2021
WEB APPLICATION SECURITY FOR INSURANCE

Attack Surface Analysis and Benchmark Study for Europe's Top 10 Insurers

Outpost24

Outpost24

EXECUTIVE SUMMARY

Web applications remain the biggest source of data breach at 39%, it's no surprise as they carry a plethora of complexities, layers and this brings potential for vulnerabilities. As businesses look towards digital transformation to support expansion and growth plans this can sometimes leave essential security controls behind. In our 2021 study we have analyzed how the insurance sector fares on application security given the vast volumes of customer and policyholder data they store and process. Using our innovative attack surface discovery and assessment tool - Scout we've looked under the hood of these publicly available insurance applications to uncover potential security weaknesses in their attack surface and how to protect these critical elements.

Similar to our 2020 retail research, we help insurers quickly discover a list of all their live applications on the Internet (including 'staging' or 'production' URLs) as very often they are in the dark about how many publicly exposed web apps are out there and the true extent of their attack surface. See detailed methodology on page 10.

In this report we have outlined the results of our web application security analysis for the Top insurance companies in Europe (EU) listed by ADV Rating to highlight the most common attack vectors affecting insurers through aggregated risk scoring. This will enable insurance security teams and developers to compare and benchmark their attack surface and take the necessary steps to mitigate the biggest threats and optimize security controls.

Key report findings:

- Top EU insurers have an average attack surface score of **38.10** (out of 58.24) vs online retailers at **42.37*** and Credit Unions at **16.39***
- Top EU insurers run a total of **7,611 internet facing web applications** over **1,920 domains**, with **2.98%** of them considered suspicious e.g. test environments
- **22.51%** of these applications identified are found to be using old components containing known vulnerabilities that could be exploited
- Page Creation Method (**77.7**), Degree of Distribution (**77.7**) and Active Contents (**54**) are the top 3 attack vectors identified
- Other security and compliance issues detected include basic SSL, cookie consent and privacy policy defects.

**Results true as of date of publication of Scout Retail and Ecommerce report 2020 (here) and Top 10 US Credit Unions research 2021 (here).*

MANAGING INCREASED RISK FROM DIGITAL TRANSFORMATION

With cyber insurance premiums becoming big business during the pandemic, insurers themselves remain a soft target for cyber attacks. Recent ransomware hits on big names include AXA's 3TB sensitive data leak and US CNA Financial who were forced to pay $40m to regain network control – there is no better time but for the insurance sector to take a magnifying glass to their own application attack surface and digital footprint.

Some of the key security challenges insurers face:

Regulatory pressure:

Insurance companies are governed by GDPR, PCI-DSS, SEC and have the legal responsibility to protect sensitive customer data. Any violation and failure of data protection can result in major fines and financial fallout.

Insider threats:

With 85% of breaches involving human error, intentionally or unintentionally, we've seen security teams feeling the strain to support the business goals and ensuring correct hierarchy of user permissions and authentication is in place to prevent unauthorized access.

Customer experience and trust:

The insurance sector is under pressure to develop and innovate, utilizing the latest application technology to improve access and ease of doing business with customers. As such insurance security professionals have a real balancing act on their hands to make sure security doesn't slip during transformative times. Delivering a first-class digital experience whilst demonstrating security best practice in data protection to maintain public trust.

Increased attack surface:

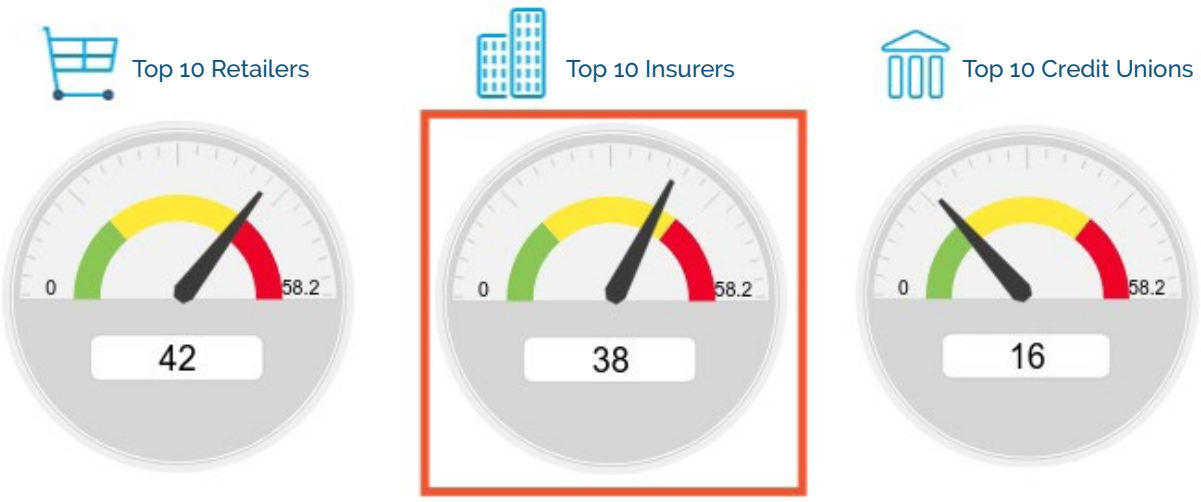
With the diversification in insurance product offerings (i.e pet, home, car, business insurance etc), each requiring their own sub domains and web applications to meet the different needs of customers, means the attack surface has massively increased. Ensuring intellectual property and sensitive customer data are properly secured everywhere against threat actors are becoming harder than ever with technology sprawl and the lack of asset visibility.

APPLICATION SECURITY CHALLENGE FOR INSURANCE COMPANIES

The industry must understand risk better than any other sector and after all, they are in the business of risk acceptance and creating hefty policies for their customers. Risk-averse enterprises across all markets transfer a portion of their cybersecurity risks to insurance companies to minimize damage in the event of a cyber-attack. With many insurers having actuaries in post to understand the liabilities associated with creating such policies for their customers, it's important to weigh up the cyberattack risk themselves.

Using our multi-layered attack surface technique, we found EU insurers to have the second largest attack surface with an average exposure score of 38.10 out of the maximum score of 58.24, compared to our previous studies for online retail (42.37) and credit unions (16.39). This is a worrying trend, as we all know the larger the attack surface, the more likely it is for threat actors to find holes in security defenses and execute potential exploits. With insurers holding millions of records of customer data (PII) and premiums (totaling $1.32 trillion in 2019) it's important to take stock of weaknesses in their application security.

Average Attack Surface Score

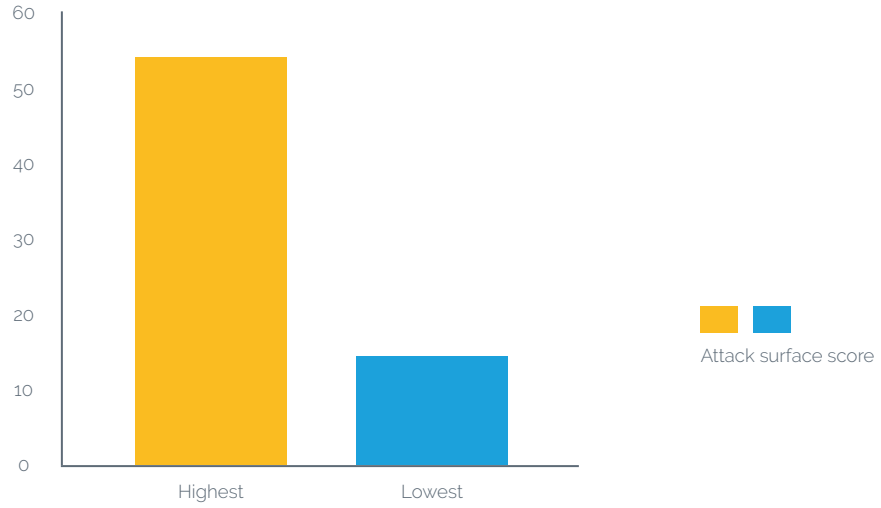


Web application security is a well-known issue facing security professionals worldwide due to the sheer volume of applications they own (the majority they don't even know exist). We found the top 10 insurance companies running almost 3x more applications (7,611) than the top 10 online retailers (2,799) we analyzed in 2020, providing a breeding ground for vulnerabilities with the greatest number of applications and domains exposed to the Internet.

Moreover, 2.98% of these insurance applications are considered suspects (e.g. Test environments that shouldn't be there) and 22.51% of them are found to be running on old components containing known vulnerabilities that could leave them open to attacks. The figure is on par with retailers but significantly higher compared to the Credit Unions who appear to have a higher level of cyber hygiene when it comes to updating outdated components.

The most disturbing finding, perhaps, is the high attack surface score at 53.87 and 51.22 (out of 58.24) respectively from two of the Top 10 EU insurance companies studied. Given the recent high profile ransomware attacks insurers must look very closely at the risks posed from their digital footprint and exercise more caution when launching new applications into the market.

Top 10 Insurance - highest vs lowest web app attack surface score



Overall, the study shows insurers aren't embracing DevSecOps and application security hygiene enough due to the large number of applications exposed and old components being used. As digital transformation takes hold and businesses release more apps at increased speed and scale – will we see this risk increase and open more doors for hackers if in-depth security risk analysis is ignored?

TOP ATTACK VECTORS AFFECTING INSURANCE APPLICATIONS

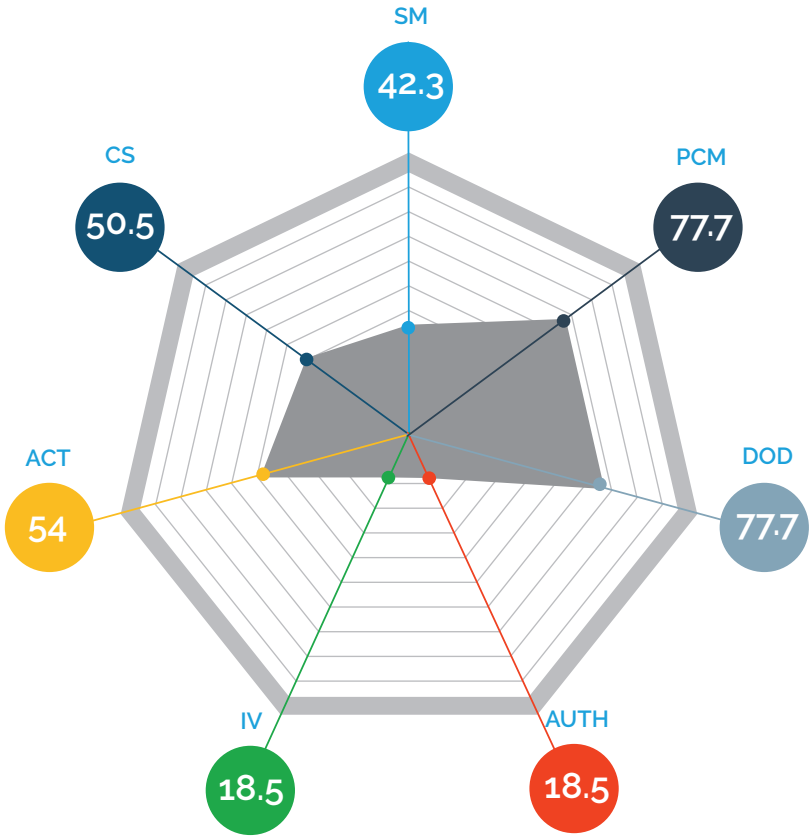
Our web application threat assessment tool is the only solution to provide continuous visibility of your attack surface and provides a risk scorecard to pinpoint potential security flaws in your application ecosystem. To do that we evaluated the public facing applications discovered against the seven most common attack vectors to quantify your attack surface.

1. **Security mechanism (SM)**
2. **Page creation method (PCM)**
3. **Degree of distribution (DOD)**
4. **Authentication (AUTH)**
5. **Input vectors (IV)**
6. **Active contents (ACT)**
7. **Cookies (CS)**

These seven vectors are common playbooks used by hackers during reconnaissance - looking at the makeup of an application for holes and checking the digital footprint of a company to find a vulnerable opening that they could launch malware or gain unauthorized access without you knowing. Hackers aren't fussy how and where they get in and will often look for the easiest entry points to get to your sensitive data. All seven attack vectors pose a threat if managed incorrectly and it only takes one backdoor access to give a hacker a foothold into your system.

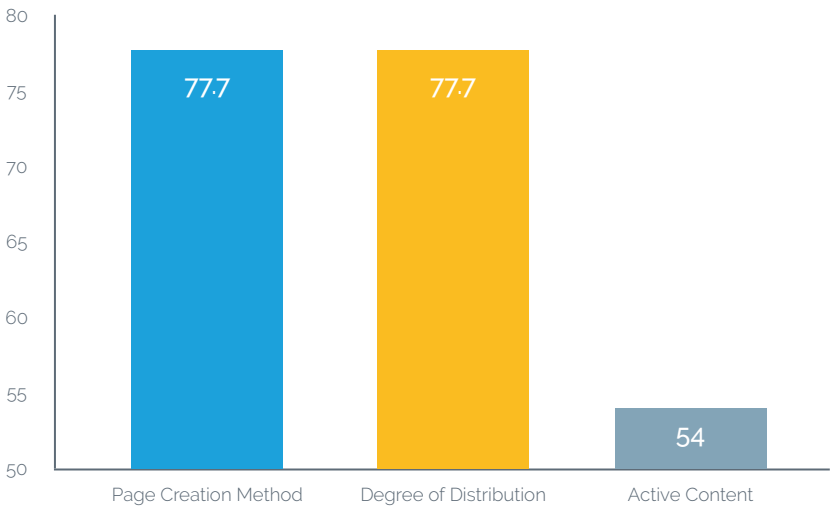
In this attack surface spider map for the top EU insurers, you can see the average weightings of the common attack vectors and easily understand where they are weakest, helping insurance security teams to visualize the potential threats that may arise as a result of poor application security hygiene and understand where further assessment is needed to strengthen controls.

Top 10 EU Insurance Attack Surface Spider Map



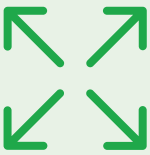
From our analysis of the insurance companies, page creation method (PCM) and degree of distribution (DOD) came out on top with an average risk score of >77, followed by active contents (ACT) at 54 as the top 3 attack vectors that are most exposed.

Top 3 Attack Vectors for Top 10 Insurance organizations



1. Page creation method (PCM)

Our tool found page creation method as the joint biggest attack surface exposure scorer amongst the 7 attack vectors. By scanning the public facing insurance domains we were able to identify application pages which have been developed using potentially insecure code which could carry potential vulnerabilities for exploitation. It's important security professionals and developers work together to locate application weakness like this during the DevOps cycle. With 70% of the top ten scoring 100/100 for this attack vector we recommend taking immediate action by running SAST/SCA during development and conducting continuous pen testing or DAST in production to rectify this as quickly as possible.



2. Degree of distribution (DOD)

This isn't a surprise to see, as many business-to-consumer applications like those offering a range of different insurance products will have a higher risk exposure score for degree of distribution. Insurance apps are likely to have many pages due to the volume of products and policies on offer. However, this directly increases the attack surface as the more pages there are, the harder it is to keep on top of the security hygiene of every single page on every domain. Not to mention the numerous input vectors and fields that could be used on each page and how they are linked internally and externally to your infrastructure, giving bad actors a plethora of opportunities to identify potential backdoor access and vulnerabilities to infiltrate your systems.

3. Active content (ACT)

In third place, we have seen more websites with a high active contents risk score, with 90% of insurance applications scoring >50 for this attack vector. The use of Javascript and ActiveX controls are common in modern application development as businesses look to create a more dynamic and real time experience for the end user by pulling in different information or data sources. It's easy for hackers to find out if your apps have been developed using vulnerable and outdated active content technologies. Although modern technologies like this are great in providing a better customer experience, however it poses a higher risk (and a larger attack surface) to the web application so regular and continuous application scanning should be a top priority to prevent script-based attacks.

OTHER COMMON SECURITY EXPOSURE

Cookies benefit both the customer experience and create added verification for businesses. They are essential for real time application security by monitoring session activity and ensuring anyone who sends requests to your website are allowed access and keep hackers away from unauthorized areas. Without cookies it can allow hackers to extract information from encrypted web connections and can be manipulated to spread across different domains and subdomains. It may sound simple, but our research revealed the insurance companies have scored an average of 50 out of 100 for this attack vector, meaning they need be more cautious and understand this could lead to basic SSL, cookie consent and privacy policy defects.

Top 10 Insurance

Average score for cookies attack vector if left unresolved could lead to extraction of data by hackers

In addition, we also found 22.51% of insurers using old components such as jQuery in their applications. That's an average of 143 outdated components in use per insurance company! The impact of this is a serious one as most of these components contain known vulnerabilities that could lead to SQL injection, Cross-Site Scripting and security misconfiguration exploits. Take the notorious Mossack Fonesca (Panama Papers) breach in 2016, which was caused by a vulnerability in an old, unpatched version of Drupal. Using old components carrying known vulnerabilities contributed to some of the largest breaches to date from older software including vBulletin and Forumrunner. Depending on the assets you are protecting, perhaps this risk should go to the top of the list.

Average # of old components used which can carry vulnerabilities if software is unpatched and can lead to increased risk of data breach

Outpost24

MEETING THE INSURANCE SECURITY CHALLENGE

Our research shows the complexity of modern-day insurance applications and how the total addressable attack surface can help security teams better understand the problem areas and focus on where they're most at risk for prioritizing remediation and security controls to prevent data breach.

Best practice for securing your web applications

The dynamic nature of insurance applications means application security discovery and assessment must be continuous. Outpost24's **Application Security Program (ASP)** is designed to help companies take a proactive view of their internet facing applications with a risk-based approach through continuous Discovery, Scoring, Alignment, Onboarding & Assessment and Reporting for successful integration with their application development workflow to fit your business needs and risk criticality levels.

- **Discovery.** Helping organizations to understand what applications they own that are visible to threat actors.
- **Scoring.** Provide an attack surface score for each of the discovered applications.
- **Alignment.** Working with the customer to align each discovered application against their business criticality and application development lifecycle and then provide recommendations on which of our full stack assessment solutions should be used to help reduce a specific application's attack surface.
- **Onboarding.** Collaboration between the Managed Service team and the organization to systematically onboard applications into the relevant solutions and tools agreed in the previous step.
- **Assessment.** Assess each application, either as a one-off activity, or on a continuous basis.
- **Reporting.** For each in scope application create detailed reports and analysis guiding organizations on the steps and activities they need to take to reduce their attack surface.
- **CMDB.** The creation of an organizations specific 'CMDB' or application repository, gathering the pertinent information for each in scope application such as, but not limited to, owner, business criticality, location, purpose etc. Along with the attack surface score and other information gathered during the discovery, scoring and assessment phases of the program.

This bespoke **Application Security Program (ASP)** best practice process will help organizations create an application repository CMDB, ensuring complete visibility of your entire digital facing ecosystem and long-term application security hygiene. It's a constant game of cat and mouse and in the fight against evolving cyber threats used by opportunistic hackers, insurers can use the data and intelligence to better understand how the makeup of their applications are directly related to their overall attack surface and building more secure apps and reducing their attack surface exposure over time.

Benchmark Your Attack Surface Now

Methodology for Web Application Discovery and Attack Surface Analysis

We help insurers locate suspected applications based on the common seven web attack vectors and providing a risk exposure score to guide their remediation effort. Outpost24 Scout, a web application discovery and attack surface assessment tool, uses the following set of processes and techniques to simulate a web application reconnaissance just like a hacker would do. Starting with information gathering to discover the potential weakness and entry points.

The 7 Steps during RECONNAISSANCE

R1: Gather information
R2: Determine the range (domain)
R3: Identify active web applications
R4: Discover open doors and entry points (7 vectors)
R5: Fingerprint the web app (score)
R6: Uncover components behind those doors (components detection)
R7: Map the apps (crawl)

Outpost24 uses multiple discovery techniques to assess a Web Application against the seven (7) vectors by crawling publicly available domains and application components to determine the attack surface with a spider chart and risk rating (1 to 58.24).

- **V1:** Security Mechanisms (SM) - How the traffic between users and the application is secured i.e is there authentication in place?
- **V2:** Page Creation Method (PCM) - This depends on the code the web app has been developed in. Developing websites with insecure code or outdated versions increase the risks of potential vulnerabilities
- **V3:** Degree of Distribution (DOD) - The more pages you have, the more risks there are, all pages must be identified, and vulnerabilities uncovered at all levels
- **V4:** Authentication (AUTH) - It is the process of verifying the identity of an individual accessing your application. Access to certain actions or pages can be restricted using user levels set up by the administrator and critical to keeping the bad guys out.
- **V5:** Input Vectors (IV) - The attack surface increases with the number of different input fields you have on a web application which can lead to a range of XSS attacks.
- **V6:** Active Content (ACT) - When an application runs scripts the content becomes active, and depending on the way those scripts have been implemented, the attack surface could increase if a website has been developed using several active content technologies.
- **V7:** Cookies (CS) - Cookies are essential for real time application security, by monitoring session activity and ensuring anyone who sends requests to your website are allowed access and keep hackers away from unauthorized areas.

The attack surface is an indication of the risk level. For example, we may have identified an application with missing SSL encryption (active application on port 80 rather than the more secure 443 port). The scan can also detect whether the application is running on outdated components which hasn't been hardened and poses a potential threat. The tool simply provides a spotlight on the areas that could lead to potential vulnerabilities and exposure (not a full vulnerability assessment report), helping security leaders prioritize what's most urgent for further investigation, whether it's through pen testing or application security scanning. More information can be found here.

Top 10 EU insurance companies analyzed:

1. Allianz Group
2. AXA SA
3. Legal and General
4. Assicurazioni Generali
5. Aviva plc
6. CNP Assurances
7. Aegon
8. Prudential
9. Zurich Insurance Group
10. Munich Re

This insurance attack surface analysis was conducted between May to June 2021 using our Attack Surface Discovery tool - Scout and is based on the Top insurance companies in Europe (EU) listed by ADV Rating 2021.

All information collected or assets scanned are available from the public domain. At no point unauthorized access was used. All data is presented in an aggregated manner to ensure individual insurance performance and scoring remain anonymous. If any of the named insurers would like to request a full disclosure of our findings in this research please contact info@outpost24.com

ABOUT US AND CONCLUSION

Data breaches are rising, and the number of successful cyber-attacks targeting businesses has jumped from an already staggering 38% to 43% and costing upwards of $300,00 or more to fix – a worrying trend which if ignored could be catastrophic for any business. This exponential growth in attacks poses a new challenge to the insurance sector, especially following recent hits on the big names. Security teams are now looking to up their cyber security spending and finding innovative ways to curb this threat from ransomware and malware attacks. With cyber security becoming more and more complex and with a potential attack creating huge damage and potentially sinking a business, it's essential for insurance organizations to discover and create inventories for all public facing applications. Continuously testing them for vulnerabilities, which could be exploited by a hacker looking for an opportunity to exfiltrate the personal identifiable information (PII) of your customers and policy holders.

The insurance sector must stand up and take notice of these new and evolving digital threats especially as they look to speed up digital transformation projects to remain competitive and support growth. By utilizing our Scout attack surface discovery tool insurers have an in-depth view into how their applications score against the common web app attack vectors to build a security blueprint for potential risks – providing vital intelligence to better understand the makeup of your applications and how to focus your efforts to fix the most deadly with the correct security controls. Freeing up valuable time and resources for overstretched security teams to focus on more important matters including supporting growth projects and boosting security awareness for their global workforce.

Request your web application attack surface score

Outpost24 Europe Headquarters
Outpost24 Europe Headquarters
Blekingegatan 1
37157 Karlskrona
Phone: +46 455 612 300
info@outpost24.com

Outpost24 US Headquarters
35 S. Washington St. Suite 308
Naperville IL 60540
Phone: +1 (630) 352 2283
info@outpost24.com

Outpost24