

The logo for CYCOGNITO, featuring the word in a bold, white, sans-serif font with a small orange square to the left of the 'C'.

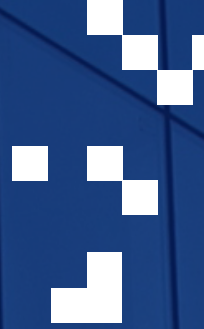
CYCOGNITO

The text 'SUMMER 2023 EDITION' in a white, sans-serif font, preceded by a small orange square.

■ SUMMER 2023 EDITION

Web Apps are Leaving PII Exposed

State of External Exposure Management Report



Welcome to the Summer 2023 edition of the CyCognito State of External Exposure Management report, offering data-driven insights and best practices to help organizations defend against the ever-evolving landscape of threats targeting external assets.

Our goal is to equip the broader cybersecurity community with the insights they need to stay ahead of these risks and safeguard their critical assets. From Fortune 500 to small enterprises, no organization is immune to risk, and most breaches are attributed to unknown or undermanaged assets. By analyzing this data, we found key external risk factors and provided practical recommendations for identifying and acting on vulnerabilities in the external attack surface that can be applied to organizations of all sizes.

Contents

Introduction	1
Key Results	2
Recommendations	3
Back to Basics	4
Web Apps in the External Attack Surface	6
Problems with Web Apps	8
Prioritization and Risk Reduction	11
Conclusion	13
Methodology	13
About CyCognito	14



Key Results

70%

of vulnerable web applications had severe security gaps, like lacking WAF protection or not using an encrypted connection, particularly HTTPS, while 25% of all web applications (web apps) lacked both.

12,000

The typical enterprise has over 12 thousand web apps and at least 30% of these web apps – over 3,000 assets – have at least one exploitable or high risk vulnerability.

74%

of assets with personally identifiable information (PII) are exposed to at least one known major exploit and one in 10 have at least one easily exploitable issue.

98%

of web apps are potentially GDPR non-compliant due to lack of opportunity for users to opt out of cookies.

1 : 133

For every easily exploitable critical severity issue affecting an organization, there are 133 easily exploitable high, medium, or low severity issues.

35% 2%

Adding additional context to issues resulted in **35% of issues being deprioritized as less critical** than their CVSS score implied. **Only 2% of issues were upgraded** based on additional context.

Recommendations

Survey often.

Infrequent surveying for external exposure combined with frequent fluctuation in the external attack surface's size adds up to serious gaps in awareness and coverage. To stay aware of risks as soon as they appear, use frequent mapping and scanning of all assets to maintain an up-to-date, comprehensive understanding of your external attack surface.

Mind your (web) apps.

Ensure web apps, particularly those that provide access to PII or e-commerce platforms, are protected with whatever tools are at your disposal, including web application firewalls (WAF) and encrypted connections.

Make sure web apps used by individuals in the EU offer the opportunity to opt out of non-essential cookies to avoid running afoul of GDPR.

Context is key.

Every security team is looking to find and prioritize the most important items on their to-do list, but it's equally important to know which items to de-prioritize. Use context about affected assets and threat actor activity related to issues to surface issues that identify issues that are less urgent to fix so you can focus on your top external risks.

Severity isn't everything.

Go beyond CVSS when prioritizing issues across your attack surface. By focusing just on severity, you may be missing other important attack vectors, like a lower-severity issue that an attacker can easily exploit.

Back to Basics

The external attack surface is everywhere an organization's assets touch the internet.

These external assets provide ways for companies to interface with employees and customers, but also serve as footholds for cybercriminals looking to gain access or exfiltrate valuable data. For most modern companies, this external attack surface landscape is sprawling and their assets are distributed across dozens or hundreds of business units that we refer to as "subsidiaries" (see "What's a Subsidiary" for more information).

Scattered across these many subsidiaries are tens or hundreds of thousands of assets like certificates, domains, web servers, web apps and API endpoints.


These assets also have subclasses such as high value assets, on-premises, or cloud-hosted, based on the types of information and access they provide or the way they are hosted. High value assets might provide access to PII, expose an API, or connect to critical business assets. While historically most if not all assets were hosted on-premises or in a private datacenter, modern organizations may now have many or most of their assets in the public cloud.

Security teams are responsible for knowing all about these assets: what other assets they connect to, who owns them, and whether the assets have any vulnerabilities or misconfigurations that could make them attractive targets for attackers. Before they can tackle any of those questions, however, they need to have a complete and accurate understanding of all the assets in their attack surface, and that's easier said than done.

What's a Subsidiary?

Because a path of least resistance to an entity's assets can come from any outside entity it connects with, mapping the attack surface actually starts with mapping the organization itself and finding all the teams, business units, brands, or child organizations that make up the parent company. These entities are referred to as "subsidiaries." CyCognito discovers and classifies these subsidiaries as part of the asset discovery process using natural language processing (NLP) and machine learning (ML) to look across public web sites, financial reports, and more.

These subsidiaries can be remote branch offices, the result of mergers or acquisitions, or separate business units that operate independently and may manage their own cyber assets but still contribute to the company's larger attack surface. They may be remote or unattached, but subsidiaries carry risks that affect the entire organization. CyCognito's April 2023 External Risk Insights brief found that **subsidiaries on average own or manage 56% of the critical and high vulnerabilities that create a path of least resistance to customer assets that attackers can exploit.**



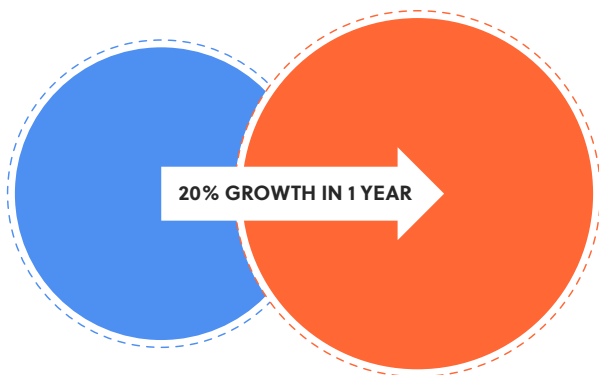
56% of critical and high vulnerabilities are owned or managed by subsidiaries.

While some of these subsidiaries will be well-managed and understood by the parent organization, many of their assets will be under-managed or even unmanaged. CyCognito's June 2022 report found that organizations are unaware of 10-30% of their subsidiaries, leaving substantial portions of the attack surface in the dark.

The Only Constant is Change

The attack surface is constantly changing. Previous research by CyCognito found that the size of the average attack surface fluctuates by nearly 10% a month. Over the last 12 months, we found that **the average attack surface fluctuation increased slightly, to just over 10% per month**. This is different from saying that every month the average attack surface gets 10% larger – if that were true, security professionals the world over would have no hope of keeping up with their runaway number of external assets! But this constant change presents its own challenges.

Even smaller fluctuations in the size of the attack surface can lead to sizable numbers of unknown assets. One major consumer goods organization examined in this report had their attack surface change by an average of only 3% every month. This may feel like a manageable amount of new assets to keep on top of, but after 12 months their attack surface had grown by 20%, adding thousands of new assets. Any of those new assets could have serious exploitable issues and, depending on when they were created, could have gone unnoticed for months.



The average attack surface fluctuation increased to just over 10% per month.

Because the attack surface is always in flux, it isn't enough to map it just once. Almost immediately, the map you make is out of date. Some security teams compromise by doing yearly or quarterly scans, but that cadence would have left this organization suddenly dealing with an attack surface 20% bigger than it was last year.

Spin Up, Spin Down

Where does this fluctuation come from? Every month, new assets may appear as teams spin up projects or add new programs, while old assets will be taken offline because they've served their purpose. Larger additions may come from the onboarding of a new team, brand, or subsidiary that brings their own roster of assets with them. On the other hand, the discovery of a new vulnerability that affects critical resources might necessitate taking a large number of affected assets offline temporarily or permanently.

While every asset in the external attack surface is important – because it can provide a foothold for attackers to access your network! – the bulk of this report will focus on some of the most complex and fascinating assets: web applications or web apps. Our discussion in the next section of a web app vulnerability that recently appeared in the news will explain why they're so important.

Web Apps in the External Attack Surface

Once the first challenge of continuously monitoring and mapping the assets in the external attack surface is tackled, it can be tempting to see the task as finished.

However, the larger project of exposure management has only just begun. Truly understanding your attack surface – and the risks it poses to your organization – requires understanding the misconfigurations and vulnerabilities that affect your assets and correctly prioritizing which of them most urgently need to be remediated. In this section, we'll discuss more about the issues we found commonly affecting a particular type of assets – web apps – and how they can put the larger attack surface at risk.

Web apps are the most complex and valuable part of the modern attack surface. In addition to being easy to deploy, they provide access to valuable data, connect businesses with employees and customers, and can have dozens of components that each can be potentially affected by security issues. The average attack surface we examined contained over **12 thousand web apps**. This represents **22% of the typical attack surface**.

12,000

WEB APPS
in the average
attack surface

CASE STUDY

MOVEit and Ransomware

MOVEit Transfer is a web app that many companies use to share sensitive information.

Data is encrypted and access-controlled. Specifically, organizations use it to share very large troves of very sensitive data securely. From an attacker's perspective, MOVEit Transfer is a very attractive target: it has high adoption rates among major companies and contains treasure troves of financial data, strategic goals, or intellectual property. This makes finding an exploit that allows decryption and exfiltration of this data a worthy investment for cybercriminals.

This was the case with a series of critical SQL injection vulnerabilities (CVE-2023-34362, CVE-2023-35708, CVE-2023-36932, CVE-2023-36933, and CVE-2023-36934) that

affects MOVEit Transfer and were disclosed in June 2023. This web app was vulnerable to attacks through HTTP and HTTPS, and, depending on the database engine used (for example, MySQL, Azure SQL, or Microsoft SQL) attackers could use these vulnerabilities to "infer information about the structure and contents of the database and execute SQL statements that alter or delete database elements." In practice, this could lead to attackers viewing, altering, or stealing the sensitive data related to MOVEit Transfer.

The initial exploit isn't the only danger that this series of vulnerabilities poses, however. Once this sensitive data is accessed or exfiltrated, attackers can then use ransomware tactics to force victims to pay to keep the information off the web. In the case of MOVEit, organizations using MOVEit Transfer became the targets of a Russian-speaking ransomware group, CL0P, that exploited these vulnerabilities to steal data and extort their victims.

Size Matters

The larger an organization is, the smaller a percentage of its attack surface is made up of web apps. This suggests that, rather than needing to be linearly increased as organizations grow, web apps can stretch to cover a larger workforce.

For example, one organization we examined had web apps make up only 5% of their active attack surface, but because their attack surface was quite sprawling – to keep up with the needs of their global business – that still amounted to over 87 thousand web applications to manage, over 11 times larger than the entire attack surface of another organization! In contrast, web applications made up over 43% of another attack surface, but that organization only contains 18 thousand web apps.

Web Apps Need TLC

We highlight this to communicate that every attack surface can contain different combinations of IPs, domains, certs, and web apps, but regardless of the assets in an organization's attack surface, web applications are the trickiest to manage.

It comes down to relative complexity. Every web app is built from a variety of layers, with a customer or employee front end that users interact with to input data or discover information and a back end with structural components that process and deliver the services of the web app. These structural components include the web app server and database server. The more complex a web app is, the more likely it is to have both additional layers and complexity within each layer.

These web apps are vulnerable both to misconfiguration and to newly discovered or exploited vulnerabilities, like zero-days. For example, if security is not included as part of the DevOps workflow, developers may push code to production that includes major security vulnerabilities.

Organizations need to be concerned not just for the initial damage from an unpatched and unknown vulnerability, but also the possible ways the vulnerability can be leveraged against them. Highly trusted software – think LastPass or SolarWinds – can sometimes be leveraged most effectively because organizations have deemed them trustworthy. In cases like these, it's vital to actively monitor and test even the most trusted assets.



Problems with Web Apps

Over the last year, about 30% of all web apps under monitoring had highly-exploitable OWASP top 10 issues at any given time.

30% of all web apps under monitoring had highly exploitable OWASP top 10 issues at any given time.

30%

However, this fluctuated significantly from month to month – in August 2022, almost half of web apps under monitoring had high or critical severity issues, while less than 20% of web apps fell into this category in May 2023. Below, we'll examine some trends we noticed with web apps under monitoring, as well as easy fixes that can make these assets a stronger part of the external attack surface.

Because CyCognito uses dynamic application security testing (DAST) to actively test customers' web applications, we can dive deeper into uncommon and complex issues that might affect these assets. Not only does this show us some interesting trends in basic protections or traits that web apps can have, we can also in some cases make some deeper extrapolations about the assets.

Down, Down, Down in a Web App Wall of Fire

For an example, let's look at web application firewalls, or WAFs. WAFs monitor and filter traffic to and from a web server, specifically preventing malicious HTTP/S traffic from reaching the web app's server while stopping unauthorized

70%

of web apps under monitoring were not protected by a WAF.

data from leaving. While WAFs don't mitigate all potential attacks, they are considered important building blocks in the protection of web apps.

Although WAFs are a fairly basic form of security for web apps, **we found that only 30% of web apps under monitoring were protected by a WAF.** E-commerce web apps and APIs were slightly more protected – only 40% of web apps that offer e-commerce and only half of APIs were protected by a WAF.

An unprotected e-commerce web app could leave customer's PII and payment card information vulnerable to exfiltration by attackers. Not only does the lack of a WAF open these assets to potentially malicious traffic, the lack of a WAF indicates that there may be other basic protections that are going unused when it comes to these assets.

■ CYCOGNITO STATE OF EXTERNAL EXPOSURE MANAGEMENT REPORT

Another basic form of web app protection is using HTTPS to encrypt and authenticate traffic between the website interface of the web app and the users' browsers, preventing malicious actors from tampering with communications in transit. While HTTPS was introduced over 20 years ago, it was initially adopted by web applications that handle financial transactions or PII.

Almost a third of web apps had homepages unprotected by HTTPS.

1/3

HTTPS is now a basic form of protection for all web applications and about 70% of websites are protected automatically.¹ We found that **almost a third of web apps had homepages unprotected by HTTPS**. Protection was stronger for the relatively small percentage of web apps that have API access, with almost 100% of those assets protected by HTTPS. Some organizations fail to protect web apps with HTTPS out of a faulty assumption that sites accessible only through intranet or a VPN are already protected, when in reality this still leaves the site vulnerable to issues from the intranet or VPN provider.

25% of all web apps lacked both a WAF and secure encryption like HTTPS.

25%

These types of missing protections become even more serious when they compound. **We found that 25% of all web apps lacked both a WAF and secure encryption like HTTPS, leaving those assets painfully exposed to attackers.** To make matters worse, assets lacking these types of basic protections may have other major security flaws, leaving the door open to even more issues down the road.

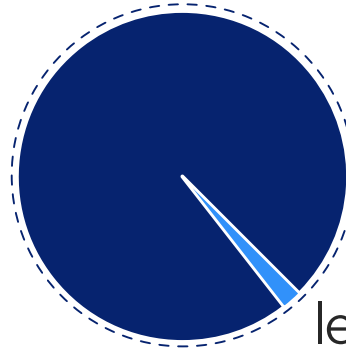
1. Troy Hunt, <https://doesmysiteneedhttps.com>

Heads and Apps in the Cloud

As spinning up and maintaining cloud assets gets easier and easier, more parts of the external attack surface can be found in the cloud instead of on-premises. While the flexibility and scalability of cloud assets can't be denied, keeping track of the cloud is key. While only **6% of assets under monitoring are hosted in the cloud, that swells to a quarter of all web apps**. Fully half of all cloud assets monitored by CyCognito are web apps.

Cookie Monsters

Depending on the site, visitors can be stuck with dozens or hundreds of cookies that can both personalize the user experience and collect behavioral data. We found that **less than two percent of web apps under monitoring offered users the opportunity to opt out of cookies**. This could indicate that the sites are failing to give users the opportunity to consent or opt out.



less than 2%
of web apps offered users the opportunity to opt out of cookies

The European Union requires websites targeting EU citizens to obtain cookie consent, including an opt-out option for non-essential cookies. Ensuring compliance is crucial for organizations using web apps that could possibly serve EU citizens. While it's possible that the site may not use non-essential cookies or does not serve EU citizens, it is likely that a large number of these assets are non-compliant with GDPR, creating a compliance headache for the organization responsible for them.

Web Apps Need a Hero

Depending on the types of web apps your team uses on a daily basis, you may be skeptical that web apps deserve this much time and attention – how much sensitive data do web apps contain, anyway? We measure this by looking to see if the web app pages contain input fields for PII like email address, name, address, or phone number (or even more sensitive information like SSN or national ID number!). We found that on average, **7% of all web apps under monitoring take PII inputs**. Across the average attack surface, this translates to approximately 53 web apps that could expose sensitive personal information.

As an example, take an insurance organization's healthcare claims portal. This portal not only has input fields for PII email address, username, and password, it also provides access to sensitive healthcare information like medical procedures, location of services, and cost of care and financial information like credit card details. CyCognito also found that this particular web portal was vulnerable to a cross-site scripting (XSS) attack that could deliver malicious javascript code to an unsuspecting user. Instead of viewing and paying a medical bill, users hand attackers sensitive PII or their credit card number.

Even relatively common forms of PII, like names or email addresses, can create headaches for users and organizations if they fall into the hands of cybercriminals.

11%

of web apps with PII are affected by easily exploitable issues.

The combination of the volume of stolen data from previous data breaches available online and the high rate of password reuse across accounts means that attackers can combine data from multiple breaches to gain access to new accounts.

To make matters worse, some assets with fields for sensitive information are also at risk, with 74% of assets with PII affected by at least one issue and one in 20 affected by issues in the OWASP top ten. These issues could create real problems for enterprises, with **11% of web apps with PII affected by easily exploitable issues**. These vulnerable high value assets create windows of opportunity for attackers looking to exfiltrate and sell data or leverage access.

It's clear that web apps are vital components of the modern attack surface but require careful monitoring and testing to ensure they don't put the organization as a whole at risk. In the next section, we'll look at how these issues can be prioritized.

Prioritization and Risk Reduction

Tens of thousands of CVEs are discovered every year – over 25,000 in 2022 alone – and it can be a full time job for security teams to sift through them.

As we discussed earlier, about 30% of web apps had highly exploitable issues. On top of that, **about 10% of all assets under monitoring are affected by security issues at any given time.** That leaves over 20,000 assets needing attention on an attack surface of average size. Prioritization is key.

Where to Start?

The first thing that most teams turn to is prioritizing by CVSS score. While this does begin to focus attention on the relatively small number of critical issues – less than 0.03% of all issues are of critical severity – it can create more problems than it solves. **Only 50% of critical issues are also exploitable by attackers,** but this vital information is not captured in the CVSS score and can leave security teams dealing with hundreds of issues that appear to be more urgent than they are.

CASE STUDY

Going Beyond CVEs

Of course, not all issues on the attack surface are caused by CVEs. A misconfiguration or neglected asset can pose just as much danger – and be just as attractive to attackers. One education organization with hundreds of global locations discovered that a Microsoft Exchange server had reached the end of its supported life.

While some IT teams can keep an on-premise Exchange server running for a bit longer than its lifetime of official support from Microsoft, vulnerabilities on these versions of Exchange can't be made safe from attackers through patching. In fact, the same month that this outdated Exchange server was discovered, Microsoft announced two new zero-day vulnerabilities that could have affected the asset.

Issues like these can also cause lost productivity – setting aside the downtime that would result from a successful attack on the server, out-of-date Exchange servers cannot communicate with modern Exchange Online servers, resulting in bounced emails and slowed communications with other teams and subsidiaries.

Once these outdated Exchange servers were discovered, the security team at the parent organization was able to reach out to the other locations and facilitate their move to a modern Exchange Online server allowing them to decommission the unsupported Exchange server. Not only was the organization now safe from breaches caused by this lingering asset, they experienced no delays in communicating with their branches.



■ CYCOGNITO STATE OF EXTERNAL EXPOSURE MANAGEMENT REPORT

Lower severity issues also deserve attention, but deciding how much attention they receive can be difficult. What about the 3% percent of issues that are high severity? Or the 26% of issues that are medium severity? And while it may be tempting to dismiss these lower severity issues as unimportant, a medium severity issue that affects a critical system, like payment processor or production server, could cause major headaches, and higher ups are unlikely to be happy with the explanation of “well, it wasn’t a critical issue.”

1 : **133**
CRITICAL : **HIGH, MED, LOW**
exploitable issue : **exploitable issues**

In general, the lower severity an issue, the more helpful the context on the issue’s exploitability. While **only 2% of high, medium, and low severity issues are easily exploitable**, they still pose a significant risk to the average organization because there are so many more of these types of issues. For every exploitable critical issue affecting an organization, there are **133 exploitable high, medium, or low severity issues**.

Incorporating additional context, like how attractive the affected asset is to attackers, whether threat actors are actively exploiting the vulnerability, and what other assets could be accessed through exploitation, can highlight issues that may have otherwise been neglected by just prioritizing by CVSS score.

35%

DOWNGRADED
with additional
context

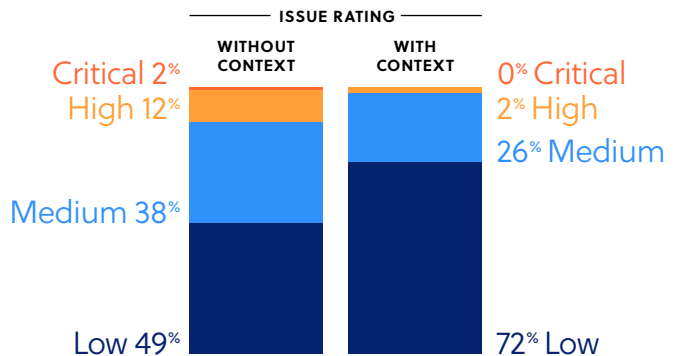
2%

UPGRADED
with additional
context

Prioritizing Goes Both Ways

While many security teams are focused on identifying what issues are most important, it is equally valuable to identify issues that are less important. After applying additional context about the affected issue and assets (see section below), **CyCognito downgraded the severity category of 35% of issues and upgraded the severity category of only 2% of issues**. This represents hours saved for potentially overworked security teams with limited resources.

Adding Context Helps Shift Priority on Risks That Matter Most



As the chart above shows, applying context shifts the distribution of issue ratings, resulting in fewer medium, high and critical vulnerabilities and more low severity vulnerabilities.

One global hospitality company’s security team had 48 issues downgraded from a Critical Severity to High, while only one issue was promoted from High to Critical. Not only was a lower priority issue elevated to ensure it was worked on more quickly, moving those 48 issues down the list helped focus energy where it was most needed.

"Contact Us" Page Gone Wrong

CASE STUDY

This organization has franchise locations all over the global, and these sub-organizations have a significant amount of autonomy. However, threats to any of these franchises can create issues to the parent organization, especially if attackers are able to use them to jump to other subsidiaries' assets.

One franchise uses WordPress to build online resources for their customers and included a "Contact Us" page as part of the WordPress site. Unfortunately, the Contact Form 7 plugin for that version of WordPress contained a vulnerability, CVE-2020-35489, that allowed unrestricted file upload and remote code execution. Attackers could exploit one security flaw to make changes to forms that used this

plugin as if they were site administrators. While changing the format of a form may not seem like much more than an annoyance, by changing the form attackers could force the website to receive uploaded executable files of malware.

This vulnerability affected about 2% of all web apps in this organization's attack surface. However, the assets owned by franchises were harder to monitor and remediate without a holistic view of the entire attack surface, creating more risk for the parent organization. Once the parent company's security team was alerted that franchise assets were vulnerable, they were able to reach out and work with their counterparts across the franchises to ensure the issue was resolved without incident.

Conclusion

Managing the ceaseless fluctuation of the modern external attack surface remains a challenge for organizations but is only half the battle.

In this report, we've identified traits that can indicate your web apps need additional attention, as well as the benefits of going beyond CVSS when it comes to prioritizing your teams' work. Organizations must go beyond simply indexing their assets and engage in true exposure management practices by identifying, testing, and prioritizing the remediation of high value assets.

Methodology

For this report, CyCognito's research team aggregated and analyzed 3.5 million assets across its customer base between June 2022 and May 2023.

All findings are anonymized and normalized. These customers span multiple industry verticals and include a mix of small, medium, and large enterprises across the globe, including Fortune 500 companies. Information about specific security vulnerabilities came from publicly available disclosure and reporting related to those vulnerabilities, and references to security scores are based on the common vulnerability scoring system (CVSS) scores derived from the National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD).²

2. National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD) <https://nvd.nist.gov/vuln>

About CyCognito

CyCognito is an external attack surface management platform designed to empower operations and security teams to identify, prioritize, and help remediate externally exposed IT risk. We were founded in 2017 by ex-intelligence agency reconnaissance experts that asked a simple question: “what if we could simulate an attacker’s reconnaissance plan starting only with the target company’s name?” Since then, we’ve helped organizations map their attack surfaces and prioritize and accelerate their remediation efforts.

Want to see how it works?

Check out our website and explore our platform with a [self-guided, interactive dashboard product tour](#). If you’d like to chat to an expert about external risks that might affect your organization, you can schedule a demo at <https://www.cycognito.com/demo>.

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit [cycognito.com](https://www.cycognito.com).

