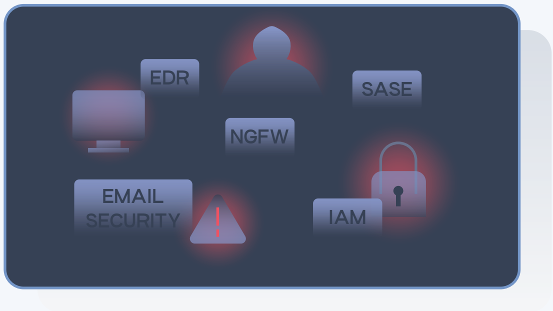
Turning Intelligence Into Action:

Threat-Informed Defense with Reach

The challenge **Knowing the Threat Isn't the Same as Stopping It**

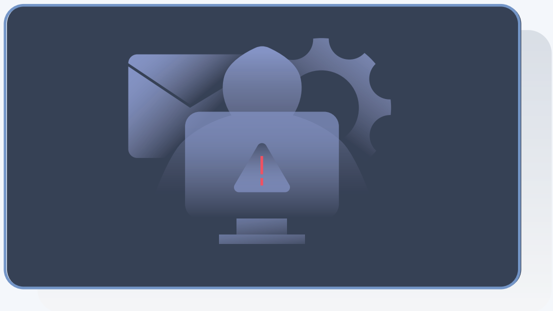
Security teams often have visibility into attacker behavior—like initial access methods, persistence techniques, or lateral movement—but turning that intelligence into practical defense remains a major challenge.

Organizations struggle to:



Map threats to meaningful defensive changes

It's difficult to connect TTPs (Tactics, Techniques, and Procedures) with the specific controls that can stop them. Those who analyze threats typically focus on detection, not prevention – and the people responsible for configurations may not be fluent in adversary tradecraft.

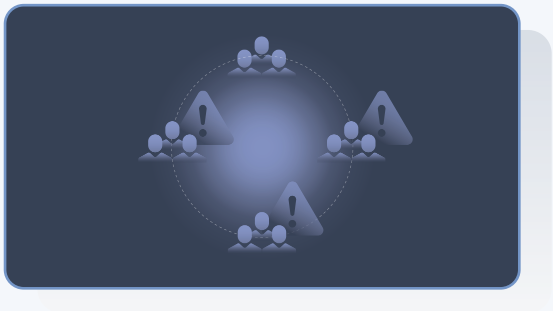


Identify exposures across fragmented tools

Defenses live in multiple products – EDR, IAM, email, firewalls – and each uses its own model and language. Without a unifying view, gaps go unnoticed.

Prioritize configuration changes by impact

Even when teams understand the threat, they can't easily determine which specific changes will reduce the most exposure to it.



Align efforts across cross-functional teams

Communication breaks down between research, engineering, operations, and delivery – slowing response and increasing risk.

The result

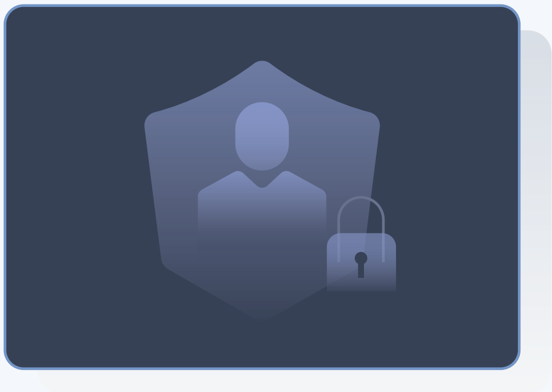
Threat Intelligence lives in slides and dashboards, while defenses remain misaligned and underutilized.

Overcoming the Gap with Reach

Threat-Informed Defense, Delivered as a Program

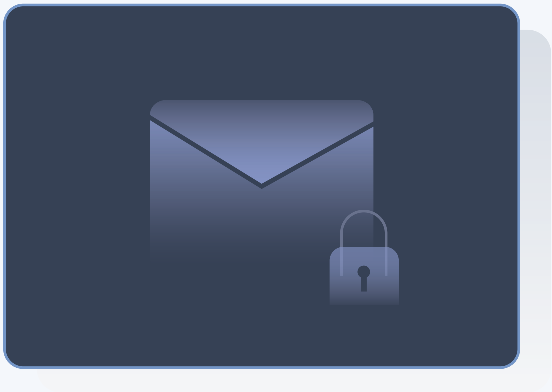
Reach turns Threat Intelligence into configuration action. By analyzing attacker tools, techniques, and procedures (TTPs), Reach creates Threat Programs – curated sets of product-specific recommendations designed to mitigate active threats.

Each Threat Program includes tailored configurations across tools like:

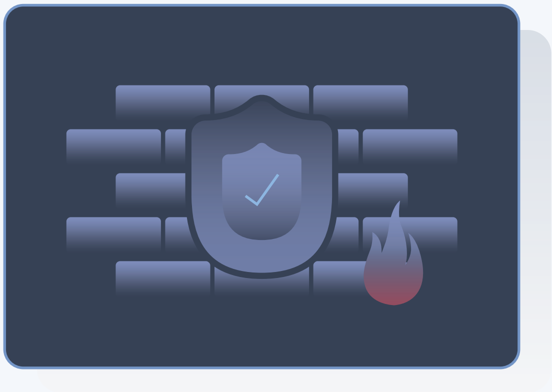


Identity & Access Management (IAM)

Endpoint Detection & Response (EDR)



Email Security



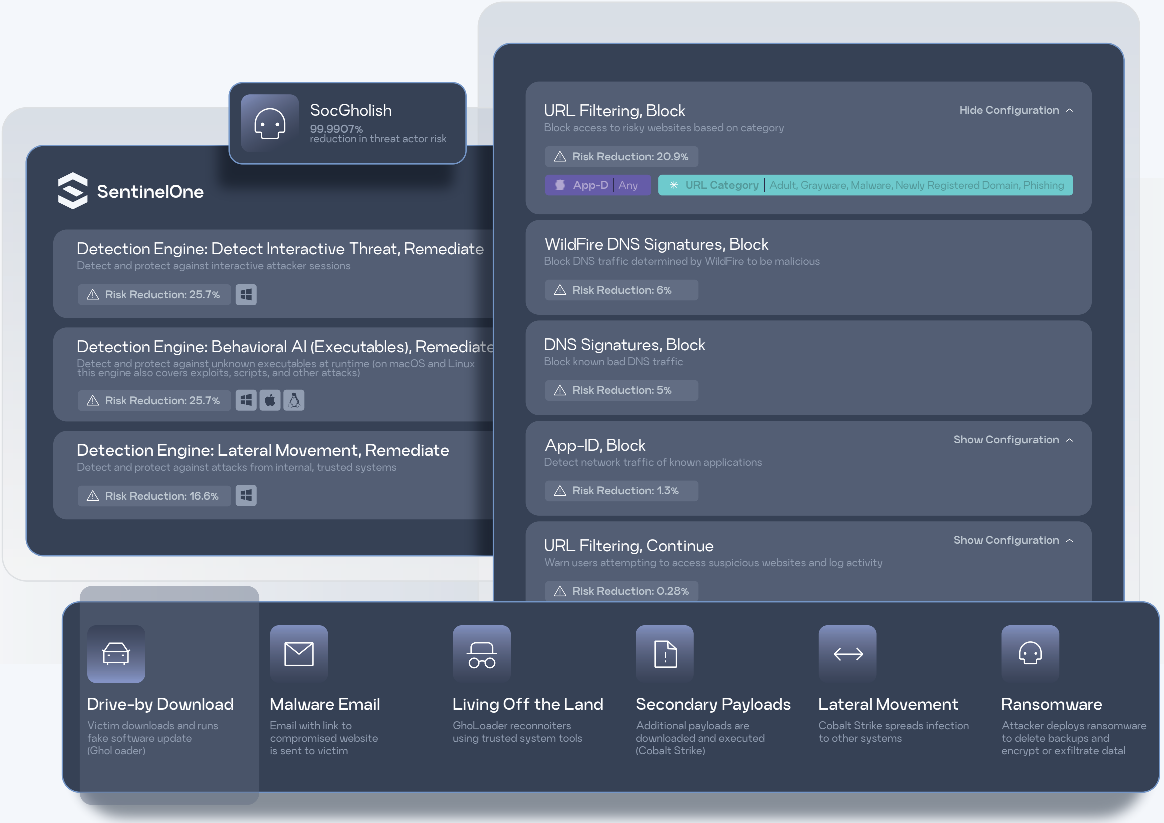
Network Security

Reach ensures that teams are not just aware of threats – but ready for them using the tools they already own.

How It Works

From Threat Actor to Defense Plan in One Workflow

When a known threat actor like **SocGholish** is observed targeting environments, Reach builds a guided remediation plan based on real tactics and tools:



SocGholish
99.9907%
reduction in threat actor risk

SentinelOne

Detection Engine: Detect Interactive Threat, Remediate
Detect and protect against interactive attacker sessions
⚠ Risk Reduction: 25.7%

Detection Engine: Behavioral AI (Executables), Remediate
Detect and protect against unknown executables at runtime (on macOS and Linux this engine also covers exploits, scripts, and other attacks)
⚠ Risk Reduction: 25.7%

Detection Engine: Lateral Movement, Remediate
Detect and protect against attacks from internal, trusted systems
⚠ Risk Reduction: 16.6%

URL Filtering, Block
Block access to risky websites based on category
⚠ Risk Reduction: 20.9%
App-D | Any
URL Category | Adult, Grayware, Malware, Newly Registered Domain, Phishing

WildFire DNS Signatures, Block
Block DNS traffic determined by WildFire to be malicious
⚠ Risk Reduction: 6%

DNS Signatures, Block
Block known bad DNS traffic
⚠ Risk Reduction: 5%

App-ID, Block
Detect network traffic of known applications
⚠ Risk Reduction: 1.3%

URL Filtering, Continue
Warn users attempting to access suspicious websites and log activity
⚠ Risk Reduction: 0.28%

Drive-by Download
Victim downloads and runs fake software update (Ghol oader)

Malware Email
Email with link to compromised website is sent to victim

Living Off the Land
GhoLoader reconnoiters using trusted system tools

Secondary Payloads
Additional payloads are downloaded and executed (Cobalt Strike)

Lateral Movement
Cobalt Strike spreads infection to other systems

Ransomware
Attacker deploys ransomware to delete backups and encrypt or exfiltrate datal

Threat Profile Creation

Reach analyzes open-source intelligence and internal research to identify relevant TTPs

Control Mapping

TTPs are matched to defensive controls across connected products – eliminating guesswork and reducing operational overhead

Configuration Recommendations

Reach surfaces specific, high-impact recommendations tailored to the customer's environment

Program Delivery

Customers can view, deploy, and track progress across all controls in a unified dashboard

Each Threat Program includes rationale, references, and mapped MITRE ATT&CK techniques to help drive alignment across security, GRC, and platform teams.

Why It Matters

Proactive Security Aligned to the Threats That Matter Most

Threat Informed Defense help teams:

- Prioritize configuration changes based on real adversary behavior
- Achieve fast wins with high-confidence control sets
- Communicate clearly across stakeholders using a threat-driven narrative
- Stay ready for the threats most relevant to their environment

With Reach, defense becomes a continuous, intelligence-led process – not a reactive fire drill.

Getting Started with Threat-Informed Defense

To learn how Reach helps operationalize threat intelligence through tailored configuration programs, visit:

Reach.Security/try-reach.