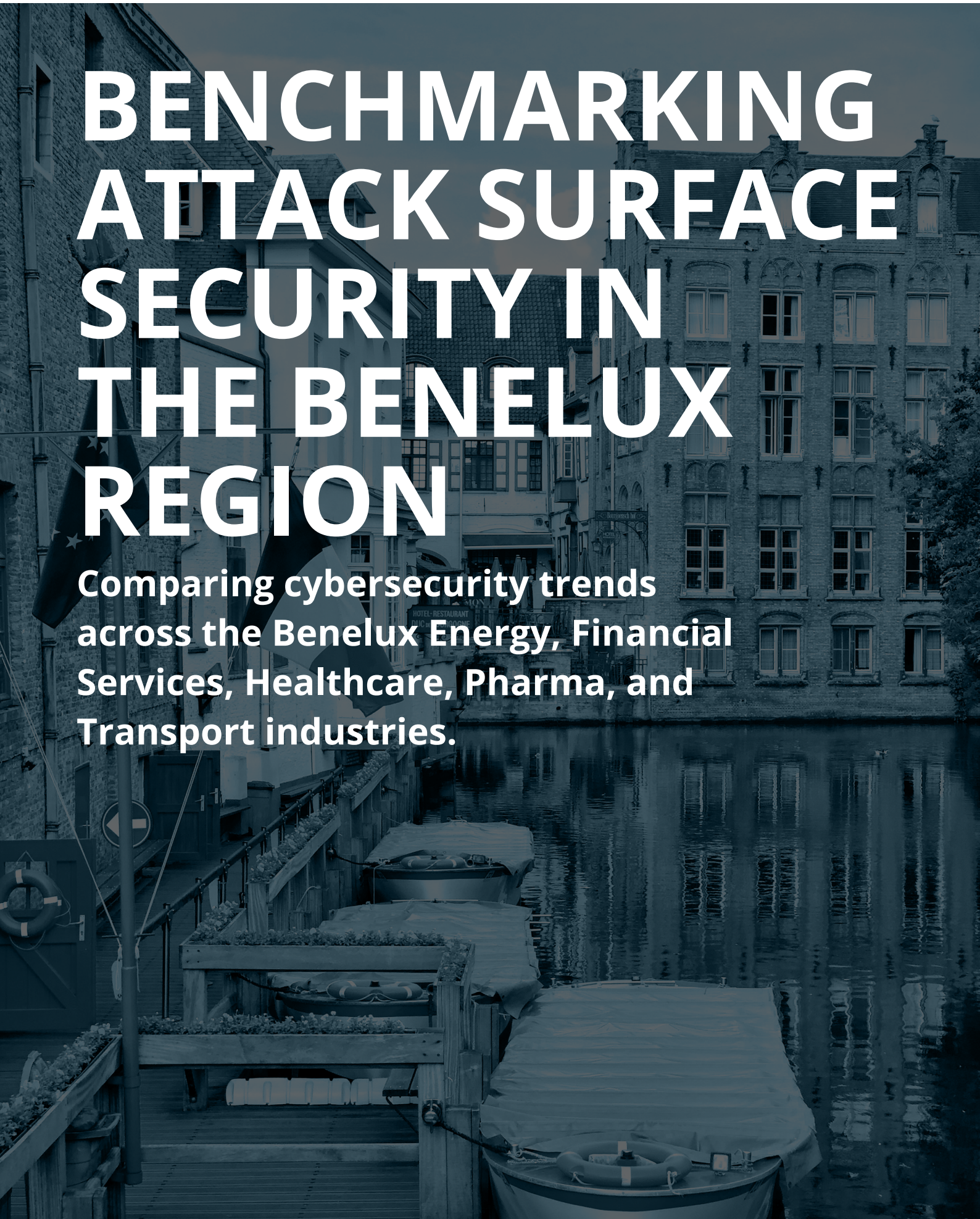
AN OUTPOST24 WHITEPAPER

Outpost24



BENCHMARKING ATTACK SURFACE SECURITY IN THE BENELUX REGION

Comparing cybersecurity trends across the Benelux Energy, Financial Services, Healthcare, Pharma, and Transport industries.

Contents

Data highlights

30,000 online assets analyzed

>18% of observations in all industries ranked critical, very high, or high

Healthcare worst with 27.2% ranked critical, very high, or high

Known Exploitable Vulnerabilities

55% of Healthcare's KEVs rated as critical or very high

Compared to just 3% in Financial Services

All industries: >20% of analyzed web servers had a 4xx or 5xx error code

Healthcare had the worst web server 'cyber hygiene' score

Energy had the lowest proportion of 4xx and 5xx errors

Financial Services: most credentials leaked on the dark web

Transport: highest number of malware-stolen credentials

Web server encryption issues

Pharma industry had highest proportion (27%)

Energy had the lowest (13%)

How we benchmarked the Benelux region's attack surface security

The Benelux region has seen increased levels of cybercrime in recent times, especially in the years following the COVID-19 pandemic. In 2022, Belgium had 94 cybercrime victims per million internet users, behind only the US, UK, and Canada. During the same period, 15% of the Dutch population over the age of 15 indicated they had been victims of online crime.

Perfection is impossible in cybersecurity – it's unlikely we'll ever see the day where there are no vulnerabilities or risks to address. Despite that, organizations want to know they're doing the best they can. For that purpose, it's interesting to know where you stand in your cybersecurity efforts among organizations within your industry. At Outpost24, we've used our external attack surface management (EASM) solution to provide a 'benchmark' of how different attack surfaces compare between some of the biggest industries within the Benelux region.

For the purpose of this analysis, we selected five major industries within the Benelux region: Energy, Financial Services, Healthcare, Pharma, and Transport. From each of these industries, we selected a mix of (non-customer) organizations, representing a healthy mix of larger well-known companies and smaller ones. Then for each organization, we analyzed an average of ten domains (a primary domain being the top domain of a business – like Outpost24.com). From there, our technical teams pulled out some of the most interesting data trends.

> **"It's interesting to know where you stand among organizations within your industry.**

Outpost24's EASM solution finds and analyzes public IT assets that are connected to the internet by simulating normal internet traffic, passive discovery, and testing techniques. This gives full visibility into both the known and unknown assets comprising an organization's assets and scores them in terms of risk. It's a completely passive process and only analyzes publicly accessible information.

The analysis was run in March 2024. This provided a snapshot which will shift over time, so some results may not be identical to when the analysis was run. However, we expect the general trends to remain consistent. We hope this provides you with some valuable context on where the most common risks and vulnerabilities are found in the region's key industries. We'll also show how you can use EASM to evaluate your own organization's attack surface and find out how you compare to the industry benchmarks.

Ranking the proportion of critical risks

We analyzed almost 30,000 assets during the benchmarking process. If an asset was found to have a security issue, we classed it as an observation and give it a score based on how serious the risk was. In terms of ranking the risk of observations, we used a simple classification system that ranks issues from the most to least serious: Critical, Very high, High, Medium, Low, and Very low.

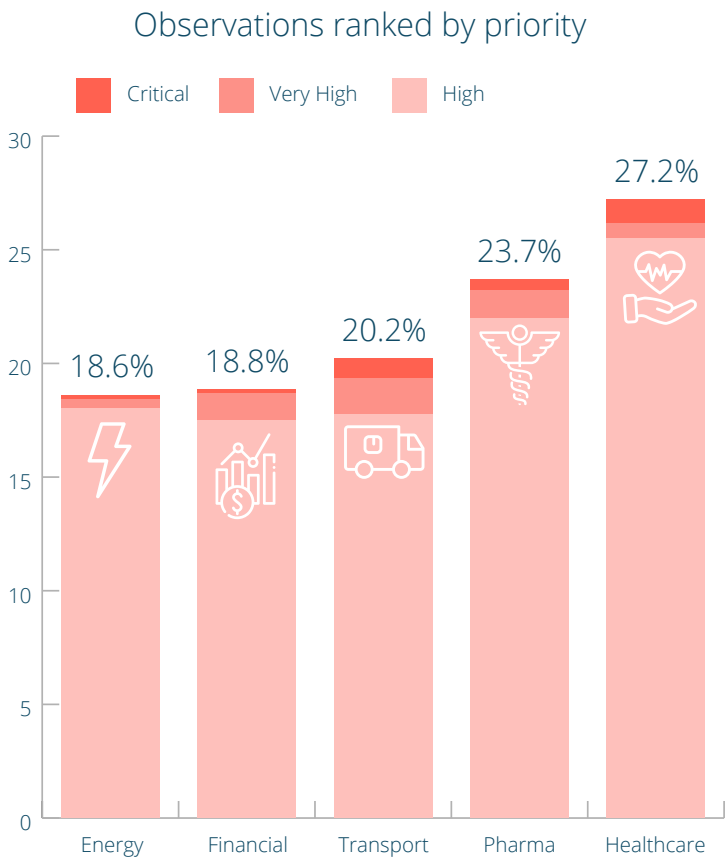
Attack surfaces are always expanding, and they can get vast pretty easily for larger organizations. It can be hard to know where to start for IT Security teams, so a key part of EASM is being able to rank issues and triage what needs dealing with first. For this analysis, we wanted to focus on the problems organizations need to solve most urgently. So how did the five industries stack up in terms of the percentage of observations ranked as Critical, Very high, and High?

What the data shows

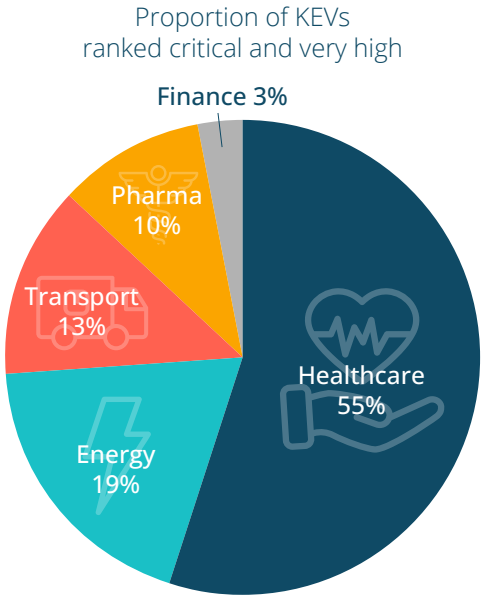
As you can see from the graph below, the healthcare industry had the highest number of observations (27.2%) ranked as Critical, Very High, and High. Energy had the smallest proportion of dangerous observations (18.6%) with financial services (18.8%) also scoring well relative to healthcare. It's hard to say for sure why these two industries had the fewest serious observations, although it could be to with industry-specific regulations. Of course, it's worth noting that >18% of high-critical observations over all industries represents a lot of potential risk across all the analyzed organizations.

From here, we broke down the data further and looked at the amount of known exploited vulnerabilities (KEVs) that showed up in each industry's combined attack surface. KEVs are vulnerabilities from databases of known risks. They're particularly dangerous, as we already know they can be (and likely will be) exploited by bad actors if left unresolved. As they're already known and documented, the intention is that organizations stay on top of remediating them.

As an example of a KEV, we can highlight CVE-2021-40438 which is regarding a known Apache exploit. This vulnerability was found spread across all sectors except for financial services.



The overall results once again paint a concerning picture for the healthcare industry, with 55% of their observed KEVs being rated as critical or very high. The Benelux financial services industry had things under pretty tight control with only 3% of observed KEVs being ranked as critical or very high. As shown in the below chart, the other industries all ranked between 10 and 20%.



OUTPOST24 ANALYSIS

Why the bad diagnosis for healthcare?

There are several possibilities why Healthcare has scored poorly in this section. Organizations in the sector process large amounts of sensitive and personal data (addresses, national registration numbers, health histories etc.). This data is an attractive target for hackers who can use it commit identity theft or sell it on to other threat actors.

The industry is under a lot of pressure. Legacy systems are more likely to be in place than in an industry such as Financial Services, and non-technical staff are understandably more focused on patient wellbeing than cybersecurity. Staff need to access systems quickly and simply, which doesn't always line up with cybersecurity best practices. Unfortunately, this makes for an environment where vulnerabilities can thrive and makes it an attractive target for threat actors.

A lack of funding for cybersecurity staff and technology compared to other industries can also be an issue with Healthcare. As why did Financial Services have so few critical and high KEVs? It's possible that tight regulations, more money available to spend on cybersecurity, and the risk of financial penalties play a part here. However, with NIS2 coming into effect on 17th October 2024, time is of the essence for Healthcare organizations to strengthen their cybersecurity posture.

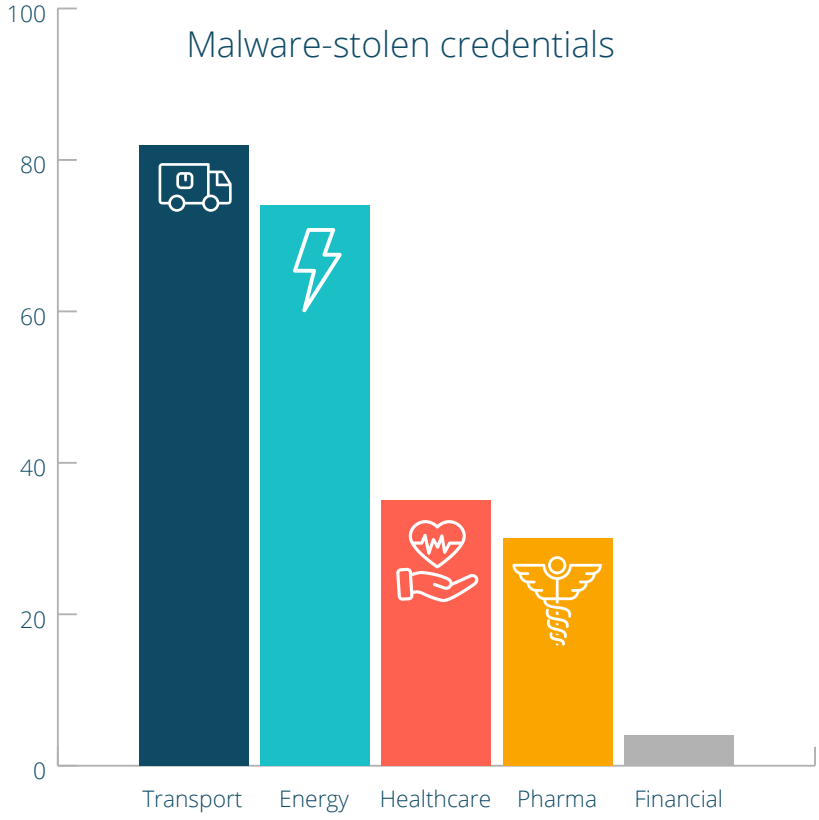
Leaked and stolen credentials

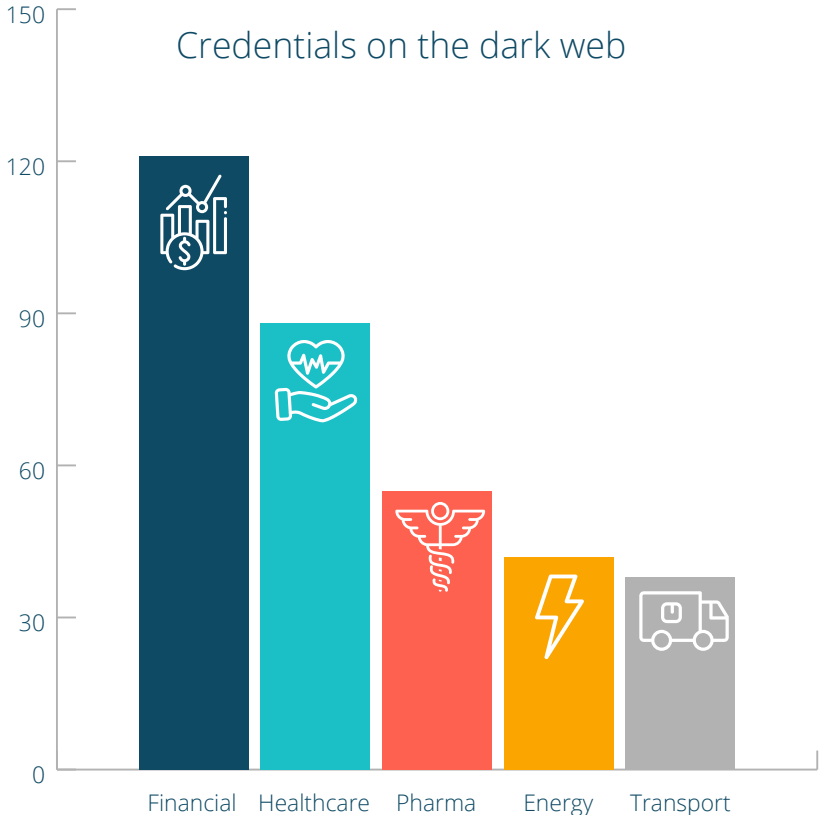
Stolen credentials are the easiest way for hackers to gain an initial foothold in your environment. During this analysis, Outpost24's EASM tool used its integrated Threat Intelligence information to detect if users from the analyzed domains have had their credentials leaked or stolen. The solution splits the results into two different categories: malware-stolen and dark web.

With malware-stolen credentials, the end user may have accidentally downloaded the malware or used an infected website on their work device, or they reused their work login credentials on a malware-infected personal device or website. Dark web credentials have been found by the Threat Intelligence team for sale on underground forums or marketplaces.

What the data shows

Interestingly, the Financial Services sector had the fewest malware-stolen credentials but the highest number of credentials for sale on the dark web. This could suggest that organizations within the Financial Services industry have invested in cybersecurity that is good at stopping malware, while also suggesting their end users' credentials are highly sought after on the dark web by initial access brokers.





This also highlights that hackers have multiple routes to pursue if they want to target specific industries. While organizations might have one area under good control, they might be vulnerable elsewhere or lacking visibility into a specific problem. If one attack route is blocked, hackers will seek alternative options for getting hold of credentials.

OUTPOST24 ANALYSIS

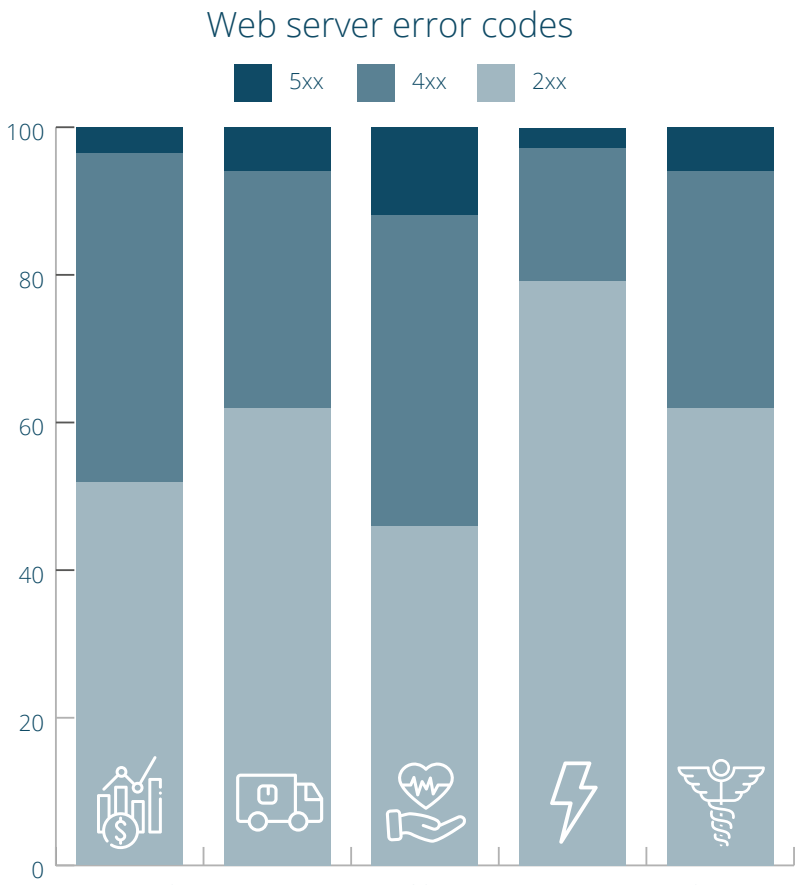
Why we hunt for stolen and leaked credentials

For most organizations, passwords are their weakest link and the easiest route in for hackers. Why hack in when you can log in? Verizon's 2023 Data Breach Investigation Report found that threat actors used stolen credentials in 49% of attempts to gain unauthorized access to organizations. Blocking this initial access is key to stopping further attacks – so it's vital to have a way of knowing whether your organization's credentials are already up for sale online.

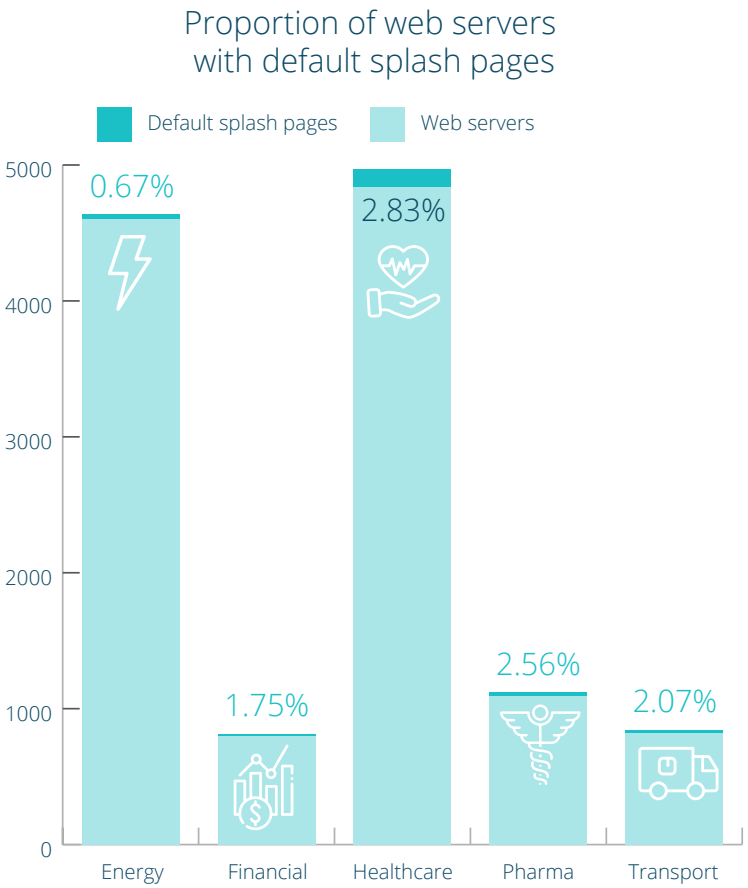
Web server hygiene and encryption

When we talk about 'cyber hygiene' we mean efforts to maintain hardware and software's basic health and security – like dealing with web server error codes. HTTP status codes classify responses from the server to the browser-side request. Sometimes a request results in an error when a user tries to interact through a browser – '404 page not found' being the common one everyone would know. All HTTP response status codes are separated into five categories, which are defined as:

- **1xx informational response** – the request was received, continuing process
- **2xx successful** – the request was successfully received, understood, and accepted
- **3xx redirection** – further action needs to be taken in order to complete the request
- **4xx client error** – the request contains bad syntax or cannot be fulfilled
- **5xx server error** – the server failed to fulfil an apparently valid request



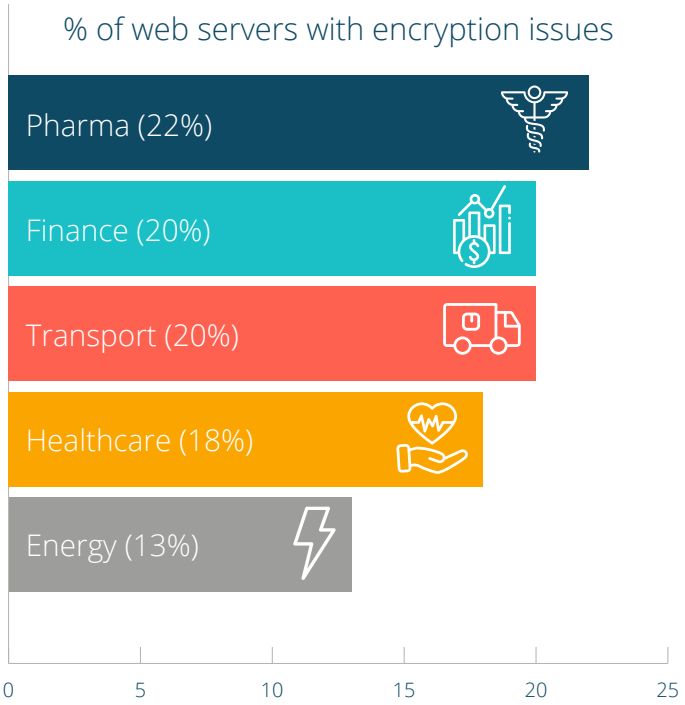
Addressing these problems should be a quick win for organizations, although that's assuming they're aware of the error codes in the first place. As you can see from the below chart, there's opportunity for digital clean up across the board in all Benelux industries. Over 20% of all web servers had a 4xx or 5xx error code. Healthcare and Financial Services had the most, with Energy having the most 'hygienic' attack surface.



Diving a bit deeper, we can also see how many web servers have a default splash page, which acts a test or placeholder page before actual website content is set up. The left-hand side chart shows the proportion of web servers that have default splash pages, with Healthcare having the most (2.83%) and Energy the fewest (0.67%). Again, this isn't a huge security risk by any means, but it does give a message to attackers that an organization doesn't have a very hardened attack surface. It's another issue that's quick and easy to fix.

Web server encryption

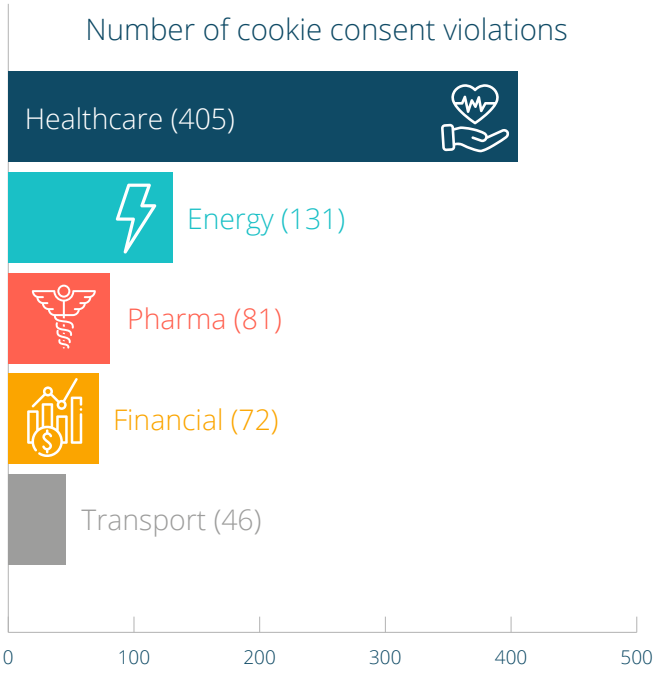
SSL/TLS certificates are digital certificates that authenticate a website's identity and enable an encrypted connection. Misconfigurations with these certificates are some of the most common issues we find when assessing an attack surface. These mistakes can include outdated encryption algorithms, incorrect certificate setup, and expired SSL/TLS certificates. When improperly set up or managed, they can lead to vulnerabilities within your organization's network and create possible entry routes for hackers.



Managing the lifecycle of these certificates can be easy to lose track of, and it's an often-overlooked issue. Expired or invalid website certificates can be off-putting for end users as well as acting as an attack signal for cybercriminals. All industries had issues with over 10% of their SSL/TLS certificates – with Pharma having the most (22%) and Energy the least (13%).

Cookie consent violations

Cookies track users, however there are certain rules and regulations around how a business can use them, which can differ depending on your location. The GDPR requires a website to only collect personal data from users after they have given their explicit consent to the specific purposes of its use. End-user consent to cookies is the GDPR's most used legal basis, so a high number of violations represents potential risk. The results were most concerning for the Healthcare industry, with 405 violations found. Transport had the fewest, with only 46.



OUTPOST24 ANALYSIS

Why does cyber hygiene matter?

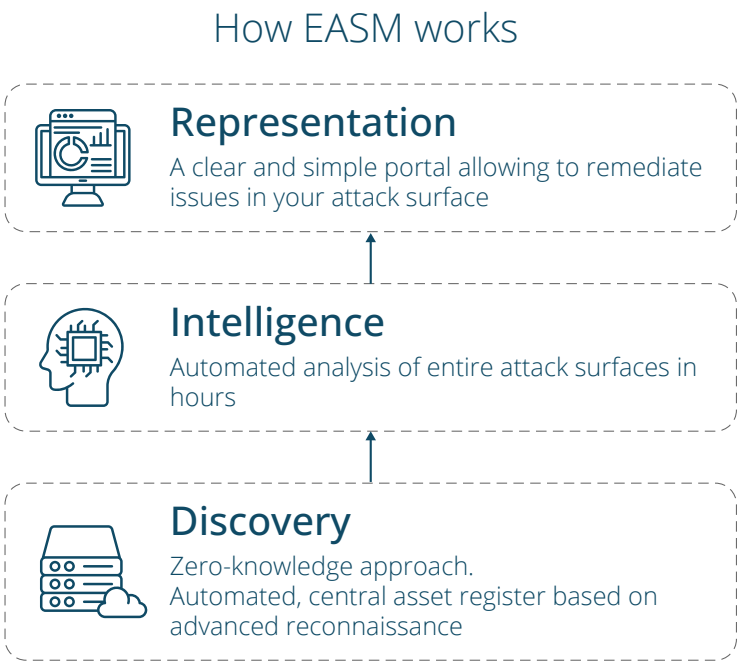
While poor cyber hygiene doesn't necessarily put critical information at risk, it shows organizations are neglecting the basics of keeping their attack surfaces clean. These are green flags for attackers that an organization might be worth attacking. They also contribute to a poorer online experience for customers. Web server hygiene can get bad pretty quickly if nobody is paying attention, so there's value in having an EASM tool to automatically find and track these issues.

Protect your organization with EASM

Processes like vulnerability management are good for evaluating known assets – but up to 30% of an organizations assets can be unknown. This is why EASM is needed to get a full picture of all your public internet-facing assets that could be exploited by attackers. An EASM solution gives IT experts access to ongoing asset discovery and continuous analysis and monitoring of changes in their attack surface.

How EASM works

We can think of EASM as operating across three layers. First, you have the discovery layer where information on every publicly-available asset related to your organization's domains is gathered. Next, information from the discovery layer is presented to the intelligence layer, where the attack surface is analyzed and insights are gathered. Finally, the data is shown in an easy-to-use and interactive representation layer – the portal you'll be able to find issues in and begin working on remediation. The API can also integrate with many third-party destinations.



Where EASM can help

A key facet of EASM is that it's continuous and automatic. An attack surface is always growing, so snapshots aren't good enough. You want to discover your unknowns before hackers do. This means security teams can always have a finger on the pulse, knowing they have an accurate and early warning perspective. Every organization is different, though there isn't one that couldn't benefit from gaining visibility over these online assets.

EASM also helps security teams to prioritize and focus on the most critical issues. Of course, this doesn't mean you ignore the rest of the problems – simply that you deal with the most potentially damaging first. Having a solution that automatically scores or prioritizes those potential risks on an ongoing basis is key, so security teams aren't investing too much time doing this manually.

How does your organization's attack surface compare?

Compare how your own attack surface stacks up to the Benelux industry benchmarks. Run an attack surface analysis with Outpost24's EASM solution to identify areas your cybersecurity is strong as well as some areas where you need to address vulnerabilities.

BOOK YOUR FREE ATTACK SURFACE ANALYSIS TODAY.

Disclaimer

This analysis was conducted externally by Outpost24, using its proprietary External Attack Surface Management (EASM) platform, Sweepatic. Outpost24's EASM finds and analyzes public IT assets that are connected to the internet by simulating normal internet traffic, passive discovery, and testing techniques. Outpost24 is not connected to the infrastructure or business processes of any of the organizations in the scope of this analysis.

About Outpost24

Outpost24 helps organizations improve cyber resilience with a complete range of Continuous Threat Exposure Management (CTEM) solutions. Our intelligent cloud platform unifies asset management, automates vulnerability assessment, and quantifies cyber risk in business context. Executives and security teams around the world trust Outpost24 to identify and prioritize the most important security issues across their attack surface to accelerate risk reduction. Founded in 2001, Outpost24 is headquartered in Sweden and the US, with additional offices in the UK, Netherlands, Belgium, Denmark, France, and Spain.

OUR LOCATIONS

GLOBAL HEADQUARTERS SWEDEN
Blekingegatan 1,
371 57 Karlskrona
Email info@outpost24.com

UNITED STATES HEADQUARTERS
123 S Broad St Suite 2530,
Philadelphia, PA 19109
Tel +1 877 773 267

SWEDEN
Vasagatan 7A,
111 20 Stockholm
info@outpost24.com

DENMARK
Axel Towers 2F, 4th floor,
1609 Copenhagen V
Tel +45 53 73 05 67

FRANCE
291 Rue Albert Caquot 06560
Valbonne, Antibes

UNITED KINGDOM
19 Eastbourne Terrace,
London W2 6AA

Poseidon House,
Neptune Park,
Plymouth PL4 0SJ
Tel +44 20 3735 4986

NETHERLANDS
Stadhouderskade 14J,
1054 ES Amsterdam
Tel +31 20 420 9560

BELGIUM
Ubicenter Gebouw A,
Philipssite 5/bus 17,
3001 Leuven
Tel +32 16 22 76 60

SPAIN
Plaça de Gal·la Placídia,
1-3, Oficina 303,
08006 Barcelona
Tel +34 933 09 61 00

UNITED STATES
35 S Washington St., Suite 308,
Naperville, Chicago, IL 60540
Tel +1 877 773 2677

CANADA
517 Wellington Street West,
Suite 400,
Toronto, ON M5V 1G1
Tel +1 877 773 2677

GERMANY
Gierkezeile 12,
10585 Berlin
Tel +49 30166 37218

Outpost24