STRIDER

UNCOVERING INVISIBLE RISK

Responding to State-Sponsored Email Solicitation with Data Intelligence

STRIDERINTEL.COM ■

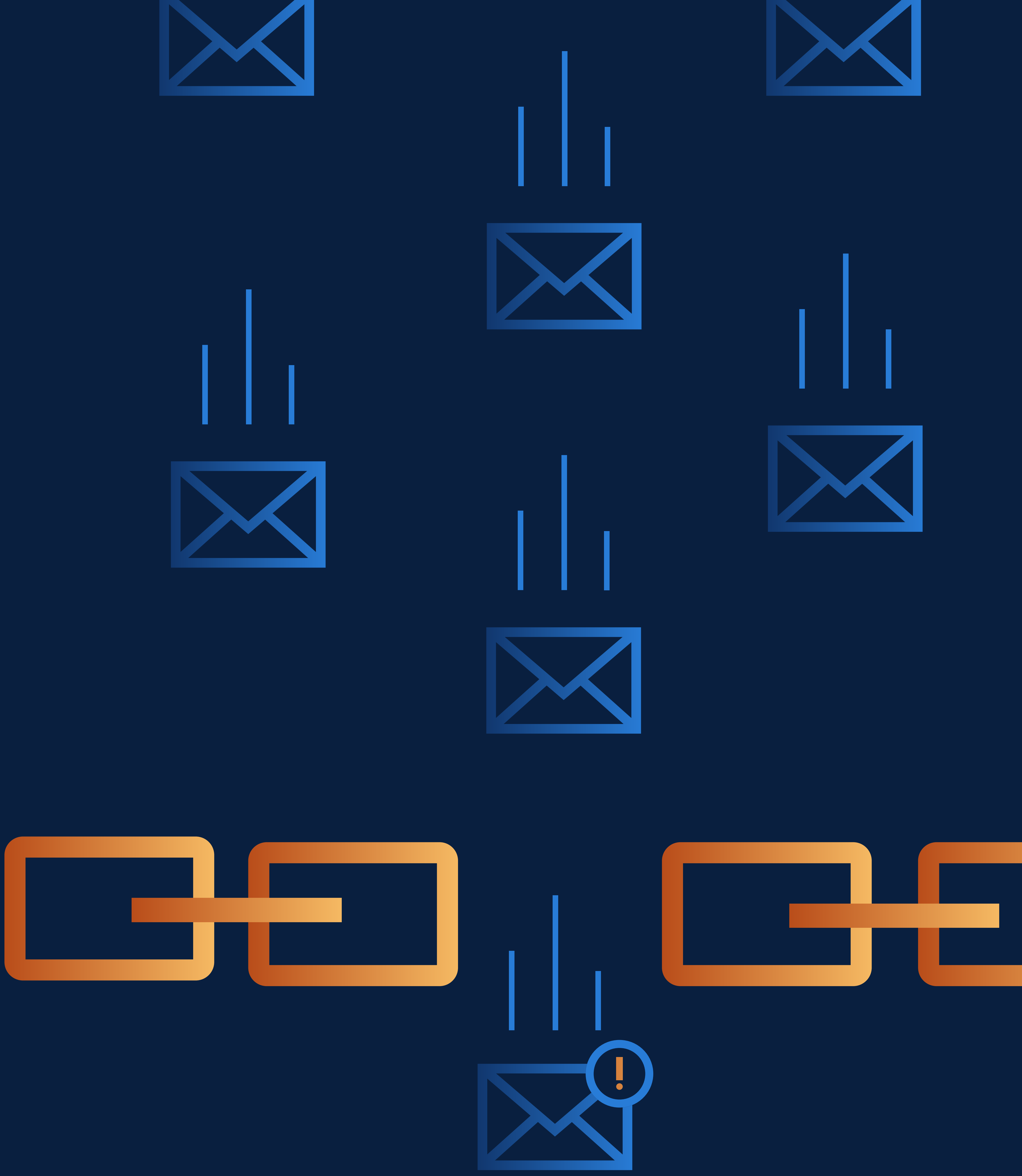
TABLE OF CONTENTS

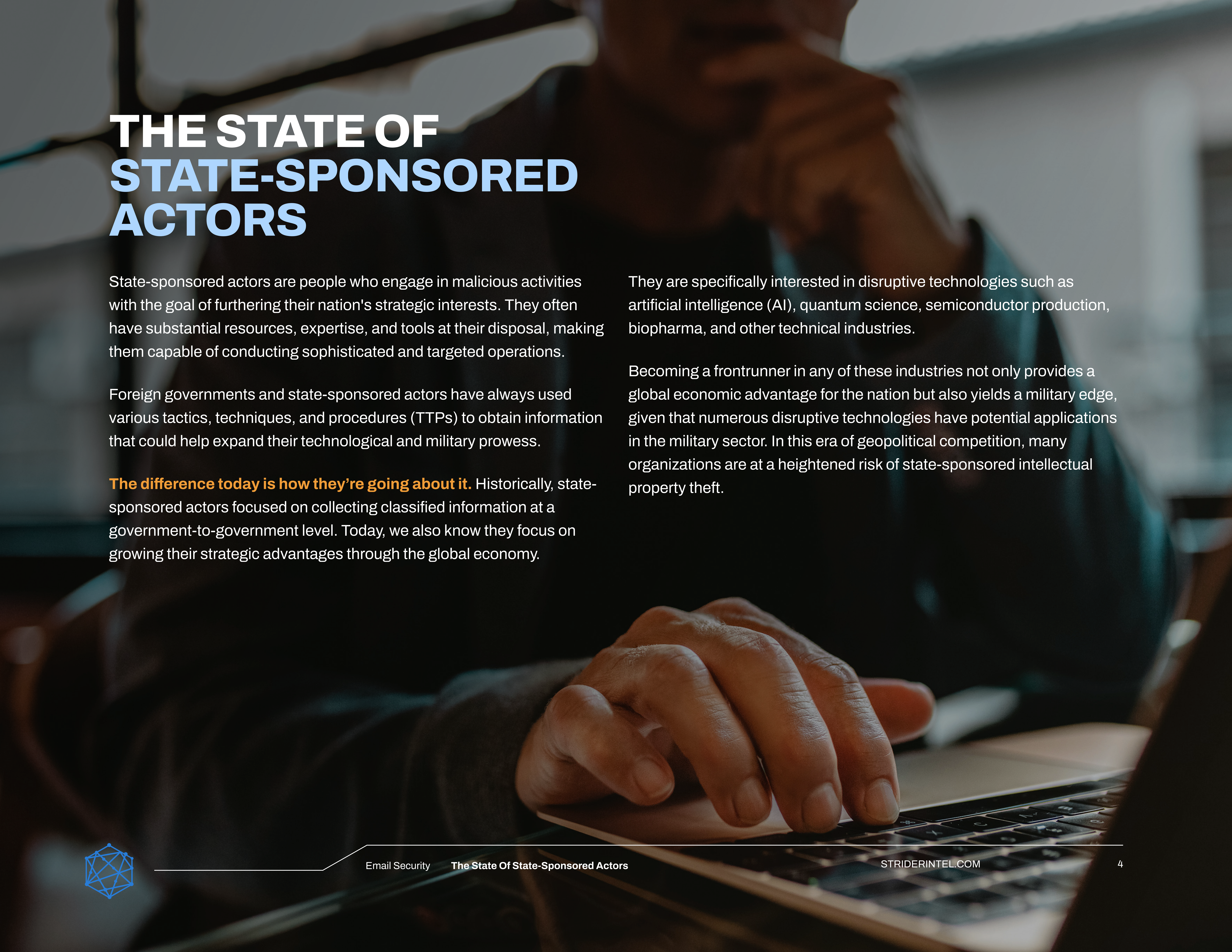
BAD ACTORS OUTSMART CURRENT EMAIL SECURITY

Robust email security is essential for protecting sensitive information in today's digital landscape. Standard email security tools focus on safeguarding email communications and systems from various cyber threats and vulnerabilities, such as spam and phishing protection, malware detection, and the implementation of encryption measures.

As important as these security measures are, many traditional email security tools struggle to detect solicitation attempts from bad actors. There are many types of bad actors with varying motivations. Bad actors working alone or with larger organizations typically seek financial gain or to cause disruption to the targeted individual or organization.

In the last few years, there has been an upward trend in bad actors representing nation-states. These state-sponsored actors work for the interest of the country they represent. If your organization operates with cutting-edge technology across any industry, it's highly probable that you are a target for state-sponsored actors.





THE STATE OF STATE-SPONSORED ACTORS

State-sponsored actors are people who engage in malicious activities with the goal of furthering their nation's strategic interests. They often have substantial resources, expertise, and tools at their disposal, making them capable of conducting sophisticated and targeted operations.

Foreign governments and state-sponsored actors have always used various tactics, techniques, and procedures (TTPs) to obtain information that could help expand their technological and military prowess.

The difference today is how they're going about it. Historically, state-sponsored actors focused on collecting classified information at a government-to-government level. Today, we also know they focus on growing their strategic advantages through the global economy.

They are specifically interested in disruptive technologies such as artificial intelligence (AI), quantum science, semiconductor production, biopharma, and other technical industries.

Becoming a frontrunner in any of these industries not only provides a global economic advantage for the nation but also yields a military edge, given that numerous disruptive technologies have potential applications in the military sector. In this era of geopolitical competition, many organizations are at a heightened risk of state-sponsored intellectual property theft.

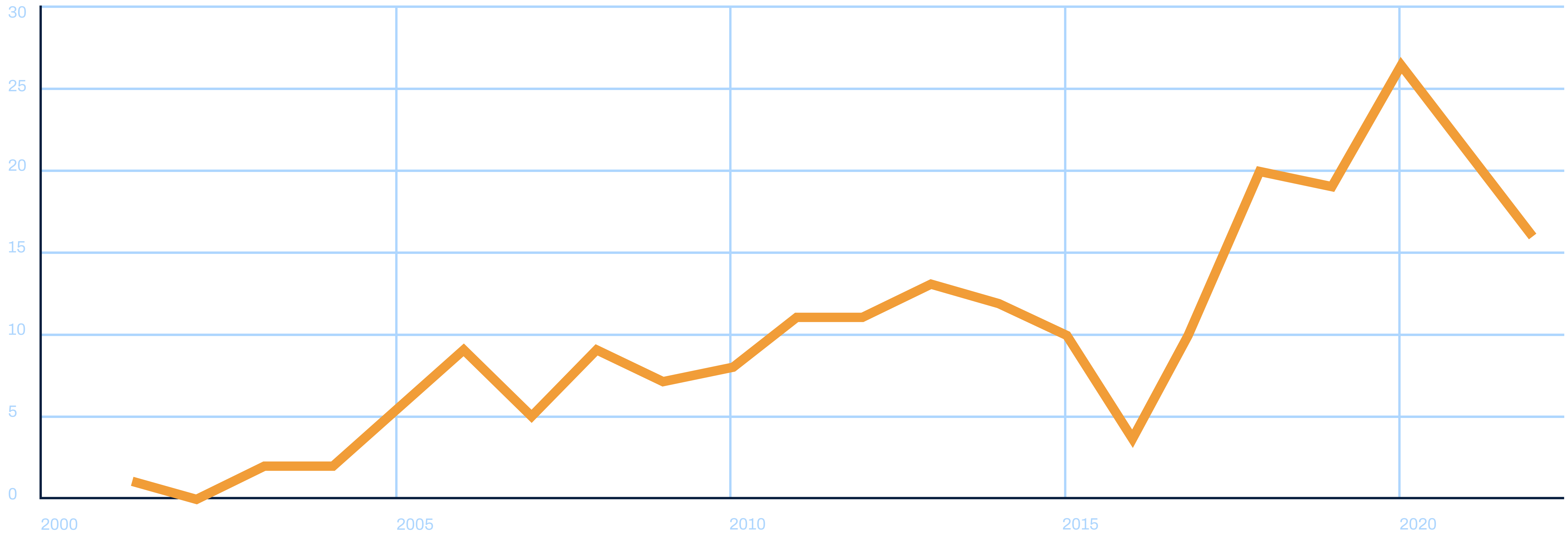
Beyond one-off phishing attempts, state-sponsored actors seek to establish professional relationships that are seemingly benign. Over time they build trust with your employees that ultimately can result in damage to your organization by recruiting them away or using them to access your valuable IP.

Because this solicitation comes from people appearing to be professionals and recruiters, detecting these attempts can be extremely challenging.

now

Especially in the current environment, taking proactive measures to protect your employees and organization from these actors is crucial.

TOTAL ESPIONAGE CASES



The chart above shows the numbers of publicly reported Chinese espionage incidents over time. Perhaps the most interesting part of this chart is the sharp dip after the 2015 agreement between President Obama and President Xi to restrict commercial espionage by government entities. The decline was quickly reversed within a year of the agreement.[1]

SEE THE UNSEEN WITH DATA

While there's no magic wand that reveals someone's true intentions, relevant and robust data can be the next best thing in conveying underlying motives. **The right data can provide situational context that can be instrumental in detecting and identifying malicious actors.**

At Strider, we do just that. We gather publicly available data from global sources in multiple languages. Using AI and patented processing methodology, we transform that data into strategic intelligence for organizations to better secure and advance their innovation.

One of the datasets Strider collects is an ever-growing list of identifiers for known state-sponsored actors.

We channel that data into our premier email security tool, Shield.

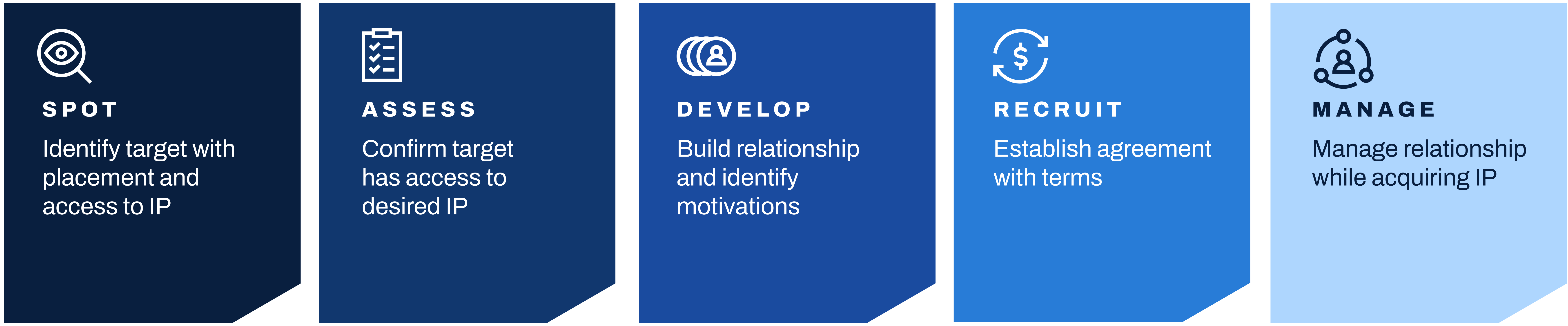
Shield provides verified email addresses, domain names, and key words directly linked to state-sponsored actors. Designed to cut through the noise and identify true positives, it can effectively identify state-sponsored solicitation with direct integration into existing cybersecurity tools.

In the following pages, we'll cover how state-sponsored actors work, what your organization's security team should look out for, and how Shield can play an integral role in your overall security posture.

UNDERSTANDING THE STATE-SPONSORED APPROACH

The approach of state-sponsored actors is deliberately subtle. Without specific identifiers like email addresses, domain names, or commonly used keywords, it can be nearly impossible to detect their true motives. **If you're aware of their recruitment cycle, you'll be better equipped to spot potential risk in your organization.**

RECRUITMENT CYCLE



SPOT

Identify target with placement and access to IP

ASSESS

Confirm target has access to desired IP

DEVELOP

Build relationship and identify motivations

RECRUIT

Establish agreement with terms

MANAGE

Manage relationship while acquiring IP

RECRUITMENT CYCLE

SPOT

In this first phase, a nation-state government agency or state-sponsored entity identifies an individual who may have access to or knowledge concerning the IP of interest. The name and background of the individual is then passed to an actor who can approach them, which begins the assess phase.

ASSESS

In this phase, the actor tasked with approaching the targeted individual seeks to establish a relationship with them. The objective is to confirm that this individual indeed has the desired access and knowledge. This is often achieved by meeting with the individual through professional associations or similar settings.

DEVELOP

Once the individual's access and knowledge are confirmed, the development phase begins. The state-sponsored actor will get to know the individual through various means. This could include inviting them to be a guest lecturer, attend prestigious conferences, or another matter of developing a professional relationship.

RECRUIT

In this phase, the targeted individual will be incentivized to join a talent program or receive funding to further their research. Often, the condition for accepting such invitations includes the obligation to share the results with the sponsoring talent program or funding organization.

MANAGE

Once the individual joins, they will be moved to the management phase. In this phase, the individual will be obligated to share their expertise in the IP they have access to with counterparts from foreign governments, either through concurrent employment or sponsorship.

ANALYZING THE RECRUITMENT CYCLE

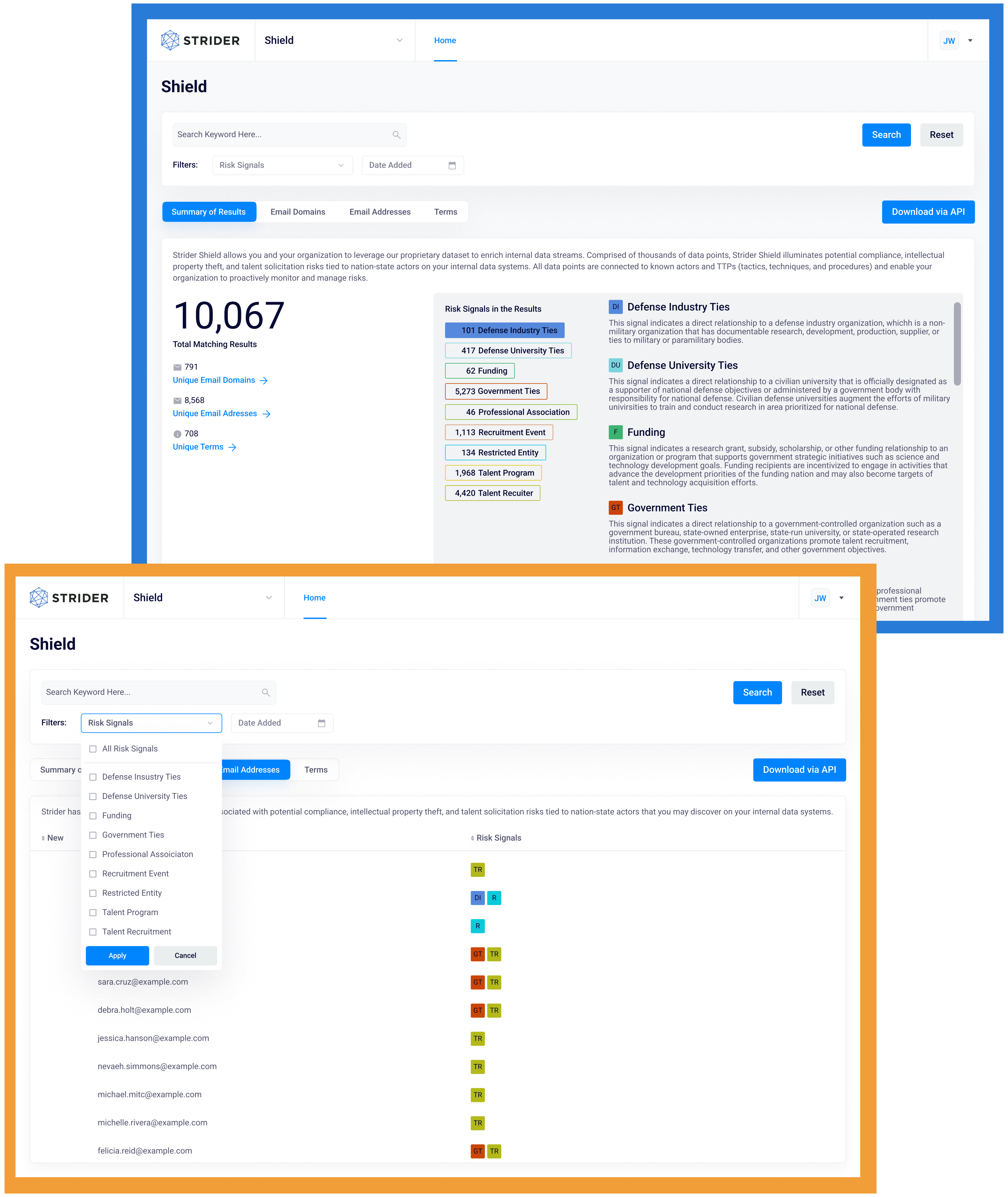
With an understanding of how state-sponsored actors conduct recruitment, Shield can offer valuable additional insights into the specific phase of the recruitment cycle that individuals in your organization may be in.

For instance, if one of your employees has been approached with an invitation to attend a recruitment event, it may be an indicator that state-sponsored actors are trying to assess the employee's expertise or ability to access desired IP. If an employee has been approached with a concurrent employment job, it may be an indicator that the employee already has developed a relationship with state-sponsored actors.

now

1

By identifying who is approaching the employees and the context of the approach, security professionals can take better steps to mitigate the risk.



Strider Shield allows you and your organization to leverage our proprietary dataset to enrich internal data streams. Comprised of thousands of data points, Strider Shield illuminates potential compliance, intellectual property theft, and talent solicitation risks tied to nation-state actors on your internal data systems. All data points are connected to known actors and TTPs (tactics, techniques, and procedures) and enable your organization to proactively monitor and manage risks.

10,067
Total Matching Results

791
Unique Email Domains →

8,568
Unique Email Adresses →

708
Unique Terms →

Risk Signals in the Results

- 101 Defense Industry Ties
- 417 Defense University Ties
- 62 Funding
- 5,273 Government Ties
- 46 Professional Association
- 1,113 Recruitment Event
- 134 Restricted Entity
- 1,968 Talent Program
- 4,420 Talent Recuiter

DI Defense Industry Ties

This signal indicates a direct relationship to a defense industry organization, whichh is a non-military organization that has documentable research, development, production, supplier, or ties to military or paramilitary bodies.

DU Defense University Ties

This signal indicates a direct relationship to a civilian university that is officially designated as a supporter of national defense objectives or administered by a government body with responsibility for national defense. Civilian defense universities augment the efforts of military univirsities to train and conduct research in area prioritized for national defense.

F Funding

This signal indicates a research grant, subsidy, scholarship, or other funding relationship to an organization or program that supports government strategic initiatives such as science and technology development goals. Funding recipients are incentivized to engage in activities that advance the development priorities of the funding nation and may also become targets of talent and technology acquisition efforts.

GT Government Ties

This signal indicates a direct relationship to a government-controlled organization such as a government bureau, state-owned enterprise, state-run university, or state-operated research institution. These government-controlled organizations promote talent recruitment, information exchange, technology transfer, and other government objectives.

Strider has sociated with potential compliance, intellectual property theft, and talent solicitation risks tied to nation-state actors that you may discover on your internal data systems.

New	Risk Signals
	TR
	DI R
	R
	GT TR
sara.cruz@example.com	GT TR
debra.holt@example.com	GT TR
jessica.hanson@example.com	TR
nevaeh.simmons@example.com	TR
michael.mitc@example.com	TR
michelle.rivera@example.com	TR
felicia.reid@example.com	GT TR

PROACTIVELY SECURE WITH SHIELD

Shield flags when a known state-sponsored actor communicates with an employee in your organization. **Shield integrates directly with your existing security tools via API.** Monthly updates with new email addresses, domain names, and key words ensure that you always have the most up-to-date information to help secure your organization.

When state-sponsored solicitation occurs, Shield provides context and connections—called risk signals—associated with the email address, domain name, or key term that caused the notification.

A state-sponsored actor may reach out as an industry professional, recruiter, government official, or even as an “old friend.” By reviewing the risk signal and context, the security team can verify what kind of relationship this person has with foreign governments. Examples include having ties to a foreign government, ties to a defense industry or university, ties to talent recruiter, and so on.

A SELECTION OF RELATIONSHIP TYPES SHIELD IDENTIFIES

now

State-sponsored actors have various types of relationships and connections linking them to nation-state governments. **The following are a few types of relationships that Shield flags:**

Restricted Entity

A direct relationship with a restricted entity. A restricted entity is an organization or person on a government-maintained list subject to technology transfer restrictions, export controls, financial sanctions, or other restrictions.

Funding

A research grant, subsidy, scholarship, or other funding relationship with organizations or programs that support government strategic initiatives. Funding recipients are incentivized to engage in activities that advance the development priorities of the funding nation and may also become targets of talent and technology acquisition efforts.

Talent Program

A direct relationship with a program designed to recruit and retain experts in support of national strategic development priorities. Talent programs may bestow awards, provide cash subsidies and other financial benefits, supply lucrative employment opportunities, or offer a combination of these incentives in recognition of an individual's commitment to provide their talents in service of government objectives.

SAMPLE INTEL FROM SHIELD

SENDER: @CUTIC.ORG ⚠

Domain name of CUTIC.

CUTIC is a non-profit professional organization based in Atlanta, Georgia. CUTIC functions as the official overseas liaison for multiple PRC government entities involved in talent recruitment and technology transfer, and is "entrusted by domestic cooperative city enterprises to recruit overseas high-level talents, senior managers, and short term technical consultations" on their behalf. CUTIC functions as a platform for technology transfer and talent recruitment from North America to the PRC. CUTIC conducts a wide range of activities that facilitate talent recruitment and technology transfer in support of development objectives of the PRC state. In its own words, CUTIC "[makes] full use of North America's outstanding technology talent resources and China's innovation and entrepreneurship needs."

SENDER: UCAHP.SV@GMAIL.COM ⚠

Email address of China Association of High-Level Professionals (UCAHP).

UCAHP supports PRC talent programs. The above email address has been used to contact several US companies that are involved in the development of advanced technology.

SENDER: @CITEF.ORG.CN ⚠

Domain name of the China International Talent Exchange Foundation.

The Foundation is a non-profit public institution directly under the Ministry of Science and Technology. It was formed by the integration of the former China International Talent Exchange Foundation and the former State Administration of Foreign Experts Affairs Training Center. It plays a central role in the management of international talent exchange funds, financing of talent introduction projects, recruitment of foreign experts, construction of international talent training bases.

now

Shield has over 20,000 data points just like these.

SENDER: @LIEPIN.COM ⚠

Domain name of Leipin.

Liepin is a large PRC talent service provider which offers job search, headhunting, onboarding, and other HR services to PRC enterprises, government, and research institutions. ("Liepin" literally translates to "headhunt and recruit.") The company claims to have brought together over 200,000 headhunters to serve more than 1 million customers in their HR needs.

SENDER: INFO@RU-SCITECH-FORUM.ORG ⚠

Email address of the RuSciTech Forum.

The RuSciTech Forum is an international conference coordinated by members of the RuSciTech Association, an organization for Russian-speaking science and technology professionals founded in Cambridge, England. Held on a biennial basis, the forum provides a platform for discussing the current state of science and technology in Russia; opportunities for boosting collaboration between Russian institutions and the Russian-speaking diaspora of scientists and technologists; and means of reversing Russia’s “brain drain.”

SENDER: RASAUSAPRESIDENT@GMAIL.COM ⚠

Email address of the Russian-American Science Association (RASA).

RASA is a US-based organization that holds annual conferences in cities across the US for leading Russian-speaking scientists to meet and discuss various topics, such as math, physics, and chemistry. The RASA Conference also presents a forum for discussions about how to improve collaboration between Russia and the Russian diaspora. RASA is an important element in the Russian government's initiatives to use the Russian-speaking scientists' knowledge to improve domestic expertise, and RASA coordinates closely with Russian state actors to accomplish its goals.

WORKFLOW

The following steps outline a method for integrating Shield into your current security protocol.

1. **Set up your API connection with Shield.**

2. **Develop log-only policies for ingested data.**

3. **Start to evaluate and identify patterns.**

   (Determine whether certain teams need more access than general organization based on their business needs, etc.)

4. **Move to deny based on your organization's policies and needs.**

CONCLUSION

The evolving landscape of cyber threats demands a paradigm shift in how organizations approach their security measures. The intricate and multifaceted strategies employed by state-sponsored actors underscore the need for a blended and holistic security approach. Siloed defenses are no longer sufficient in the face of such sophisticated threats. Organizations must be proactive, discerning, and data driven.

Strider's Shield provides unparalleled insights into the nuanced tactics of state-sponsored actors. By leveraging advanced analytics and machine learning, Shield offers a level of context and understanding that was previously inaccessible. In a world where data is the key to proactive security, Shield empowers your security team with the tools to discern subtle approaches and stay one step ahead of the adversaries.

now

1

Reach out to a Strider representative today to demo the product, get questions answered, and learn more →

STRIDER

STRIDERINTEL.COM ■