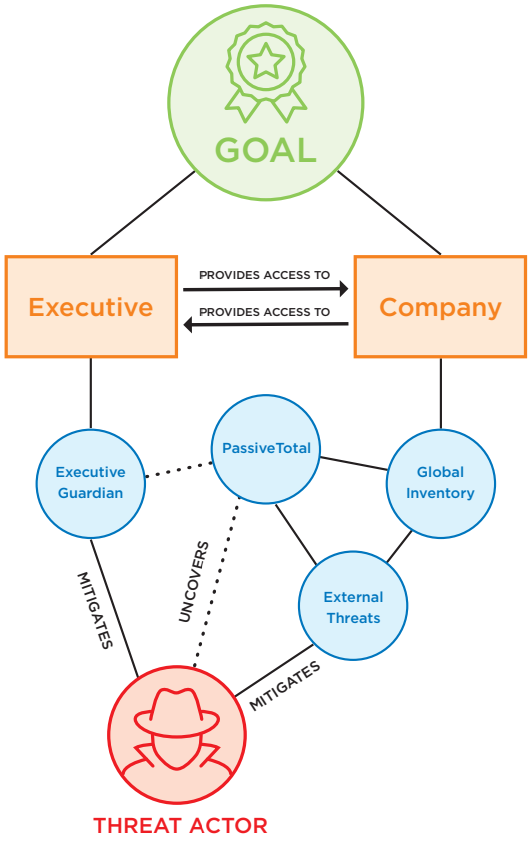
RISKIQ®

RiskIQ Incident Investigation and Intelligence (i3) and Executive Guardian™

Vigilance in the Digital World, Security in the Physical World

RiskIQ's *Incident Investigation and Intelligence (i3)* team's attack surface management service and products discover and investigate your company's true risks and vulnerabilities. We partner with your physical and cyber security teams enabling them to "speak the same language" and develop a process that better safeguards your company and the individuals with the most risk.

To mitigate threats, organizations must understand their entire attack surface.



What We Provide, i3:

- **Incident Response**
  - Support for your internal investigation team
  - Reactive and capable of mitigating high threat incident
- **Investigation Services**
  - Sophisticated lenses on internet data and exposures
  - Travel itinerary vetting and monitoring during trip
- **Intelligence**
  - Tailored intelligence reports
  - Annual risks and vulnerability reports
  - Counterintelligence reports and briefings
  - Threat-actor monitoring
  - Threat attribution, assessments, mitigation, and management

We Work for You and Partner with Your Security Department - i3

Partnering with RiskIQ enables businesses to enjoy the benefits of having a fully-staffed virtual security department for less cost. At RiskIQ, *Incident Investigation and Intelligence (i3)* security services are the backbone of what we do for more than 300 individual clients.

You gain a complete, full-service *Incident Investigation and Intelligence (i3)* department. That relationship includes experienced leadership with C-level clients and subject-matter experts from multiple security and intelligence disciplines. The greatest benefit is that you immediately have access to a team of highly trained experts with advanced capabilities and tools, many times for the cost of one employee.

Partnering with RiskIQ i3 is **scalable**, allowing companies to better **manage cash flow and investment**. It is our mission to staff experienced, trained individuals to remain current on the latest threat strategies.

You Need an Attack Surface Management Strategy

As cyber and physical security converge, a robust and holistic attack surface management strategy needs to take into account more than just the company's digital assets. Companies must also understand where the high-value targets reside within their hierarchy, and what their exposure rests. Only after these key figures have been identified can threats to your company's most critical assets be mitigated.

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com