Reach

Security Impact Summary: Reducing Risk and Maximizing Value with Reach

This document highlights the type of visibility and impact Reach delivers within the first few months of deployment. The example shown is based on a demo environment and reflects what many customers observe shortly after onboarding and operationalizing Reach: clear visibility into missed controls, underutilized tools, and prioritized actions to reduce risk.

1. Value Delivered

The metrics below reflect outcomes from a representative deployment and are based on what Reach surfaces through its analysis of existing tools and controls. These metrics illustrate the types of insights and improvements Reach enables early in the engagement.

91	14	6/10	39%	$534k
Outstanding Controls	Deployed Recommendations	Capabilities in Use	Risk Reduction	Avoided Breach Costs

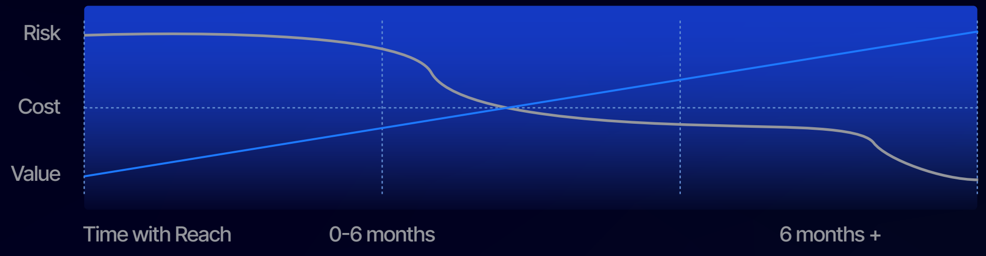
Reach rapidly uncovers unseen exposure and underused capabilities across your security stack starting with identity, email, endpoint, and firewall tools. Within minutes of connecting, Reach highlights where risk hides and what's not being used.

- Controls they already **have access to but aren't using**
- How much of the paid-for licensed tool capabilities are **being leveraged**
- The **real-world risk reduction** enabled by even partial deployment

2. How Reach Reduces Risk and Unlocks Value

Reach helps reduce risk and increase the value of existing security investments by identifying underused controls and supporting targeted deployment. The chart below reflects a common pattern observed across environments: as controls are implemented, risk declines and value increases, all while cost remain steady. This highlights the impact of optimizing what's already in place, rather than investing in more tools.

Strategic Deployment Drives Compounding Value Over Time



ASSESSMENT GUIDE

Reach Helps Customers

- Identify security blind spots from misconfigured and underused security and IT tools
- Prioritize action based on real-world risk and control capabilities
- Guide remediation to rapidly deploy changes and improve security posture
- Continuously validate to detect configuration drift, keep defenses aligned to policy, and maintain a strong security posture

reach.security

Reach reduces risk by identifying unused but available security features and helping teams to deploy them in a structured way. These features are often already licensed but not fully configured or turned on. At the same time, Reach improves value realization by:

- Highlighting which tools and controls are underutilized
- Mapping risk reduction to every control and recommendation
- Tracking posture and progress across every tool and integration

The result is a steady increase in security posture using existing infrastructure to maximize value while reducing risk.

3. Examples of What Reach Surfaces & Supports

The table below outlines examples of what Reach commonly identifies across core security domains and how those insights can translate into action. While the sequence and priorities vary by customer, this highlights the type of control-level visibility and remediation Reach supports from the outset.

	Phase 1 Identity CSP Block Zones & EDR Recommendations Value Realized 4 – 8 Weeks	**Phase 2** Deploy MAP Groups Value Realized 2 – 4 Months	**Phase 3** Implement Firewall Recommendations Value Realized 4 – 8 Months
Action	Deploy Reach recommendations for CSP Network Zone block controls Review sign-on policies utilizing risk and behavioral attributes Implement Detection Engine controls and custom logic rules	Implement MAP group recommendations in a phased approach creating more stringent policies on disproportionately attacked users	Deploy Palo Alto Next Gen Firewall security controls not currently in-use Apply URL filtering blocks
Outcome	Restrict unauthorized access and reduce the risk of account takeovers, unauthorized logins, and credential abuse Enhance threat detection with custom high-fidelity behavioral detections	Reduce exposure to targeted attacks such as phishing, credential theft, and endpoint exploitation Enhance identity protection, endpoint resilience, and email security minimizing the likelihood of compromise	Improve security hygiene Prevent access to malicious & high-risk sites Zero Trust enforcement
Products	okta SentinelOne	okta CROWDSTRIKE SentinelOne proofpoint.	paloalto NETWORKS

Only With Reach

- Real-world threat context vs. generic best practices
- Purpose-built MastermindAI vs. off-the-shelf models
- Actionable changes across your stack vs. shallow visibility
- Deep, multi-tool integration vs. shallow visibility
- Continuous validation vs. point-in-time reports

Get Started!

reach.security/try-reach

Join the community of customers enjoying the benefits of Reach and learn more about how to reduce risk, optimize ROI and drive trust in your organization.

reach.security