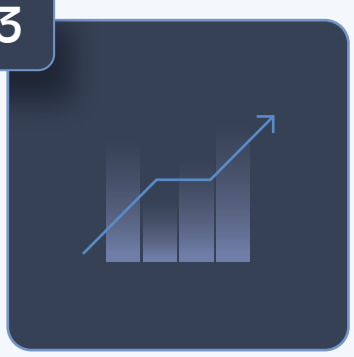
1

Proliferation of access within a perimeter-less world.

2

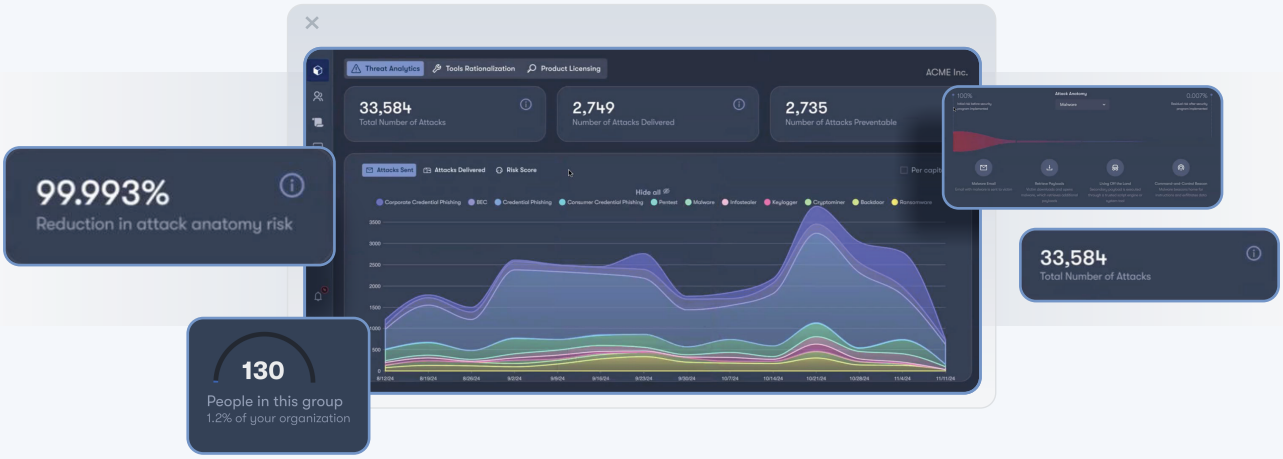
An attack surface constantly changing.

3



An overwhelming number of technical controls to maintain over an increasingly complex organization.

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



Reduce human risk exposure with:

Immediate identification of risks across enforcement points

Automatically understand risk exposure of your people by connecting to tools with the correct visibility.

Automated prioritization based on your unique threat profile

Gain the ability to reduce risk based on the threats relevant to you.

Effortless remediation

Bridge the gap between tool owners and security, with remediations that have a deep understanding of your tools, their configurations and your environment.

Immediate identification of risk exposure

Digital transformation and the desire to work from anywhere have changed the dynamics of protecting people in an organization. People are connected to the organization's systems, data and each another in more ways than ever. This makes identifying risk exposure across all channels necessary, but extremely challenging.

With Reach's Most Attacked People exposure management capabilities, security teams can easily identify where risk exists by correlating security events, threat forensics, and end-user data across email, network, endpoint, SaaS application, and Identity Access Management channels.

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

Automated prioritization based on your unique threat profile

What is relevant to an organization drives priority and action. Determining the unique threat profile of an organization and controls that can be applied takes expertise in the threat landscape, the tools owned and the risk profile of the organization.

Reach combines your Most Attacked People exposure to the unique threat profile and tool capabilities at your disposal to prioritize and provide remediation actions. Modeling from Reach automates the research done by security engineers and architects who need to consider billions of seemingly disparate data points.

Effortless remediation

All forms of remediation require a deep understanding of existing configurations, licensing, and risk context. Each piece of data takes time to aggregate and understand at an individual and collective level. At Reach, we dedicate as much effort to ensuring remediation steps are precise and tailored to customer needs as we do automating the recommendations. This focus is essential because, in many cases, the biggest challenge lies in convincing stakeholders that the proposed changes deliver greater rewards than the risks they pose to the business. Reach's remediation capabilities include customer-context driven deployment guides, change tickets, and deployment options.

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