THE STATE OF DIGITAL EXPOSURE TO CYBERCRIME OF EUROPEAN RETAIL

Ethiack

Index

Executive Summary

This report presents the results of an analysis of the digital exposure of 1,722 domains belonging to European Retail companies, representing over 57,898 exposed digital assets. The analysis provides CISOs, CTOs, and CFOs in European Retail with a data-driven perspective on the attack surface exposed to cybercrime and how their organizations compare to industry peers.

For this analysis, an internal tool of Ethiack was used, which performs a passive, non-intrusive reconnaissance of an organization's attack surface. This refers to the digital infrastructure exposed to the outside world that can be targeted in a cyberattack.

Our analysis revealed three major security gaps in the European retail sector:

- 16% of HTTPS connections use invalid or outdated SSL certificates, creating opportunities for man-in-the-middle attacks and data interception. These are fundamental security hygiene failures that persist due to incomplete attack surface visibility.
- 17% of web servers expose sensitive version and software information, providing cybercriminals with reconnaissance data to quickly identify and exploit known CVEs without additional effort.
- 1,208 critical assets, including email servers, admin dashboards, VPNs, and checkout flows, show concerning weaknesses, with webmail systems exhibiting the worst posture: 34% exposed configurations and 10% with SSL bad practices.

These findings carry three significant implications for European retail leadership:

- Visibility gaps create undefendable attack surfaces. If security teams don't know what assets exist, they cannot protect them. This mirrors industry research showing 37% of enterprise attack surfaces are unknown—a foundational weakness that makes all other security investments less effective.
- Traditional security approaches cannot match threat velocity. With Time-to-Exploit now averaging -1 days (meaning zero-days are exploited before patches exist) and CVE disclosures up 16% in 2025, annual or quarterly penetration tests are fundamentally inadequate. The attack surface changes faster than periodic assessments can capture.
- Critical business assets face disproportionate risk. The assets most vital to operations, such as payment systems, customer databases, and administrative access, show security weaknesses that could result in business disruption, regulatory penalties, and reputational damage. Recent breaches at Marks & Spencer (£300M loss) and Harrods (500K customer records exposed) demonstrate the financial and brand impact.

Luckily, the solutions to these problems are already available out there and ready to be implemented:

- First, organizations need extensive Attack Surface Management (ASM) to maintain real-time visibility of all exposed digital assets, including third-party and supply chain connections, eliminating blind spots that attackers exploit.
- Second, by using autonomous, AI-powered penetration testing with event-driven triggers for code changes, infrastructure updates, and new threat intelligence, vulnerabilities are discovered and validated at the speed of modern development cycles.
- Third, with automated detection and correction of basic security hygiene issues, organizations can resolve low-hanging fruit that significantly reduces attack surface risk with minimal investment.

The results of this study suggest that there is an increased risk of exposure to cyberattacks across European retail, and it is prudent to consider implementing preventive measures and incentivising collaboration with security researchers. Organizations that embrace continuous, autonomous security testing will discover, prioritize and remediate vulnerabilities before they become breaches. Those that rely on periodic assessments will continue to appear in breach headlines.

Methodology

To conduct this analysis, we've used our proprietary recon tool. This tool allows for a passive, non-intrusive reconnaissance of an organization's exposed digital infrastructure, using only its main web domain.

The tool can identify:

- The total number of exposed digital assets (subdomains, applications, IPs, and others);
- Types of web servers, services, technologies, and integrations;
- Server information exposure and configuration of secure digital certificates.

We've also analyzed data from our hacking agent, Hackian, to give you more context on vulnerability trends regarding Retail companies.

In addition to quantitative attack surface analysis, this report incorporates insights from in-depth interviews with cybersecurity leaders at European retail organizations. These conversations provide context on the real-world challenges of defending retail infrastructure, current threat patterns, and the gap between industry best practices and common practices.

We spoke with Ali Aziz, CISO at Nemlig.com, Denmark's leading online grocery retailer operating a 100% digital business model, and Gabriel Moliné, CISO at Carrefour Spain, one of Europe's largest traditional retailers. Together, these perspectives represent both ends of the retail spectrum—from pure-play digital to complex multi-channel operations—and inform the practical recommendations throughout this report.

Notes and Important Limitations:

The tool used performs a preliminary reconnaissance of the attack surfaces in question. This means that the tool only accesses information available in various public databases and via legitimate access to various web domains, without resorting to any active testing. In other words, the tool is non-intrusive. Furthermore, this analysis only reveals digital assets exposed on the web, which does not include all digital assets of an organization. Missing are, among others, mobile applications and internal networks and assets.

Thus, the results presented here are limited and may differ from the actual situation, as they result from an analysis restricted to a very limited period. Generally, attack surfaces are larger and present more vulnerabilities. Therefore, the scenarios presented can be considered as "best-case scenarios". A more in-depth and realistic analysis could be carried out with the proper legal authorization from the responsible parties of the web domains under study.

Finally, all listed domains were obtained through public databases and via legitimate access to various web domains.

Introduction

This report was created using public-facing data sources, opinions collected from industry experts, and data from the external attack surface of 1,700 European Retail companies. Our goal is to provide CISOs and security practitioners with information on the state of the industry, so they can understand risks and compare their own efforts with what's being done in the industry as a whole.

Cybersecurity Landscape in Retail

Recent years have seen more attacks on some of the biggest Retail companies in Europe. The year started with attacks on Marks & Spencer and Co-op, which led to losses of £300 and £206 million, respectively. Harrods was also a high-profile target, being compromised twice in the same year and leading to a leak of data for nearly half a million customers. Retail companies contain lots of valuable customer data, liable to be extorted in ransomware attacks, and often use old technology, as we'll see later in this report.

This follows the overall trend for European businesses. One in eight faces cyberattacks annually, with enterprises facing the biggest risks, and often without knowing where. Reports by HackerOne reveal that 37% of enterprise-level attack surfaces are unknown, which is a weak point to start with. If you don't know where an attack can come from, it's impossible to defend yourself.

This assessment is corroborated by security practitioners on the front lines. Ali Aziz, CISO at Nemlig.com, characterizes the retail sector's overall preparedness as "*horrible*," citing fundamental gaps in leadership understanding: "*Many CISOs are elevated legal counsels or managers, not technical security experts. Boards don't understand the cyber threat landscape or financial implications.*"

The consequences of this preparation gap are visible in recent incidents. The Marks & Spencer ransomware attack resulted in a five-week operational outage—an outcome that Aziz attributes to inadequate ransomware preparedness and recovery planning. "*If you're 100% digital retail like we are, a cyberattack is a single point of failure for your entire business,*" he notes, highlighting the existential stakes for modern retailers.

> "If you're 100% digital retail like we are, a cyberattack is a single point of failure for your entire business."
>
> Ali Aziz, CISO at Nemlig.com

To add to this, there's the risk from connections with third parties, which only increases the risk of cyberattacks. Recent examples include the attack on the Eastern European operator of IKEA store in April, which lost USD 23 million after a ransomware attack, or Adidas' data breach which was also linked to a third-party customer service provider. Ever-increasing attack surfaces, combined with the attack vectors offered from unsecured and untested third parties, paint a dire picture for European retail.

Gabriel Moliné, CISO at Carrefour Spain, focuses on customer loyalty programs as a top-three risk category: "*Loyalty ecosystems are high-value targets due to the volume of customer data and third-party integrations. These partnerships often create technology and data flows outside traditional IT governance, increasing exposure.*"

Supply chain attacks have evolved beyond traditional software compromise. According to Nemlig.com's CISO, social engineering targeting suppliers has become the primary attack vector: "*Attackers breach a supplier or vendor first, then impersonate them to target our customer service or finance teams. We see this consistently. They're not infecting software but instead compromising third-party relationships for social engineering.*"

Additionally, there's an increase in the number and impact of CVEs being disclosed. While this increase is in part due to more researchers sharing their findings, it's also a consequence of the presence of software in all aspects of our lives, combined with the increase in the speed of writing and deploying software caused by coding agents. The number of CVEs published in 2025 increased 16%, and as if this wasn't concerning enough, sources like Mandiant have revealed that Time-to-Exploit, which tracks the average number of days between a patch release and active exploitation, has dropped to -1 days for the first time. In other words, zero-day vulnerabilities are now being actively exploited in the wild before a patch is even available.

It's in this critical context that we write this report. Our goal is that this report helps you understand how Retail companies are doing and what threats they face, so you can analyze your current practices and adapt accordingly.

Analysis of Digital Exposure

In this section, two preliminary and superficial analyses of the exposed digital infrastructure associated directly or indirectly with these companies are presented, to obtain an initial assessment of the potential risk of exposure to cybercrime.

Through these analyses, it is possible to quantitatively and qualitatively evaluate the attack surface of various organizations, that is, the digitally exposed assets that are susceptible to cyberattacks. This provides a general idea about the security posture of the digital infrastructure.

Type of Organizations Analyzed

Firstly, to paint a picture of the kind of companies we're analyzing, it's important to mention what companies compose the sample.

As mentioned, 1,722 companies were analyzed. 23% of these companies have over 5,000 employees, and about 48% have between 201 and 1000 employees. We only analyzed Retail companies in the European Union and the United Kingdom, with a minimum of 200 employees. If your organization falls within these brackets, the vulnerabilities we've identified are statistically likely to exist in your infrastructure.

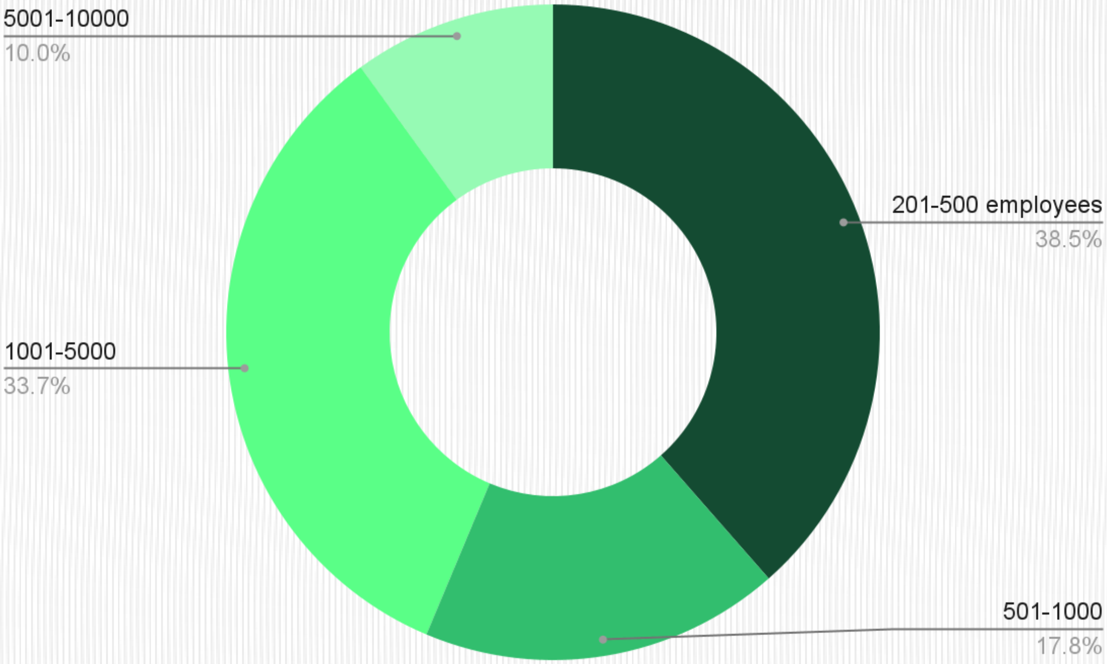

Image 1 - Distribution of companies by number of employees

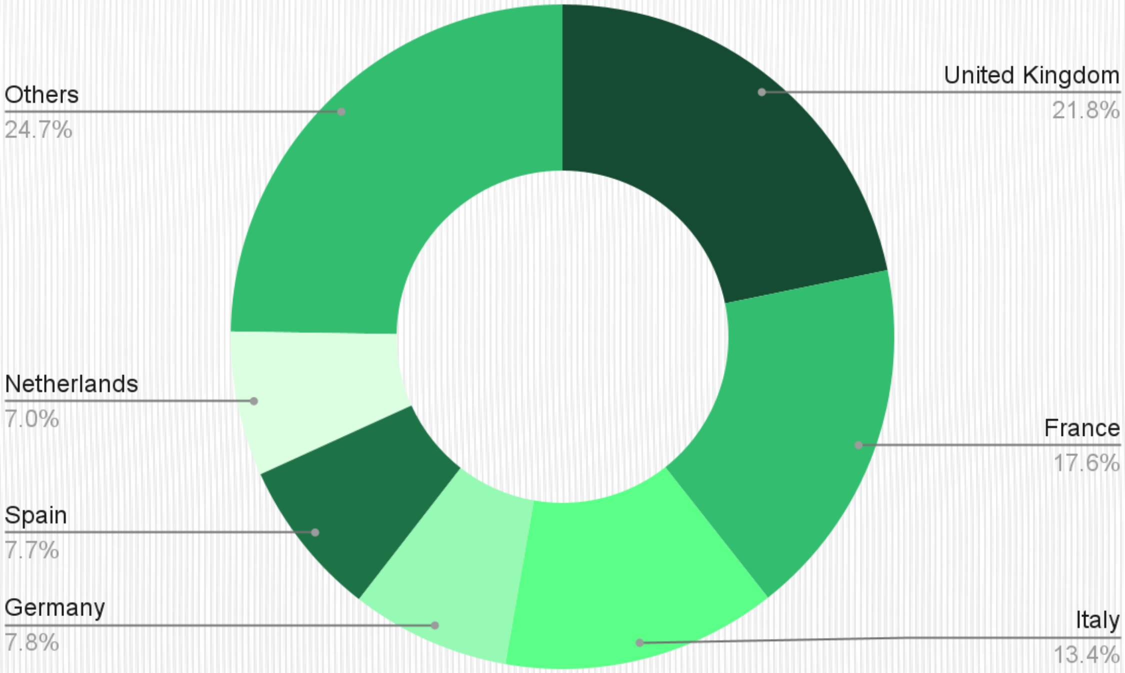

Image 2 - Distribution of companies by country

Regarding revenue, most companies fall in the 100M to 1B bracket (51% of sample), with a third of the sample grossing over USD 1 billion per year. The United Kingdom, Germany, and France are the most represented countries, respectively.

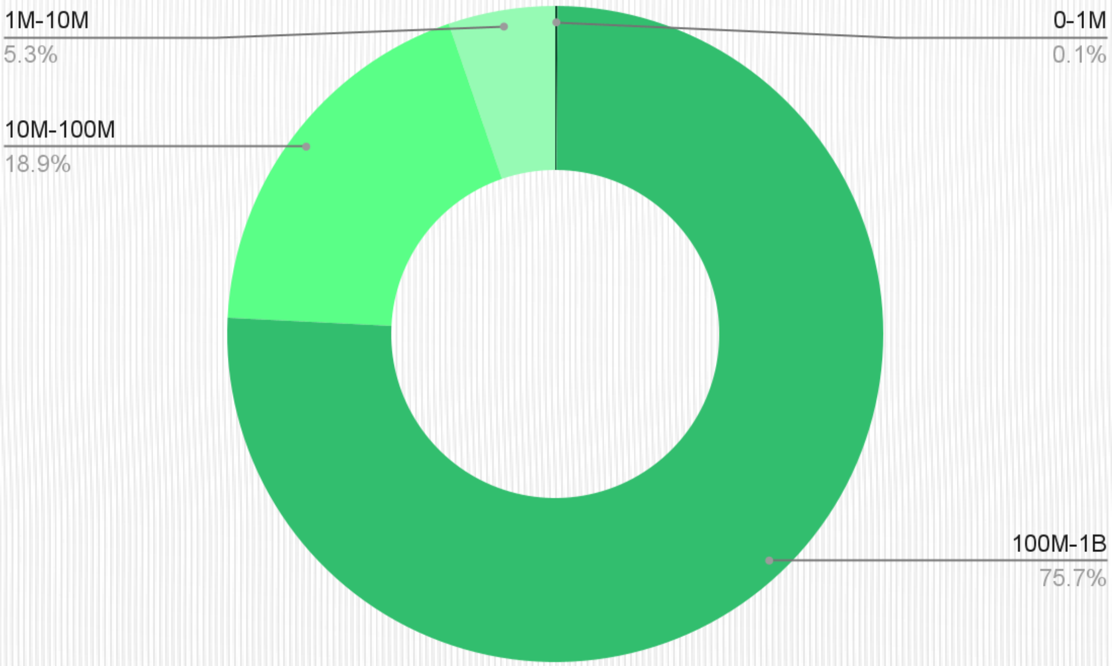

Image 3 - Distribution of companies by yearly revenue

The diversity of our sample reflects an important reality: "retail" is no longer a monolithic category. Modern retail organizations operate far beyond traditional stores and e-commerce. Carrefour Spain, for example, encompasses 11 separate companies, including financial services, telecommunications, travel agencies, and infrastructure rental operations, each with distinct technology stacks, regulatory requirements, and attack surfaces.

"*We're not just managing retail systems,*" explains Gabriel Moliné, CISO at Carrefour Spain. "*We have payment systems, customer loyalty programs integrated with external partners like airlines and ride-sharing services, warehouse operations, telecommunications infrastructure, and financial services—all creating interconnected exposure.*"

This complexity explains why even mid-sized retailers in our sample average 33 exposed assets. Each business function, partnership, and customer touchpoint adds to the attack surface. For security teams, this means defending not a single perimeter, but multiple overlapping ecosystems with varying security maturity levels.

Size of the Exposed Digital Infrastructure

Initially, we analyzed the digital assets of these organizations, providing an insight into the size of their digital infrastructure. For this report, any exposed domain or subdomain is considered an asset. We analyzed all assets under the main domain of each organization.

A total of 1,722 main web domains were analysed, resulting in the identification of 57,898 exposed assets. We found that each domain has, on average, 33 exposed assets.

Breaking this down, we notice that most companies have between 10 and 100 assets (56% of the sample), with only 6% exceeding this range. It's also interesting to note that companies with 10,000 or more employees heavily skew the sample, as they average 71 assets, while the average across the entire data set is, as mentioned, just 33 assets. It's also clearly noticeable that as the employee count increases, so does the number of assets. This trend is also visible when breaking down the data set by revenue bracket.

From this analysis, it's easy to conclude that even mid-sized retailers have a substantial attack surface that cannot be effectively secured through manual processes alone, as each asset requires manual, repetitive security work.

This problem only gets trickier the bigger the organization. Enterprises with 10,000+ employees average 71 assets, which means exponentially more complex security challenges. Larger attack surfaces have more interconnections, more third-party integrations, and more potential lateral movement paths for attackers.

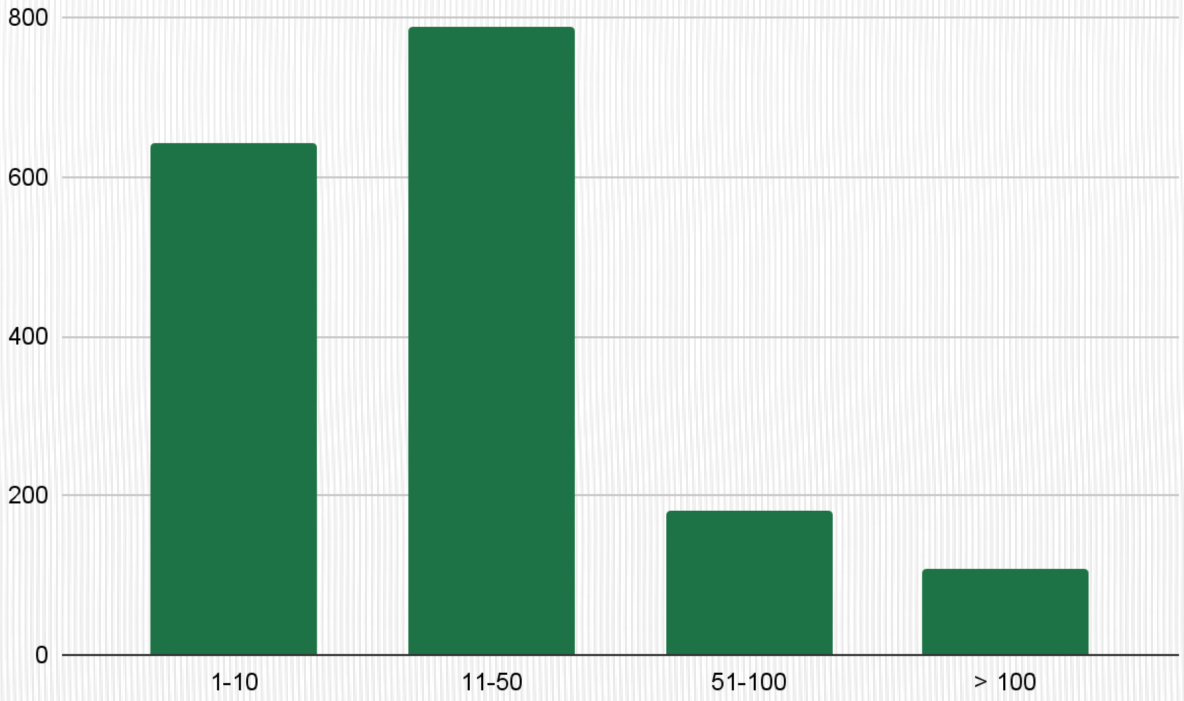

Image 4 - Distribution of companies by number of assets on their main domain

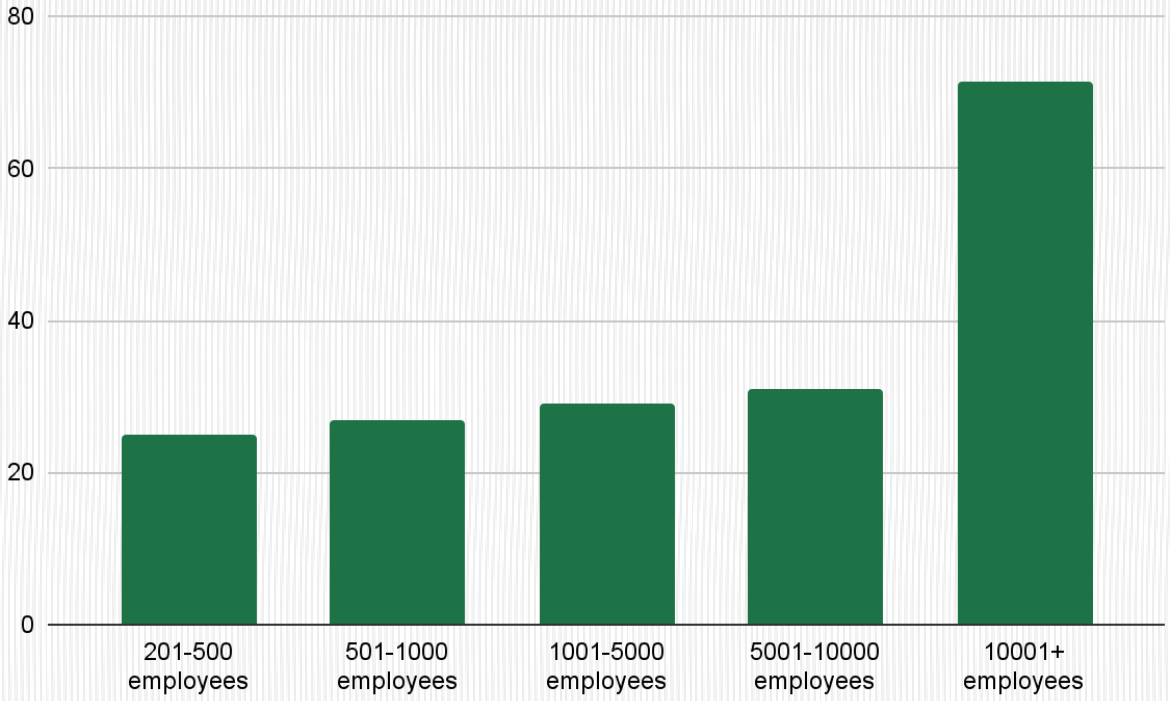

Image 5 - Average number of assets by number of employees

Typology of the Exposed Digital Infrastructure

A qualitative analysis of the exposed digital assets was also conducted to evaluate the attack surface from the perspective of services, servers, technologies, integrations, and even the most commonly used products by organizations.

PHP is the most widely used technology, which contrasts with other analysis we've done. It's an old technology, but widely used, with many known CVEs for multiple packages, CMSes and frameworks. This doesn't imply it's unsafe, but it does require more upkeep from security teams. We've also found other technology choices, this time more common, such as Nginx, Cloudflare, or AWS Cloudfront, widely used across every industry.

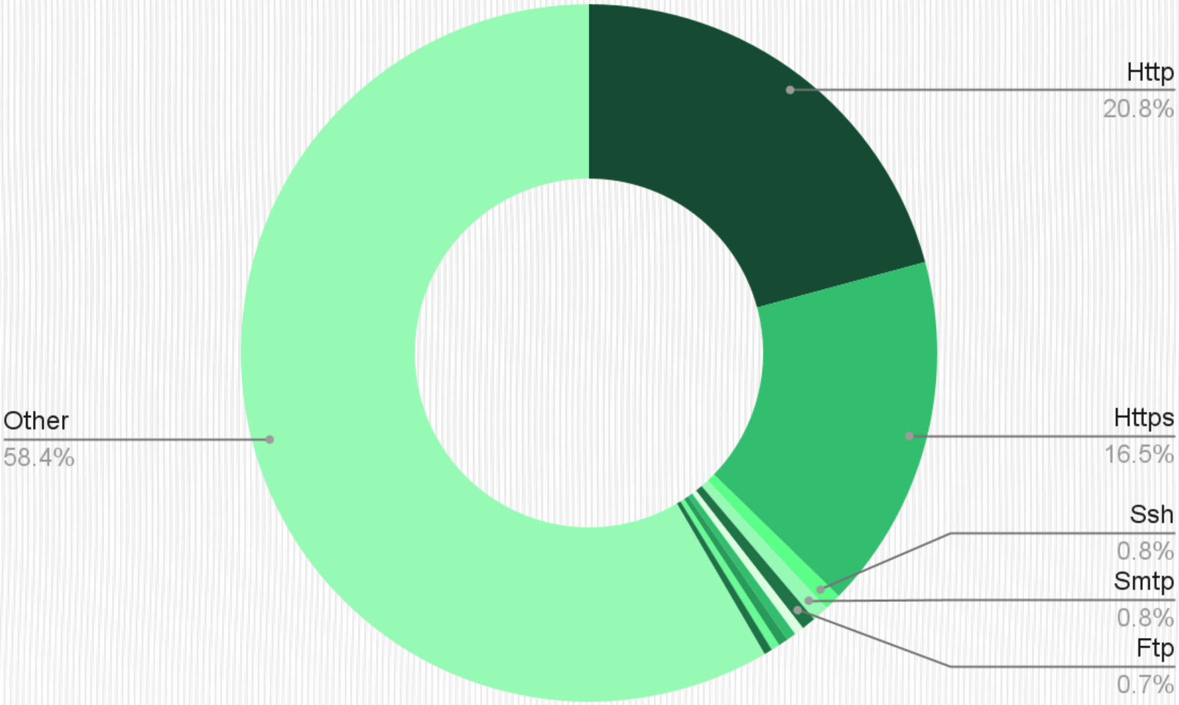

Image 6 - Distribution of services used

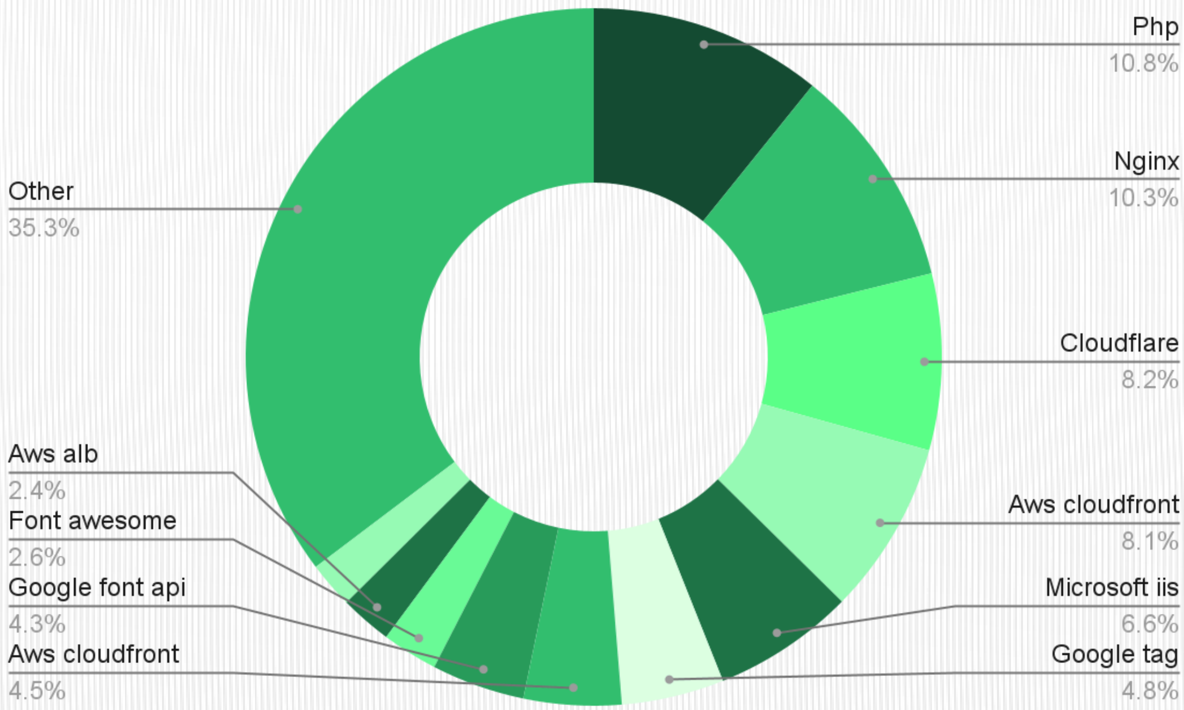

Image 7 - Distribution of technologies used

When it comes to web servers, Cloudflare dominates, representing 28% of web servers analyzed. Nginx and Apache follow closely, with 21% and 15% of web servers using them, respectively. These are the most common options we observe, and together they account for nearly two-thirds of web servers analyzed.

Using common choices brings advantages and disadvantages: while on the one hand they're proven and, if there's a vulnerability, a fix should be quickly rolled out, the fact that they're so widespread can lead to chain reactions, as we've seen from the impact of the recent Cloudflare downtime events.

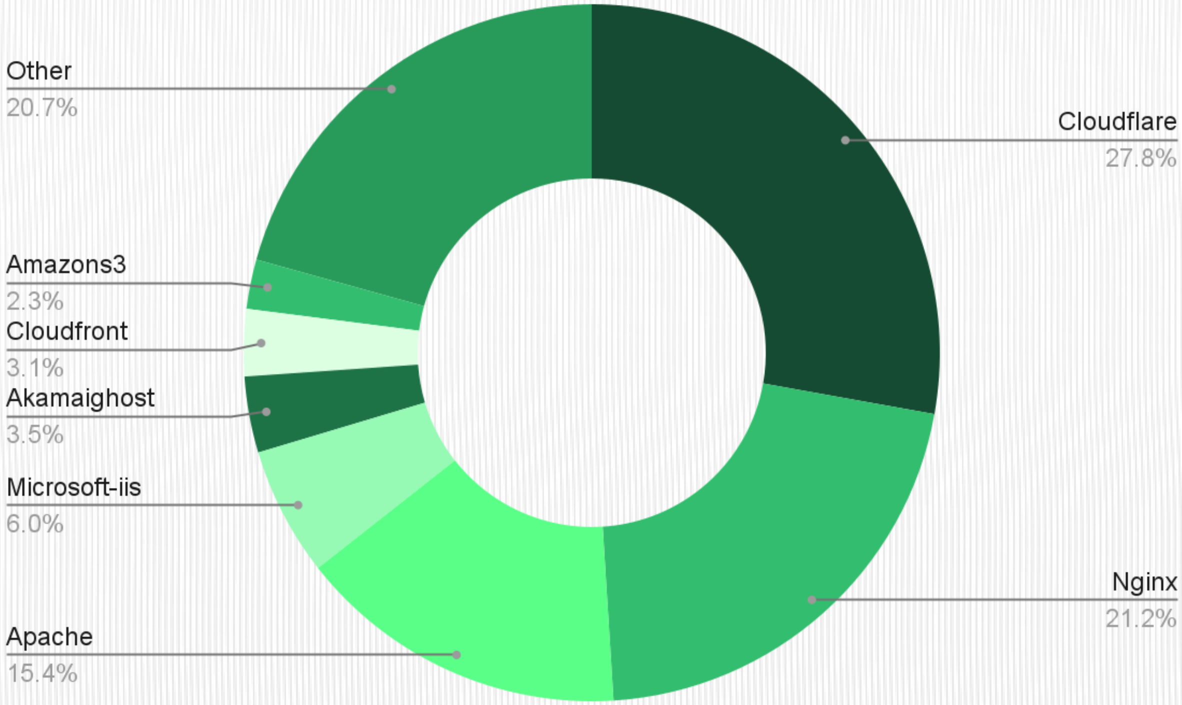

Image 8 - Distribution of web servers used

Despite the massive difference in the average number of assets, there isn't a big discrepancy in the technologies used. The most common web servers, regardless of size, are Nginx, Cloudflare, Apache, IIS, and Akamai, suggesting that as Retail organizations grow, the underlying tech stack remains the same.

Shadow IT and Ecosystem Complexity

While our reconnaissance tool identified 57,898 exposed assets across 1,722 domains, this represents only the visible tip of the attack surface. A significant blind spot in retail cybersecurity is shadow IT: systems, integrations, and data flows created outside formal IT governance, often by marketing, product, or business development teams pursuing partnerships and customer engagement initiatives.

This challenge is particularly acute in customer loyalty and partnership ecosystems. When retailers integrate with airlines for points-sharing, with ride-sharing services for promotional campaigns, or with financial services for co-branded credit cards, each integration creates technical dependencies that may not be fully visible to security teams.

"*Shadow IT in retail doesn't usually come from rogue employees installing unauthorized software,*" explains Gabriel Moliné, CISO at Carrefour Spain. "*It comes from legitimate business initiatives: a marketing team* *launching a loyalty partnership, a product team integrating a new customer experience feature. These generate real technical infrastructure and data flows that security teams discover after the fact.*"

The traditional "security as gatekeeper" approach fails in this environment. Moliné advocates for a fundamental shift: "*Security should be part of the ice cream, not the topping. We need to be closer to business processes rather than being 'Mister No.' Focus on understanding people before technology.*"

This organizational challenge explains why even security-conscious retailers struggle with complete attack surface visibility. The 99% external asset coverage achieved by leading digital retailers like Nemlig still leaves AI implementations and third-party integrations as acknowledged blind spots—precisely the areas where shadow IT emerges.

"*Shadow IT in retail doesn't usually come from rogue employees installing unauthorized software. It comes from legitimate business initiatives: a marketing team launching a loyalty partnership, a product team integrating a new customer experience feature. These generate real technical infrastructure and data flows that security teams discover after the fact.*"

Gabriel Moliné, CISO @ Carrefour Spain

Security Posture in Exposed Assets

Regarding the security posture associated with the exposed digital infrastructure, it was possible to analyze the use of valid SSL digital certificates and the exposure of information from web servers.

In terms of SSL certificates, it was found that 16% had either invalid or outdated certificates, following bad practices. Such a situation could allow an attacker to intercept traffic when connected to the same network, enabling attacks such as eavesdropping and man-in-the-middle.

This lack of updates often happens due to a lack of visibility on their attack surface, which leads to these weaknesses going unnoticed. This is corroborated by the fact that companies with more than 100 assets, and therefore more complex attack surfaces, show a worse posture, with 19% of them using bad practices in SSL certificate management. Companies with fewer assets show a better posture, with those having fewer than 50 assets averaging 16%, and those with fewer than 10 assets averaging 12%.

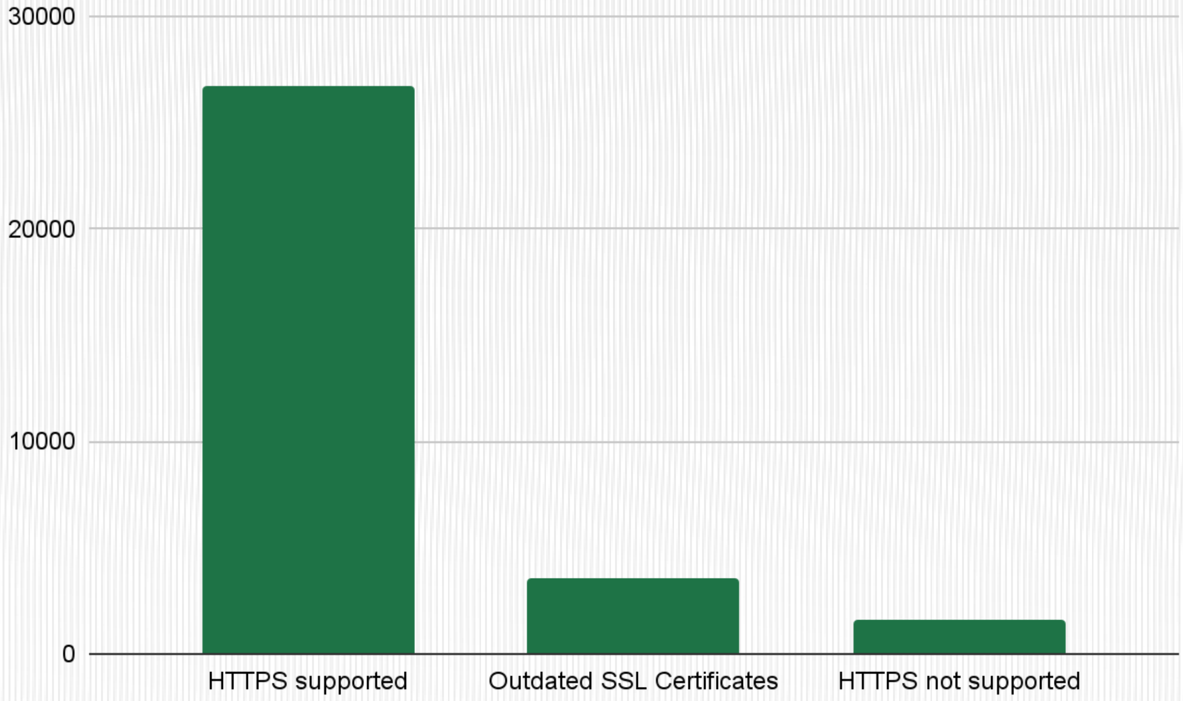

Image 9 - Types of SSL certificates

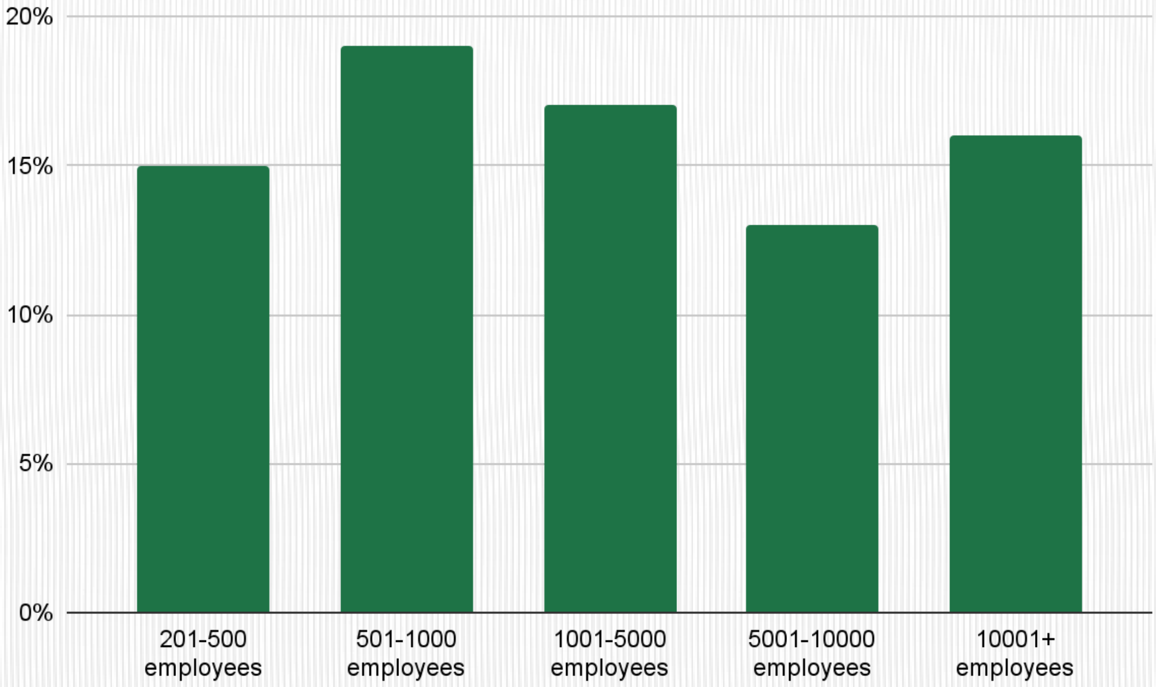

Image 10 - Percentage of SSL certificates with bad practices based on employee size

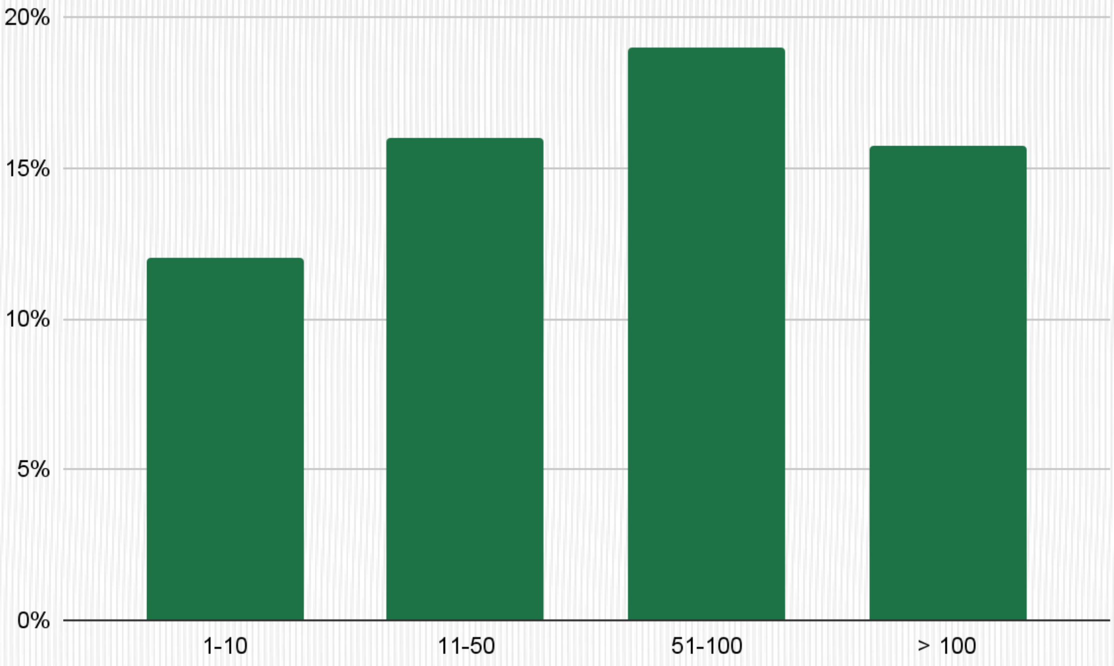

Image 11 - Percentage of SSL bad practices by asset bracket of the company

An example of best practice in remediation is Nemlig's approach. The goal is a one-week MTTR (Mean Time To Remediation), with a hard maximum of three weeks for the most complex scenarios. This is achieved through an offensive-first security strategy that includes 24/7 SOC coverage, continuous vulnerability assessment, and an aggressive prioritization approach that treats anything above CVSS 4.0 as serious—particularly for Internet-exposed assets.

"*We combine CVSS and EPSS scoring with deep understanding of our infrastructure connectivity,*" explains Aziz. "*If something is externally exposed, it's automatically a high priority regardless of theoretical scoring.*"

Another concerning situation identified, which may increase the risk of cyberattacks, stems from the fact that approximately 17% of web servers expose information about their version and software. When exposed, this information can be used to exploit vulnerabilities associated with it and ease the work of cybercriminals, as they can quickly look up known CVEs and vulnerabilities of these web servers.

While we initially thought bigger attack surfaces would lead to more web servers with exposed information, we were surprised to find that as the number of assets increases, the percentage of exposed web servers decreasing, following the opposite trend observed with SSL certificates.

We found two explanations for this divide. First, bigger companies are more rigorous in their security processes and often standardize their tech stack choices, including web servers. Additionally, while there are many places where an SSL connection can be invalid or outdated, servers are easier to patch, and one server can be used for many assets.

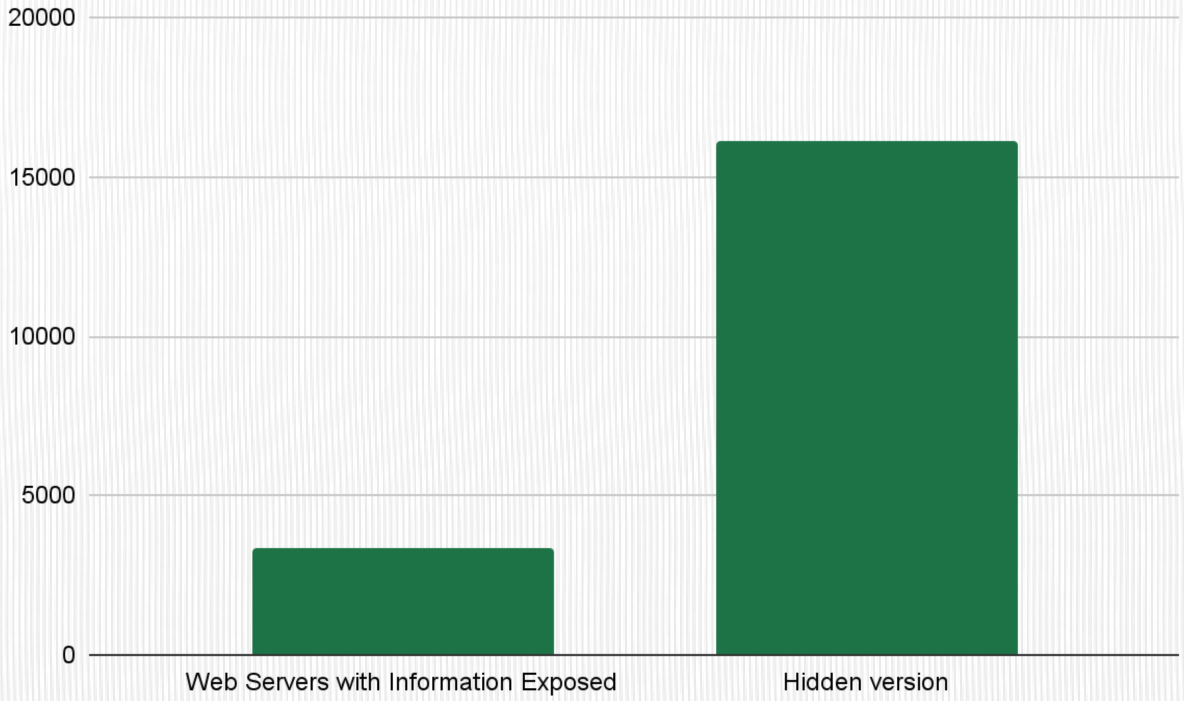

Image 12 - Number of web servers with exposed configurations

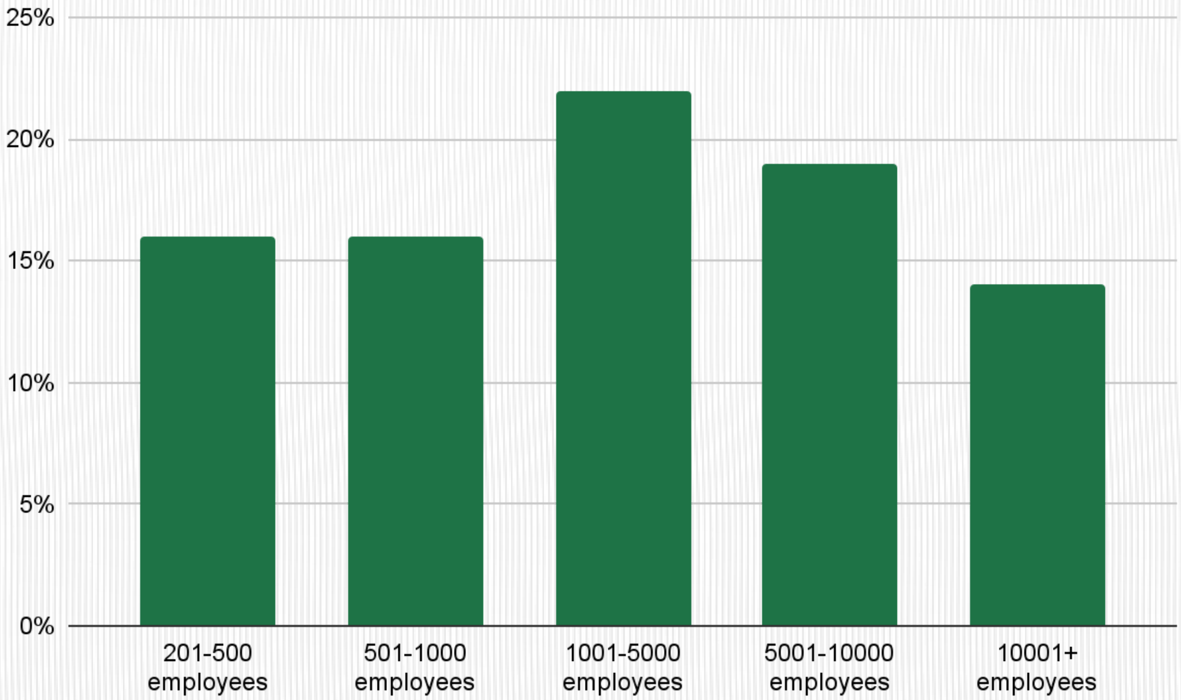

Image 13 - Percentage of web servers with exposed configurations by employee size

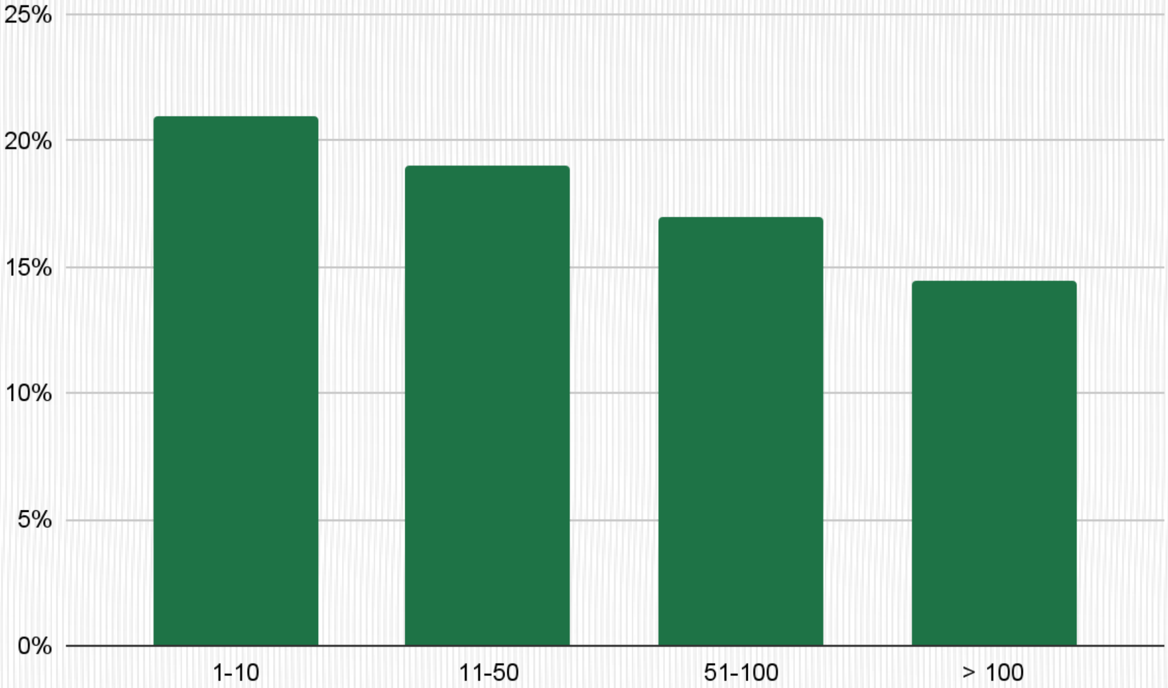

Image 14 - Percentage of exposed web server configs by asset bracket of the company

Analysis by Country

An interesting analysis to be made is a breakdown by country. As previously mentioned, the United Kingdom has the most assets, with over 15,000 assets belonging to British companies. France takes a distant 2nd place, with 8,700 assets, followed by Germany with 6,500. Smaller countries, like Latvia, Cyprus, or Bulgaria, occupy the bottom of the table with fewer than 50 assets each.

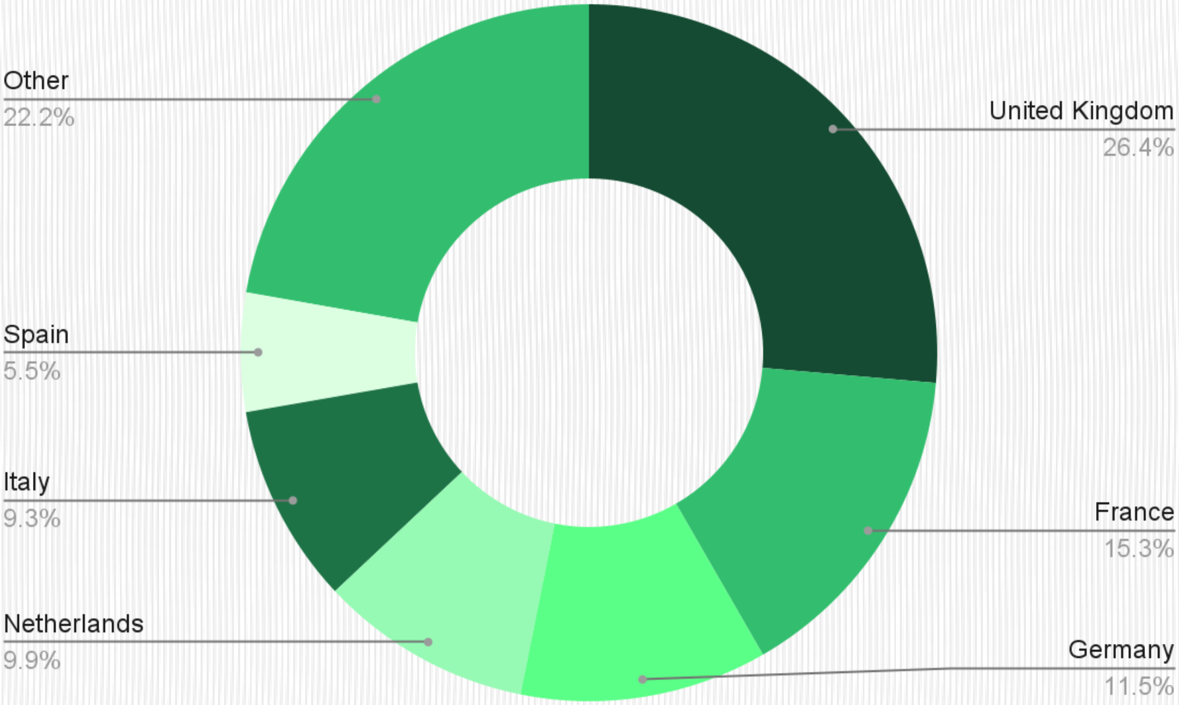

Image 15 - Distribution of assets per country

Looking at which countries have the most weaknesses, Ireland stands out for having the worst practices for SSL certificates, as we observed them in 22% of the cases. They were followed by the United Kingdom with 19.8%. As for exposed webservers, 27% of Danish servers were revealing them, followed by 26% of Swedish assets.

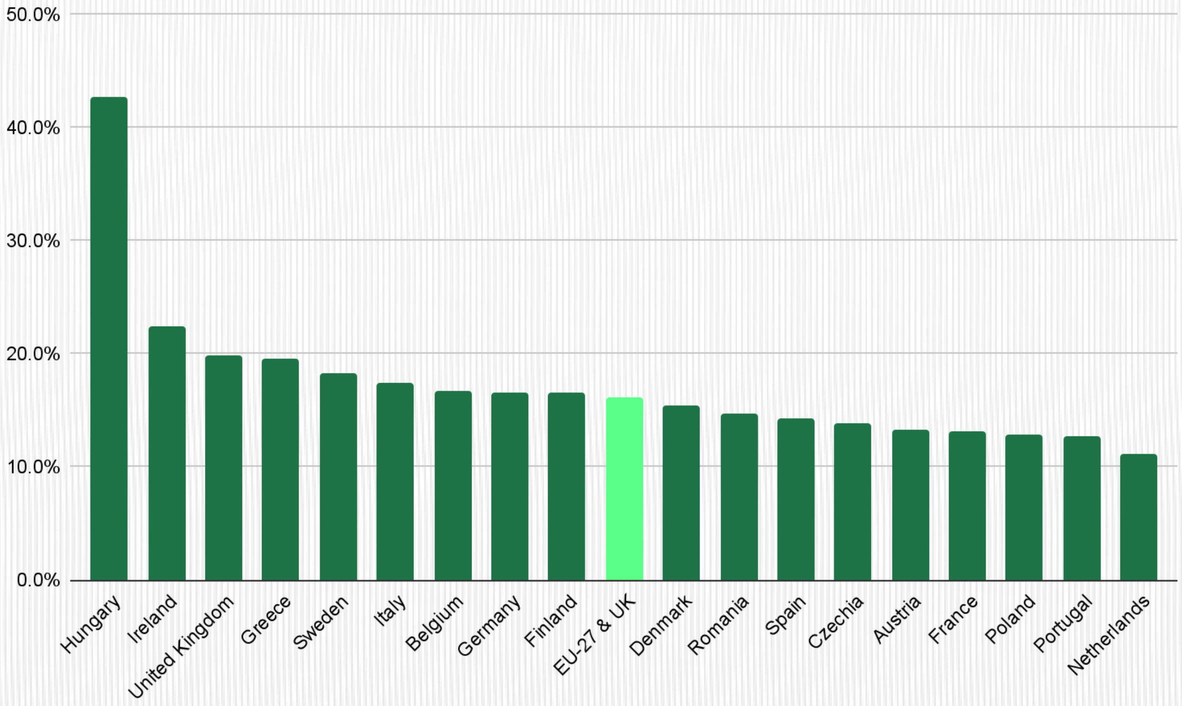

Image 16 - Percentage of SSL bad practices by country

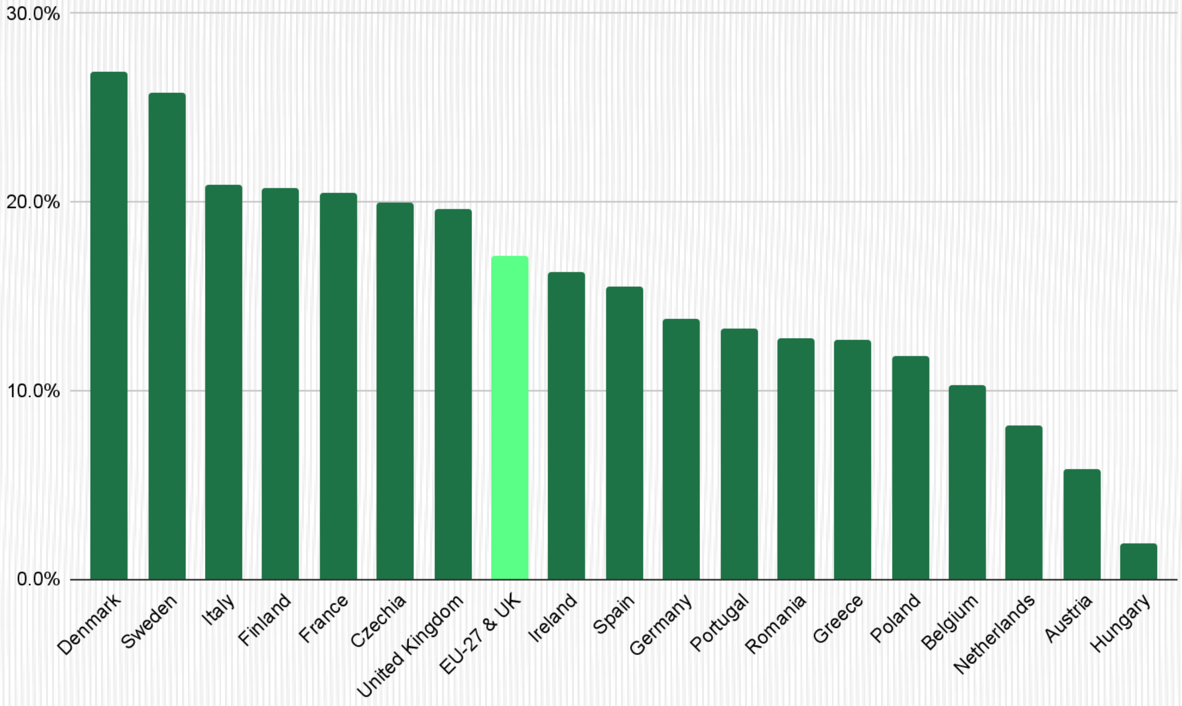

Image 17 - Percentage of exposed web servers configurations by country

Another country that stands out is Poland, for having an above-average security posture compared to its European peers. While Polish GDP per Capita lags behind the European average, it has been a prime target for cyberattacks, especially by state actors. Microsoft's Digital Defense Report puts Poland as the 3rd most targeted country in Europe, and the target of 3% of Russia's threat actors. This pressure emphasizes the need of investing in cybersecurity, especially when the same report reveals retail is the target of 7% of nation-state actors.

Analysis by Asset Importance

We also dove into the importance of assets being used and their weaknesses. Assets vary by importance, depending on their impact of business operations in case of a breach. An email server, or an asset containing critical business information, would obviously be more impactful to the organization in case of a breach.

That being said, we found 1,208 assets we deemed important – email servers, admin dashboards, VPNs, checkout flows, etc – and in these, we found several weaknesses. 12% of important assets had exposed web server configurations, and 3.72% had SSL bad practices. Webmail assets had the worst security posture, with 34% exposing their configs and 10% having SSL bad practices.

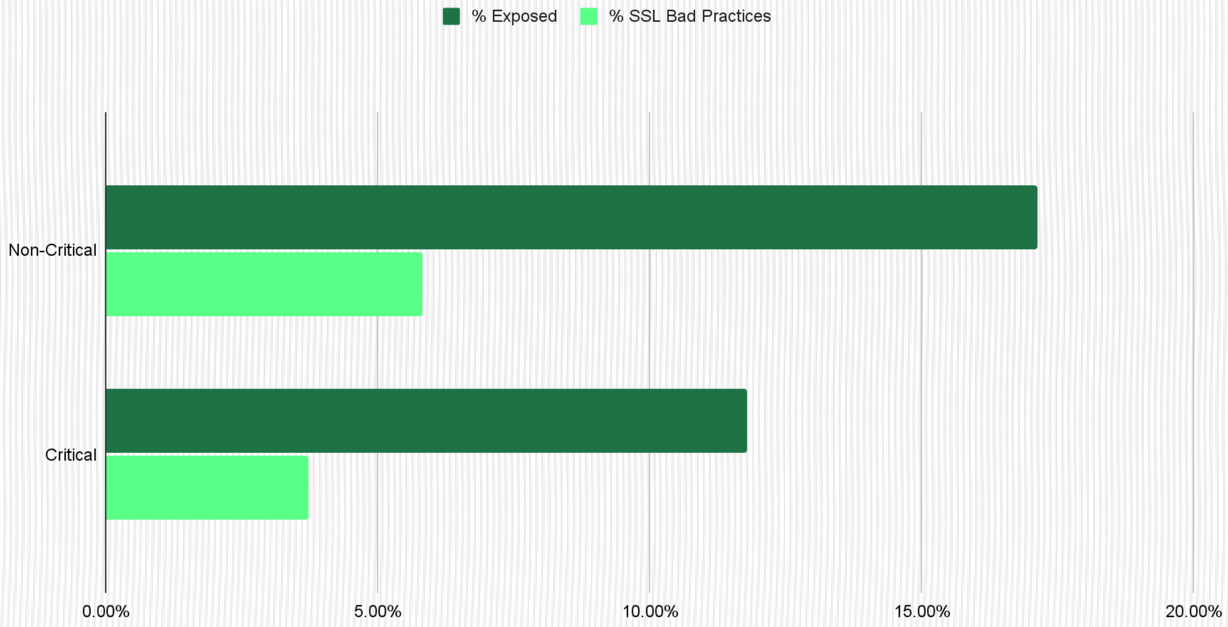

Image 18 - Exposed Web Server Configurations and SSL bad practices by asset importance

It's important to note that, despite these gaps in security, critical assets still show a better security posture compared to non-critical assets. 17% of non-critical assets exposed their web server configuration files, and 5.8% displayed SSL bad practices. Companies are aware of their importance, but it's far from perfect.

Many of these issues could be fixed by implementing proper Attack Surface Management (ASM) tools, which would map these assets and maintain security teams posted on how their infrastructure is growing. Combined with AI Pentesting, they could find out which weaknesses and vulnerabilities exist in their assets as they appear.

Analysis of AI Pentesting Data

By testing multiple Retail organizations, often with hundreds or thousands of assets under scope, we're able to collect information on the overall trend regarding vulnerabilities in the sector.

Some of the most common CVEs we see in retail are CVE-2020-10770, CVE-2023-5558, CVE-2021-20323, CVE-2023-24243, CVE-2019-11248. These are impactful under the CVSS system, with scores ranging from 5.30 to 8.90, highlighting that even with extensive security teams and policies, CVEs can show up.

Of these, CVE-2019-11248 (Kubelet Exposed Debug Endpoint) is an interesting example - while EPSS data shows it has a 3% probability of being exploited in the wild, our data set shows it's quite common in Retail organizations.

This often happens due to the massive infrastructure and complexity of retail organizations, together with the fact that it's simply impossible for a human-only team to keep up with all the code changes, new CVEs, and testing requirements.

CVE	CVSS	EPSS
CVE-2020-10770	5.3	0.9228
CVE-2023-5558	6.1	0.0313
CVE-2021-20323	4.3	0.6605
CVE-2023-24243	7.5	0.8861
CVE-2019-11248	8.2	0.9121

Source: cvedetails.com

As for impact, CVE-2020-35489, CVE-2022-22536, and the recent CVE-2025-55182 (React2Shell) are among the most impactful vulnerabilities found in Retail. These are highly impactful vulnerabilities, with devastating consequences for business if exploited – reinforcing the need for the rapid results provided by AI pentesting.

CVE	CVSS	EPSS
CVE-2020-35489	10	0.9011
CVE-2022-22536	10	0.9383
CVE-2025-55182	10	0.7780

Source: cvedetails.com

Prioritizing Remediation

Even if you know all the risks and vulnerabilities, you'll still need to patch them – and that's a whole other battle. The more critical challenge facing retail security teams is prioritization and remediation at scale, particularly for organizations managing legacy systems during cloud migration.

Gabriel Moliné, CISO at Carrefour Spain, describes a common mistake: "*Handing IT a raw list of findings ranked only by CVSS does not drive effective remediation. Prioritization must be aligned to exposure, business criticality, and exploitability.*"

The gap, according to Moliné, is due to a "*lack of realistic, ecosystem-specific vulnerability prioritization*." A CVSS 8.0 vulnerability in an Internet-isolated legacy system may represent less real-world risk than a CVSS 5.0 vulnerability in a customer-facing payment API. Yet many organizations lack the contextual infrastructure understanding to make these distinctions.

Leading retailers address this through exposure-based prioritization. At Nemlig, CISO Ali Aziz explains: "*We combine CVSS and EPSS scoring with a deep understanding of our infrastructure connectivity. If something is externally exposed, it's automatically a high priority regardless of theoretical scoring. Anything above CVSS 4.0 gets taken seriously.*"

This approach, combining automated scoring with infrastructure context and exposure analysis, is precisely what AI-powered continuous pentesting enables. Rather than generating undifferentiated vulnerability lists, autonomous testing with proof-of-exploitation validates which vulnerabilities are actually exploitable in your specific environment and infrastructure configuration.

Conclusions and Recommendations

The findings of this report paint a concerning picture of the cybersecurity posture of European retail companies. With an average of 33 exposed assets per organization (and significantly more for larger enterprises) the attack surface available to cybercriminals is substantial and growing. This expansion, combined with the persistent use of legacy technologies like PHP and widespread security misconfigurations, creates an environment ripe for exploitation.

Five critical vulnerabilities stand out across our analysis:

First, **visibility gaps remain pervasive**. Over 15% of SSL connections display bad practices, and 17% of web servers expose sensitive version information. These are basic hygiene issues that persist because organizations lack complete visibility into their attack surfaces. This mirrors industry research showing that 37% of enterprise-level attack surfaces are unknown to security teams. You cannot defend what you cannot see.

Second, **critical assets are insufficiently protected**. Our analysis identified 1,208 high-importance assets—email servers, admin dashboards, VPNs, and checkout flows—with notable weaknesses. Webmail showed the worst posture, with 30% exposing configurations and 10% running SSL bad practices. These are precisely the assets that, if compromised, would cause maximum business disruption and data loss.

Third, **the vulnerability landscape is accelerating faster than organizations can respond**. Our AI pentesting data reveals multiple high-severity CVEs actively present in retail infrastructure, including critical CVSS 10.0 vulnerabilities. With Time-to-Exploit now averaging -1 days and CVE disclosures up 16% in 2025, traditional periodic pentesting approaches are fundamentally inadequate.

Fourth, **large organizations play a key role in eliminating the digital divide**. Smaller companies are most vulnerable, and by having large organizations test their third parties and enforce strong cybersecurity standards, they can at the same time protect themselves, creating a "group immunity" effect.

Fifth, **the retail sector faces an AI-accelerated threat landscape that will intensify in 2026**. Security practitioners observe that AI enables attackers to scale and personalize social engineering campaigns while conducting sophisticated automated pentesting. "*AI will absolutely become a major problem next year. The defensive advantage we have today shrinks rapidly.*"

The recent attacks on major European retailers—from the £300 million loss at Marks & Spencer to the data breach affecting nearly half a million Harrods customers—demonstrate that these are not theoretical risks. They are active, costly realities.

Recommendations

Based on these findings, European retail organizations should prioritize the following actions:

- **Move beyond point-in-time assessments to continuous discovery and testing** of all exposed digital assets, including third-party and supply chain connections. Implement a Continuous Threat Exposure Management (CTEM) program with Attack Surface Management (ASM), Adversarial Exposure Validation (AEV) and Pentesting as a Service (PTaaS).
- **Deploy autonomous, AI-powered penetration testing.** Traditional annual or quarterly pentests cannot keep pace with modern development cycles and the velocity of new vulnerabilities. Continuous, event-driven testing triggered by code changes, infrastructure updates, or new threat intelligence is essential.
- **Address basic security hygiene immediately.** Invalid SSL certificates and exposed server configurations are low-hanging fruit for attackers. Automated monitoring and remediation of these issues should be standard practice.
- **Prioritize critical asset protection.** Map and continuously test high-value assets—authentication systems, payment flows, customer databases, and administrative interfaces—with particular attention to validation and proof-of-exploitation, not just detection.
- **Test third-party assets.** Several high-profile breaches happened due to compromised third-parties, and industry experts reveal these are even being used for social engineering. By enforcing good security postures on their suppliers, large organizations can help create a "group immunity" effect.
- **Establish or expand Bug Bounty Programs (BBPs) or Vulnerability Disclosure Programs (VDPs).** Enable the security research community to help identify vulnerabilities before malicious actors exploit them.

The correlation between company size, revenue, and security posture suggests that cybersecurity investment scales with resources—but it shouldn't take a breach to prioritize security. Smaller companies in our sample showed higher vulnerability rates per asset, indicating they face disproportionate risk relative to their defensive capabilities.

The European retail sector stands at a critical juncture. Attack surfaces are expanding, threat actors are accelerating, and the margin for error continues to shrink. Organizations that embrace continuous, autonomous security testing—combining AI speed and scale with human expertise—will be positioned to discover and remediate vulnerabilities before they become breaches. Those who rely on periodic assessments and reactive measures will continue to appear in breach headlines.

The choice is clear: evolve security practices to match the threat landscape, or accept that a breach is not a question of if, but when.

Ethiack