Infosec is a Chess Match.

These **Five Security** Intelligence Moves Win the Game

Today, those who understand the relationships between an organization's dynamic, complex, and unique internet presence and the global threat landscape—good guy or bad guy—are the ones who win the match.

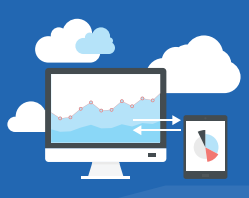
Modern, dynamic security intelligence should have five critical elements fully loaded and operationalized. Here's a game plan to help organizations define themselves, their risks and dependencies, and those targeting them to stay ahead of their adversaries:

MOVE 1: Know Yourself

Attack Surface Intelligence

Gain visibility into each digital asset and connection across your digital footprint.

The global remote desktop software market is projected to reach **$4.69B** by 2027, a CAGR of 15.1%



Cloud IT infrastructure is expected to grow at a five-year CAGR of 10.6%, reaching **$110.5B** in 2024 and accounting for 64.0% of total IT infrastructure spend

Attacks on web applications represent **39%** of all breaches

Attack surface intelligence identifies digital relationships within and throughout an organization's unique slice of the worldwide attack surface—internet-exposed hardware, software, and underlying components. This real-time view speeds up triage, analysis, and incident-response by identifying how threats and vulnerabilities connect to your organization.

MOVE 2: Know Your Allies

Third-Party Intelligence

Understand the risks across your digital supply chain and how they impact your security posture.

70% of IT professionals indicated a moderate-to-high level of dependency on external entities that might include third, fourth, or fifth parties

53% of organizations have experienced at least one data breach caused by a third party

40% of security breaches are now indirect, as threat actors target the weak links in the supply chain or business ecosystem

<10% of deals globally contain cybersecurity due diligence today

With a real-time graph of the internet, organizations can go far beyond just a static reputation score that uses potentially murky or inconsistent criteria. This third-party intelligence provides a layered view of risk across your digital supply chain using precise exposure indicators to give teams a deep, nuanced, and contextualized view of third-party dependencies.

MOVE 3: Know Your Enemies

Cyber Threat Intelligence

Identify the threat systems and actors targeting your organization across the global attack surface.

In many cases, tracking threat infrastructure is more important than the threat groups themselves. Different groups will recycle and share infrastructure—IPs, domains, and certificates—and borrow each other's tools, such as malware, phish kits, and C2 components, tweaking and improving them to fit their unique needs.

560,000 new pieces of malware are detected every day

In 2020, the number of detected malware variants rose by **62%**

The number of phishing kits advertised on underground cybercrime marketplaces **DOUBLED** between 2018 and 2019

RiskIQ detects a Cobalt Strike C2 server every **49 minutes**

MOVE 4: Know Your Ever-Changing Surroundings

Security Operations Intelligence

Enrich core security solutions with extended enterprise intelligence to improve investigation and response.

SecOps intelligence built with precomputed digital relationships creates knowledge at scale, a guided path for security teams. This way, they can then focus only on what matters to their organization, shrinking the global attack surface from impossibly large to manageable—and shrinking their unreasonable workload in the process.

Phishing Domain detected every **6** minutes across 478 unique brands

5.5 domain infringements every minute across 170 unique brands

14.6 COVID-related hosts created very minute

RiskIQ has observed **61,651,839,751** new hosts over the past year

MOVE 5: Know Your Weaknesses

Vulnerability Intelligence

Identify which vulnerabilities matter, how critical they are, and how to align all the teams in your organization.

Next-gen vulnerability intelligence is the glue that connects all the teams across an organization. Vulnerabilities can lie throughout every layer of the enterprise attack surface, at a depth that only security intelligence fortified with internet intelligence can illuminate. With this view,teams can stay ahead of early-stage vulnerabilities and prioritize and speed up remediation.

18,000+ vulnerabilities were published in 2020

300,000+ servers were affected by the Microsoft Exchange vulnerability

18,000 government and private users downloaded compromised SolarWinds Orion versions

RISKIQ®

Don't let your king get captured.
Read the white paper to master these moves.

DOWNLOAD TODAY