breachlock

2024

BreachLock Penetration Testing Intelligence Report

Table of Contents

FOREWORD

Seemant Sehgal
Founder & CEO, BreachLock

A New Frontier That Leaves More Questions Than Answers

Today more than ever, Chief Information Security Officers (CISOs) face increasing cyber security challenges. As cyber security rushes into a new frontier, CISOs are facing the rise of generative AI, new incident reporting rules by the U.S. Security and Exchange Commission (SEC), and the EU's NIS2. As these changes seek to hold enterprises more accountable, it leaves CISOs and practitioners unsure of what lies ahead. They seem to be facing more questions and none more so than: ***"How do I modernize cybersecurity while meeting the board's risk appetite?"***

CISOs and leadership teams are under more scrutiny to continuously reassess risks by identifying threats and vulnerabilities and quantifying the potential impact financially. They need to provide business-oriented programs that drive ROI and reduce risk.

Having worked directly with multiple CISOs and experience at top enterprises, I've observed a significant disparity in resource allocation between defensive and offensive security. Upon scrutinizing the ROI, it was evident that offensive security consistently yielded superior outcomes. Offensive solutions like penetration testing proactively identify vulnerabilities and mitigate risk to prevent exploits, thus demonstrating a clear ROI. However, companies invest less in penetration testing despite its benefits.

At BreachLock, we have dedicated years to addressing the limitations of traditional pentesting to enhance accuracy, agility, scalability, and cost-effectiveness, overcoming the shortcomings of conventional methods.

The 2024 BreachLock Penetration Testing Intelligence Report aims to demonstrate how full-stack penetration testing can enhance offensive security and provide continuous protection. We emphasize the need to continuously test assets, using frameworks like OWASP and MITRE ATT&CK to equip security teams with the latest threat data.

Cybersecurity is a team sport. This year's report is a testament to our commitment to help the CISO community learn from each other, share knowledge, and improve our cyber threat resilience using a data centric and fact-based approach.

Seemant Sehgal

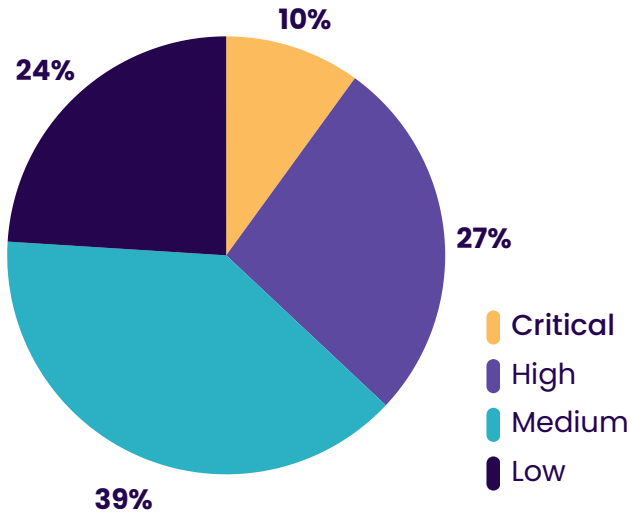
HIGHLIGHTS

In our 2024 report, BreachLock analyzed anonymized threat intelligence from over 4,000 global penetration tests conducted over the past 12 months. We examined affected assets, associated vulnerability types, prevalence, severity, and the most impacted industries.

We also considered enterprises by employee size and geography to determine if there were influencers related to vulnerability prevalence and impact.

This year we chose to include **MITRE ATT&CK** adversary tactics and techniques to see how our real-world observations and data compared, as ATT&CK threat models and methodologies are a big component of the BreachLock framework. We also examined BreachLock threat intelligence and exploits compared to **OWASP Top 10** categories by asset-specific vulnerabilities across the Top 5 most impacted industries.

Overall Risk Severity of Vulnerabilities



TOP 5 IMPACTED INDUSTRIES

1. Computer Software & Technology
2. Professional Services
3. Banking & Financial Services
4. Healthcare
5. Retail & eCommerce

TOP 5 OVERALL SECURITY ISSUES WEB APPLICATIONS

1. Cross-Site Scripting (XSS)
2. Outdated Software Versions
3. Insecure Direct Object References (IDOR)
4. Lack of Security Headers
5. Insecure Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Protocols

TOP 3 Critical Severity Findings

1. SQL Injection
2. Broken Authentication
3. Remote Code Execution (RCE)

TOP 3 High Severity Findings

1. Cross-Site Scripting (XSS)
2. CSV Injection
3. Cross-Site Request Forgery (CSRF)

INTRODUCTION

Welcome to the BreachLock Penetration Testing Intelligence Report for 2024.

This year's report is larger, including the analysis of 4,000 penetration tests and vulnerability assessments, which is 1,000 more tests compared to last year. This means more tests covering a wider range of assets and geographies. In 2024, we saw some of the same reported vulnerabilities, and a few new ones, affecting different industries than in the past, specifically in the technology and healthcare sectors.

As Penetration Testing as a Service (PTaaS) becomes one of the pinnacles of Offensive Security, organizations are turning to pentesting more than ever to provide the data needed to align both security and business objectives. Just in the past few years, we've seen penetration testing become a driving force for enterprises who want to implement more proactive security measures.

The results presented in this report can help security professionals understand how penetration testing, alongside other offensive security solutions, can excel their vulnerability identification and remediation efforts, and fill gaps and weaknesses to better secure the ever-changing attack surface before a breach occurs.

We understand that today's security professionals and DevOps teams have increased responsibilities, and must do more with less, all while keeping their attack surface secure. Like many who lack resources or skills, BreachLock will partner with you to conduct expert-driven pentesting effectively across your security ecosystem. We offer both human-driven and on-demand continuous penetration testing, providing a hybrid approach and the flexibility, scalability, and speed to test what you want, when you want.

METHODOLOGY & SCOPE

Despite a more sophisticated threat landscape, stringent compliance requirements, and escalating geopolitical tensions, a report by ISACA indicates that 41% of organizations find cybersecurity becoming easier to manage compared to previous years while 46% find it more difficult.

With tools and platforms that enable better collaboration and the ability to identify and mitigate threats faster, every pentesting engagement can offer visibility and in-depth context into attackers methods and the potential impact.

This report is comprised of data collected from over 4,000 penetration tests conducted over a 12-month period between June 2023 and June 2024. These tests covered a wide range of assets including web applications, networks, APIs, mobile applications, IoT devices, and cloud environments.

The data has been anonymized and aggregated for comprehensive analysis by our pentesting researchers.

Our methodology involves a hybrid approach with a combination of BreachLock proprietary scanning technology and manual pentesting. Data points include vulnerability types, severity levels, affected assets, and industry-specific insights.

BreachLock has been performing continuous security testing for years, conducting tens of thousands of penetration tests. Our extensive experience has provided us with deep knowledge of potential attack paths and TTPs for various technology stacks. Adhering to standards such as MITRE ATT&CK, OWASP, NIST, CIS benchmarks, and OSSTMM, our automated algorithms and NLP-supervised AI models enhance our proprietary pentesting framework so that our pentesters can focus on identifying complex security flaws, ensuring a maximum ROI.

REPORT SCOPE

12-Month Timeframe

4000+ PENTESTS Performed Globally

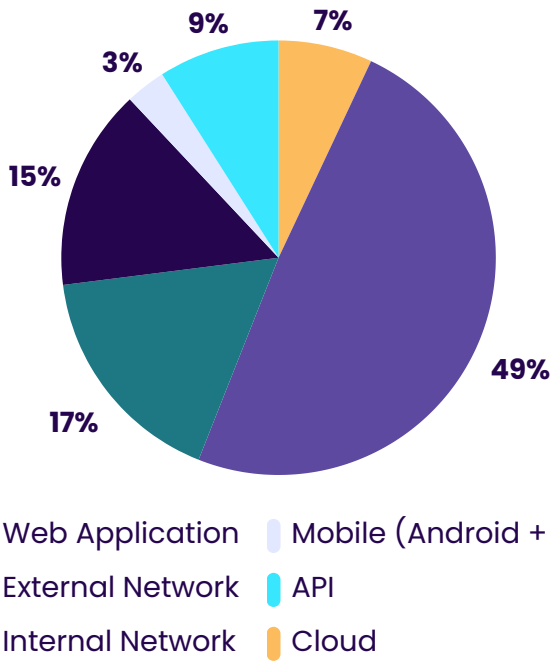
Assets Included

- Web Applications
- APIs
- Mobile Applications
- Cloud Environments
- Internal Networks
- External Networks
- IoT Devices

Industries Covered

- Financial Services
- Education
- Healthcare
- IT & Prof. Services
- Manufacturing
- Media Services
- Public Sector
- Retail & eCommerce
- Telecommunications

Assets Tested from 2023-2024



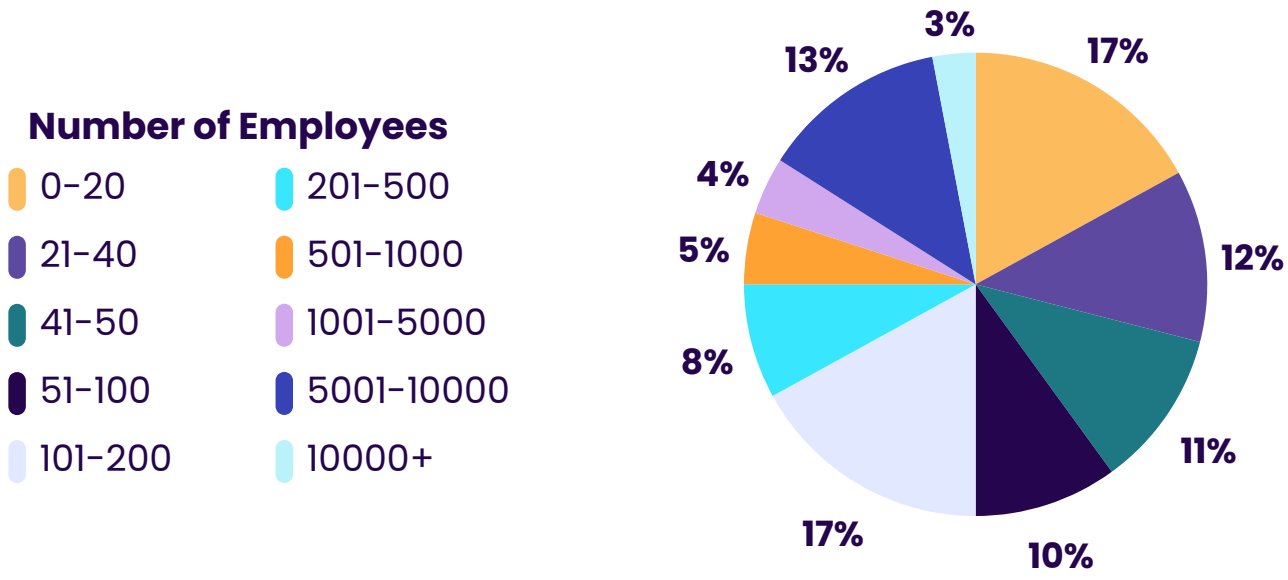
DEMOGRAPHICS

In analyzing enterprise segments for a pentesting report, it's crucial to identify and evaluate the distinct areas within the organization that are most susceptible to cyber threats.

Small Enterprise: 1 to 50 employees represent 40% of pentesting analysis
Mid-size Enterprise: 51 to 1000 employees represent 35%
Large Enterprise: 1001 to 10000 employees represent 25%

In the past 12 months, we have seen an increased interest by large enterprises to conduct penetration testing as part of their offensive security strategy. Large enterprises typically have vast and intricate IT infrastructures, including numerous applications, networks, and systems. Continuous security testing can automate the pentesting process and handle this scale more effiiciently, ensuring comprehensive coverage. This positive trend indicates an understanding that continuous security testing allows enteprises to identify and address vulnerabilities in real-time, perform tests much faster, and enable more frequent assessments, which is crucial when changes in IT environments occur regularly.

Enterprise Demographics



ALIGNING WITH OWASP TOP 10

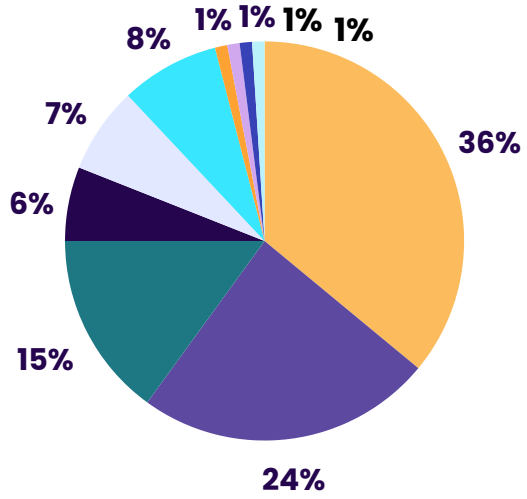
The OWASP Top 10 is globally recognized by developers as the first steps towards more secure coding. It represents a broad consensus about the most critical security risks to web applications. The OWASP Top 10 list is a great starting point to identify the most common risks in not only web applications, but APIs, cloud, and more covering the most common attacks. Many other risks are not covered, and this is where the OWASP ASVS comes in. The OWASP ASVS is a much more comprehensive awareness document covering many aspects of application security, including dangerous vulnerabilities. We will only be referring to OWASP Top 10 in this section.

The Top 5 most identified vulnerabilities by OWASP align with BreachLock's top 5 findings as follows:

1. A05:2021 - Security Misconfigurations
2. A02:2021 - Cryptographic Failures
3. A01:2021 - Broken Access Control
4. A04:2021 - Insecure Design Injection
5. A06:2021 - Vulnerable and Outdated Components

These Top 5 categories aggregated together represent 88% of the findings and security weaknesses in the report's full data set.

Findings Categorized with OWASP Top 10



- Security Misconfiguration
- Cryptographic Failures
- Broken Access Control
- Insecure Design
- Vulnerable and Outdated Components
- Injection
- Identification and Authentication Failures
- Server-Side Request Forgery (SSRF)
- Security Logging and Monitoring Failures
- Software and Data Integrity Failures

OBSERVATIONS

OWASP 2021 Top 5 Ranking	BreachLock Observed Top 5 Ranking
A01:2021 - Broken Access Control	Security Misconfigurations (36%)
A02:2021 - Cryptographic Failures	Cryptographic Failures (24%)
A03:2021 - Injection	Broken Access Control (15%)
A04:2021 - Insecure Design	Insecure Design (6%)
A05:2021 - Security Misconfigurations	Injection (8%)

MITRE ATT&CK® TECHNIQUES

MITRE ATT&CK is a global knowledge base of adversary tactics and techniques based on real-world observations. BreachLock uses the latest ATT&CK data in its NLP-based algorithms and AI models to update and enhance our pentesting methodologies. This allows certified pentesters to define multiple attack paths and provide a comprehensive overview of potential exploitation routes for critical vulnerabilities.

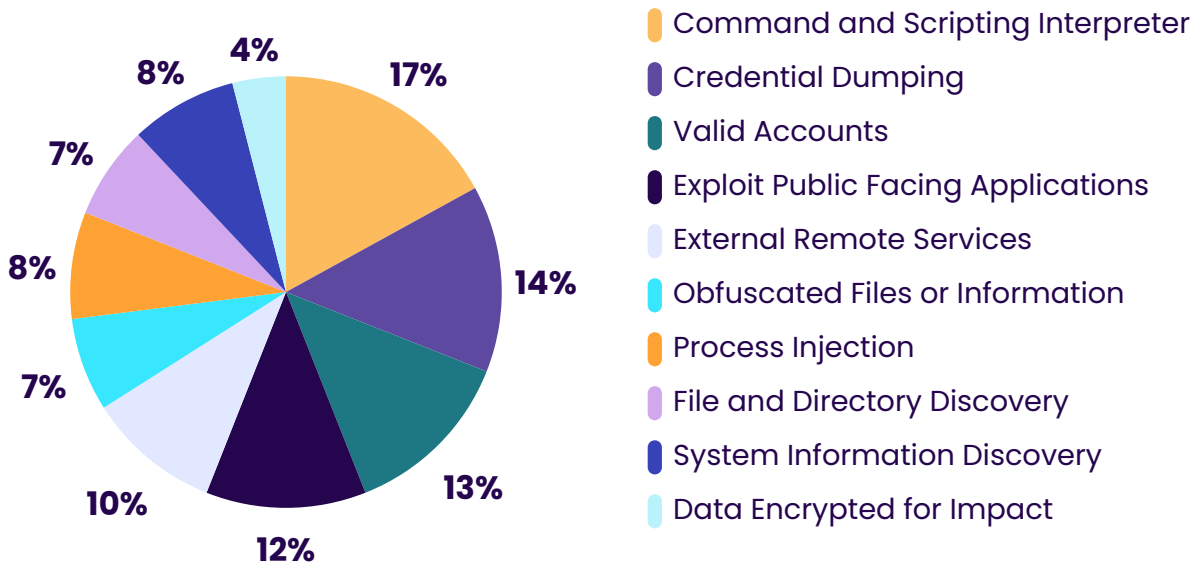
Alignment with ATT&CK Data

Below are ten of the most commonly exploited MITRE ATT&CK techniques discovered in our 2024 pentesting findings along with estimated prevalence by percentage.

MITRE ATT&CK Techniques	ID	Prevalence
Command and Scripting Interpreter	T1059	55%
Credential Dumping	T1003	46%
Valid Accounts	T1078	42%
Exploit Public Facing Applications	T1190	38%
External Remote Services	T1133	32%
Obfuscated Files or Information	T1027	22%
Process Injection	T1055	24%
File and Directory Discovery	T1083	22%
System Information Discovery	T1082	27%
Data Encrypted for Impact	T1486	12%

Top 10 MITTE ATT&CK Techniques

Aligning with MITRE ATT&CK techniques ensure that identified vulnerabilities correspond to real-world attack techniques, validating the relevance and severity of our threat findings. By identifying vulnerabilities associated with the most common and impactful attack techniques, organizations can prioritize their remediation efforts to address the most critical and probable threats first.



ASSETS

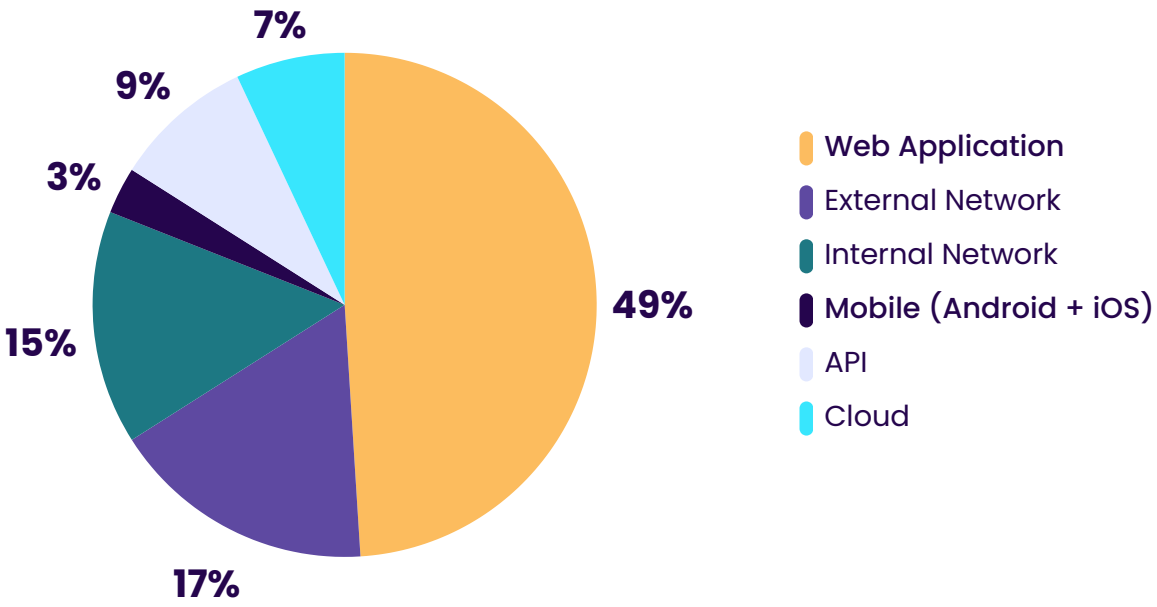
BreachLock has extensive experience and accumulated knowledge of potential attack paths, as well as Tactics, Techniques and Procedures (TTPs), tailoring our pentesting to diverse technology stacks and contexts.

We deliver penetration testing through our PTaaS Model, testing all assets in both the internal and external attack surface. Using our proprietary penetration testing framework, we are able to enhance the speed and scalability of continuous security testing across industries and geographies.

The asset types that resulted in the greatest number of findings are as follows:

1. Web Applications
2. External Network
3. Internal Network
4. APIs
5. Cloud
6. Mobile Applications (Android and iOS)

Assets Tested from 2023-2024



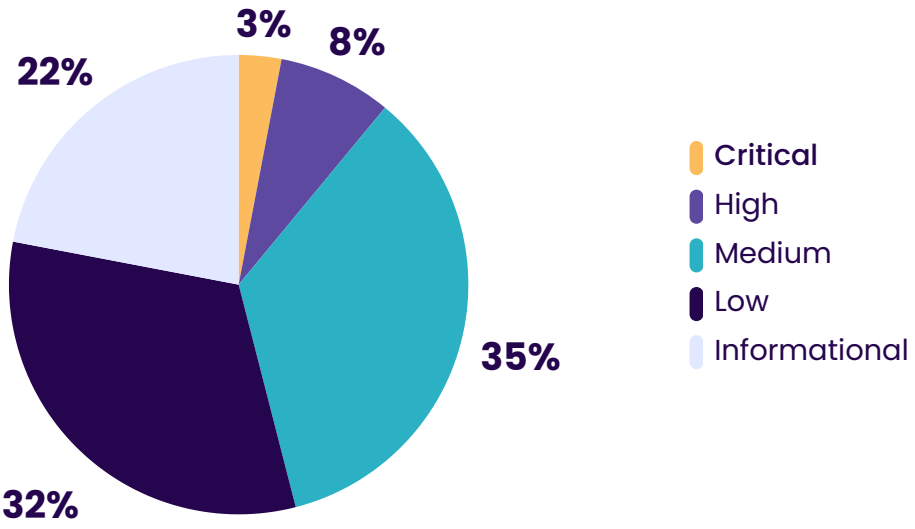
WEB APPLICATIONS

According to Gartner, web applications are critical to all aspects of the digital organization. The ubiquity of application delivery platforms and the fast pace of development contribute to the growing attack surface in 2024 for malicious actors.

Web applications are frequent targets by attackers, making their protection a crucial part of any comprehensive offensive security program. Organizations benefit from proactive security strategies that leverage automation and deployment capabilities to enhance application security.

Across industries, web applications constituted 49% of all assets tested in this report, highlighting the significant focus by customers in application pentesting. This underscores organizations' recognition of web applications as vulnerable areas that require prioritized security measures to mitigate risks. It also underscores the critical role of web application security in an organization's offensive security strategy.

Overall Risk Severities Web Applications

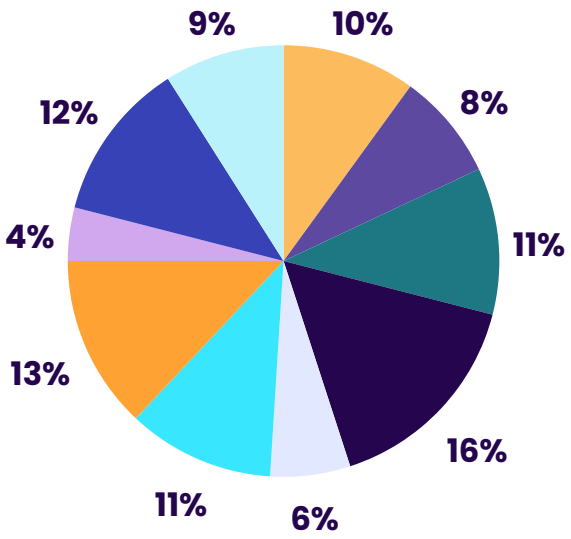


Risk Severity Analysis:

The data reveals the distribution of risk findings in web applications with Critical findings (3%) which is up 2% in 2024 or a 150% increase compared to 2023. This may be due to the addition of more checks and enhancement of automation and TTPs. High severity findings also increased from 5% to 8% or up 60% in 2024, with a over two-thirds of findings falling into Medium (35%), and Low (32%), respectively. Risks identified during pentesting that were classified as Medium severity means that a significant portion of the vulnerabilities are serious enough to warrant attention but may not be Critical. These Medium severity risks could potentially be exploited by attackers, leading to substantial negative consequences and should be addressed in a timely manner.

Top 10 Critical Vulnerabilities in Web Apps

The top 10 Critical vulnerabilities in web applications are listed below. Many align with the OWASP Top 10 and share common root causes. Input sanitization is crucial for preventing several vulnerabilities, particularly injection attacks. However, other measures such as proper access control, secure design practices, cryptographic integrity, and correct configuration are equally important.

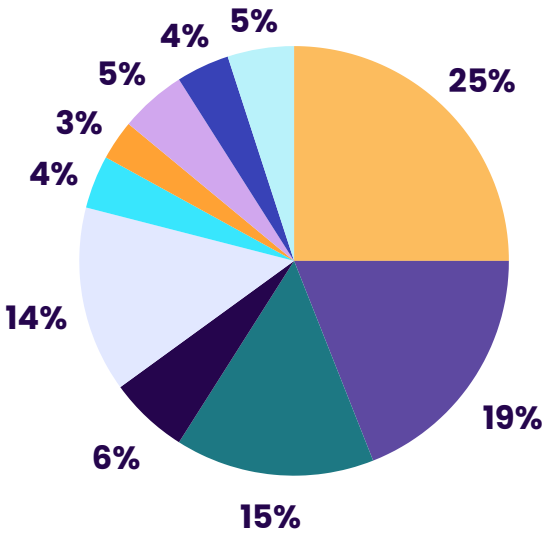


- Injection Attacks
- Missing Security Headers
- Arbitrary File Upload
- Function-Level Access Control Missing
- Concurrent Sessions
- Authentication Bypass
- Privilege Escalation
- Remote Code Execution
- Insecure SSL/TLS Cipher Suites
- Cross-Site Request Forgery (CSRF)

Top 10 High Vulnerabilities in Web Apps

The #1 vulnerability, Cross-Site Scripting (XSS), has decreased from 37% in 2023 to 25% in 2024. Other findings remain relatively unchanged in 2024 as well. XSS vulnerabilities remain prevalent due to the complexity of modern web applications and the use of client-side scripting like JavaScript. Remediation includes input validation, data encoding, implementing CSP and HTTPOnly, and other security measures.

- Cross-Site Scripting (XSS)
- Injection Attacks
- Web Application Vulnerable to Cross-Site Request Forgery (CSRF)
- Improper Session Handling
- Privilege Escalation
- Concurrent Sessions
- Insecure Direct Object References
- Functional Level Access Control Missing
- Sensitive Data Exposure
- Authentication Bypass



State of Web Applications Security

Millions of applications are developed each year and the demand for web applications continues to grow. The adoption of progressive web apps (PWAs) and the rise of microservices architecture contribute to this trend.

Industries consuming the most web apps and are most vulnerable include **Retail,** accounting for **37%** of global web application and API attacks.

The **transportation** sector follows closely with **19%** of attacks with other notable industries such as Software as a Service **(SaaS) (8%), Telecom (8%)**, and **Utility (4%)**.

Recent high-profile cyberattacks on web applications include those on UnitedHealth-owned Change Healthcare, Ascension Health System affecting emergency care, and CDK Global, which affected thousands of car dealerships.

OBSERVATIONS

In 2024, security teams as a whole continue to face mounting security challenges and web application security is no exception. Across industries injection attacks remains the foremost Critical severity in web applications since 2022, indicating a primary threat vector. As mentioned previously, Cross-Site Scripting emerged as the most prevalent High security vulnerability in 2024 constituting a staggering 25% of all such vulnerabilities. Arbitrary File Upload ranked as the 3rd most common Critical severity , account for 11% of these vulnerabilities. These correspond with our report findings and OWASP Top 10.

The overall threat landscape continues to expand and organizations still struggle with risk density and managing vulnerabilities effectively. Mean Time to Remediate (MTTR) Critical vulnerabilities take an average of 100 man-days for remediation. Prioritizing risks based on asset criticality remain crucial and regular patching and maintenanceis essential for defending against exploitable vulnerabilities.

RECOMMENDATIONS

Based on our data findings, organizations should consider the following remediation efforts and best practices for web applications:

- **Continuous Pentesting and Vulnerability Scanning:** Ensure your vulnerability scanning solution scans all internet-accessible domains, subdomain, and IP addresses associated with your organization. Maintain an asset inventory of these IPs to track scanning coverage to prioritize remediation based on vulnerability severity.

- **Static Application Security Testing (SAST) :** SAST is a white box pentesting method that analyzes source code to find security vulnerabilities that make applications susceptible to an attack. SAST takes place very early in the SDLC and helps DevOps teams identify vulnerabilities in the early stages of development so they are not passed to the appliation's final release.

- **Dynamic ApplicationSecurity Testing (DAST):** This is a black box pentesting method that identifies vulnerabilities based on various inputs that are sent. Responses are analyzed later in the SDLC after an application is deployed and running in a testing or production environment.

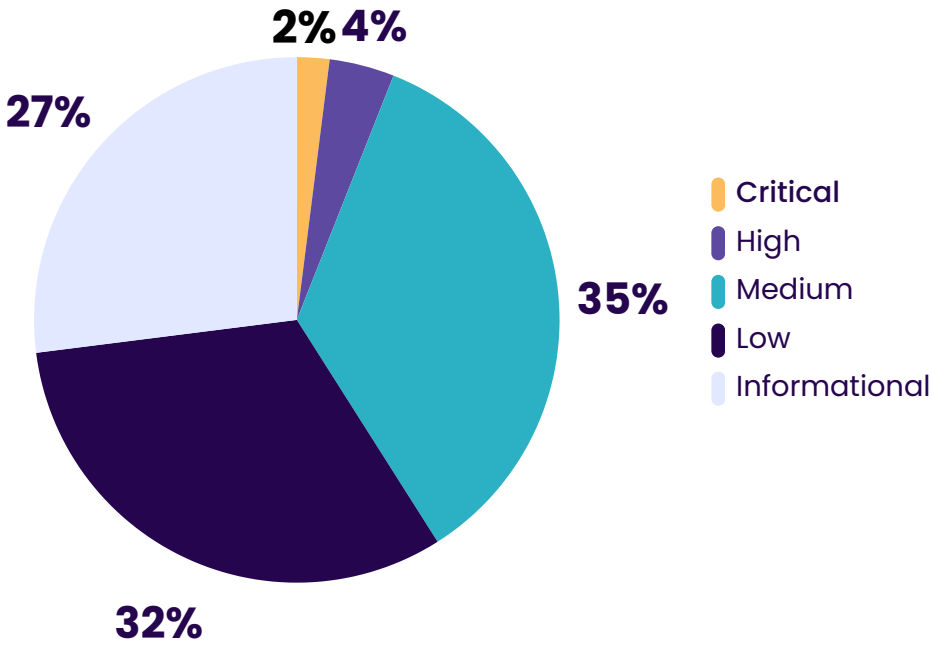
NETWORK INFRASTRUCTURE

Network security requires a multifaceted approach from investing in advanced security technologies and adhering to comprehensive and continuous assessments, to implementing a proactive offensive security strategy.

The proliferation of devices, applications, and users connected to networks, including IoT devices and remote workers, has expanded the attack surface, making it harder to secure all entry points. Cyber attackers are using sophisticated techniques, often remaining undetected for extended periods. New and previously unknown vulnerabilities (zero-day exploits) are continuously being discovered and pose signiicant risks before patches and defenses can be implemented.

Collectively, **network penetration testing represents 32% of the complete data set.**

Overall Risk Severities Network (External + Internal)

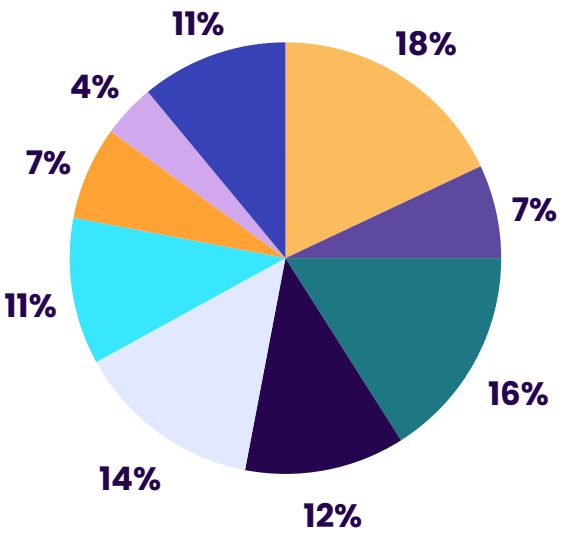


Risk Severity Analysis:

The risk distribution shows Critical (2%) and High (4%) findings. These findings have increased since 2023 at 100% and 200%, respectively. Medium (35%) findings have also increased in 2024 with Low (27%) decreasing from 2023. Overall we are seeing higher risk severity of Critical, High, and Medium network vulnerabilities across both internal and external network systems.

Top Critical Vulnerabilities in Networks

The top 3 Critical network vulnerabilities, Default Credential (18%), Remote Code Execution (7%), and Use of Expired SSL/TLS Certificates (16%) combined have increased exponentially in 2024 by a total of almost 20% vs. 2023. All three can facilitate unauthorized access to attackers resulting from easily guessed default credentials, and attackers executing malicious code via remote code execution to gain control over the system. Expired SSL/TLS certificats can lead to man-in-the-middle attacks, compromising the confidentiality and integrity of communications.

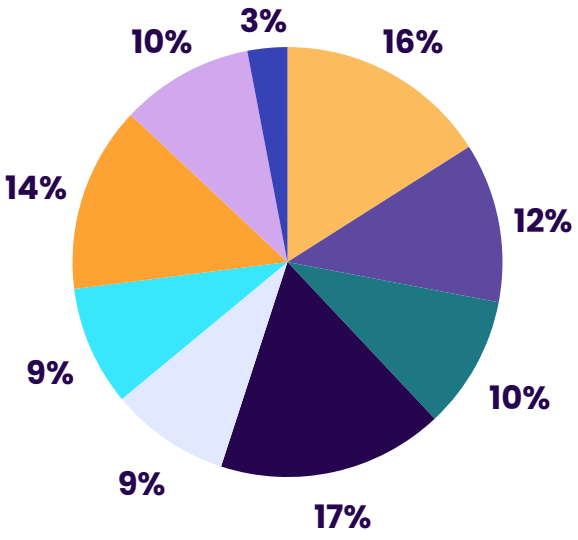


- Default Credentials
- Remote Code Execution
- Use of Expired SSL/TLS Certificate
- MS15-034 HTTP Protocol Stack Request Handling Denial-of-Service
- Server Supports Weak SSL/TLS Connections
- Authentication Bypass
- Web Service HTTP Header Remote Overflow
- Root Access Without Password
- Systems with Known Vulnerabilities

Top High Vulnerabilities in Networks

Weak passwords contributed 16% of all High vulnerabilities behind a similar vulnerability, default credentials, for both internal and external networks. This is surprising as these vulnerabilities did not even show in the Top 10 of last year's report. Unfortunately, this can be attributed to the such common factors as human error and convenience, lack of awareness by employees, system limitations, legacy systems, and inadequate enforcement by organizations who fail to have policies in place.

- Weak Passwords
- Inconsistent Forward and Reverse DNS Lookup Results
- DNS Server Cache Snooping Remote Information Disclosure
- Default Credentials
- FTP Anonymous Login
- OpenSSL 'ChangeCipherSpec' MiTM Potential Vulnerability
- SSL Certificate Signed Using Weak Hashing Algorithm
- Directory Listing
- NFS Share User Mountable



State of Network Security

Both internal and external networks are vulnerable to attacks due to several common factors such as:

- Modern networks are often complex with numerous interconnected devices and systems
- Misconfigurations and weak security practices like weak passwords and insufficient use of encryption
- Legacy systems may not receive updates or support
- Lack of effective proactive network assessments that can prevent timely detection and mitigation of attacks

The Top 3 industries most impacted by Network Attacks include:

Financial Services (30%): High value targets due to financial data and transactions

Healthcare (20%): Due to sensitive patient data

Retail (15%): Payment systems and customer data are key targets

OBSERVATIONS

Across industries approximately 26% of vulnerabilties are related to networks, emphasizing the need to secure network edge devices and security gateways. Ransomware, DDoS, malware, MitM attacks, SQL injection, and remote code execution are all attack vectors enabling bad actors to infiltrate and target network systems.

External networks are the first targets against cyber threats. Securing it against potential attacks is crucial to safeguard sensitive data and assets. External attackers continuously develop new techniques and exploit vulnerabilities to breach external networks.

Internal networks are just as susceptible to security breaches as external networks. Preventing unauthorized access and implementing stringent security protocols are critical to safeguard valuable information and assets from both insider threats and attacks.

Internal and external networks are highly vulnerable to cyber attacks today due to a combination of factors; the increasing complexity of network architectures, including numerous interconnected devices and systems, allows the attacker to possibly explore multiple attack paths with an increased probability of a successful exploit.

RECOMMENDATIONS

Based on our data findings, organizations should consider some of the following best practices to safeguard networks:

- **Continuous Network Security:** Continuous security testing of both your internal and external networks includes securing all servers and virtual machines, paying particular attention to cloud service administrative accounts.
- **Patch Management:** Ensure that all software, hardware, and network devices are regularly updated with the latest security patches and updates to protect agains known vulnerabilities.
- **Vendor Management:** Trusted third-party vendors are often seen as a potential risk. Vet them carefully to confirm their compliance with relevant regulatory requirements. Identify and inventory connected assets and run scans for any associated vulnerabilities that could affect your network, and ensure there is a security plan in place so that vendors meet your security standards.

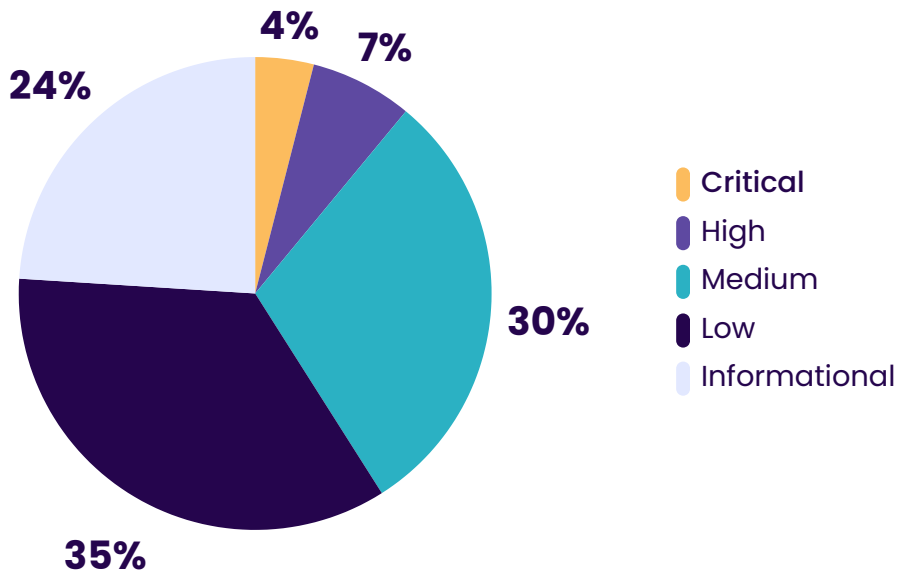
APIs

APIs are essential to furthering innovation and competition for organizations around the world. Consequently, APIs have become one of the leading targets for attackers to compromise systems based on the vast amount of sensitive data that is exchanged between APIs.

APIs are different than web applications and your standalone software programs. APIs serve as a set of rules and functions that allow different software systems to communicate with one another. Their function is to enable interaction between applications, services, or components. Whereas web applications are designed for user interaction, data management business logic, and integration, users can access web apps from any device with an internet connection. APIs simply return data. However, it is that data exchange that make APIs so susceptible to malicious actors if APIs are not secure when users request data to be retrieved or transferred.

APIs represent almost 10% of overall risk of all assets tested. That is substantial if 1 in every 10 pentesting finding represents a vulnerable API, of which 4% are of critical severity and 7% are high. If 1000 APIs are tested in a given period, 100 would represent a potential vulnerable API, and 40 could be Critical and 70 could be High.

Overall Risk Severities APIs



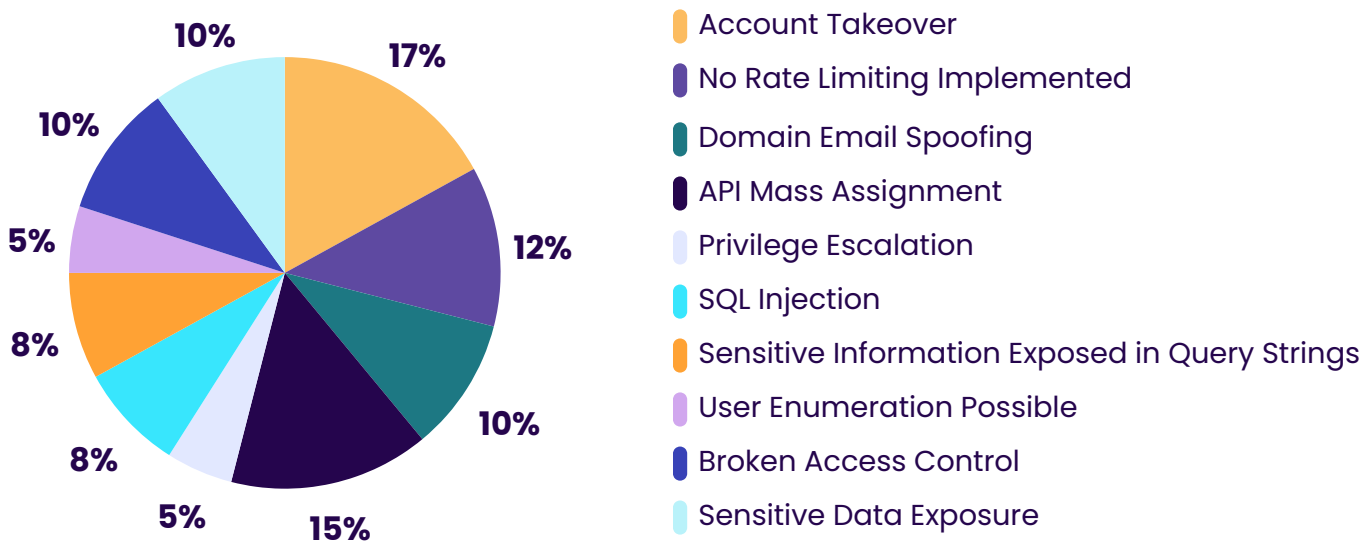
Risk Severity Analysis:

The risk distribution shows Critical(4%) vs. 1% in 2023, which is a 400% increase. High findings (7%) highlight the most significant shift increasing 700% vs. 2023. Medium (30%) findings have also increased in 2024 with Low (35%) slightly decreasing from 2023. Overall we are seeing higher risk severity of Critical, High, and Medium API vulnerabilities.

Top Critical and High Vulnerabilities in APIs

The #1 Critical API vulnerability is **account takeover representing 17%** of all API vulnerabilities in the 2024 report. This is notable as it is a vulnerability that can be easily mitigated. Many APIs suffer from inadequate authentication and authorization methods allowing attackers to exploit poorly implemented security controls leading to access to user accounts.

In comparison to 2023, "**no rate limiting implemented**" was not even represented in the Top 10 criticalities. In 2024 it represents the 2nd highest Critical vulnerability **(12%)** due to the increased reliance on APIs for various applications and services. This amplifies the potential lack of awareness by many developers who may not fully understand the importance of rate limiting or prioritizing functionality over security, leading to its omission in API design.



Lastly, domain **email spoofing ranked as the 3rd highest API vulnerability (10%)** which comes as no surprise. Because many APIs rely on email communication for user authentication or notifications, if not properly secured attackers can spoof domain emails to trick users into disclosing sensitive information or clicking on malicious links. In addition, APIs that do not implement strong email validation and verification processes remain vulnerable to spoofing. Attackers will exploit these weaknesses to send fraudulent emails that appear to come from legitimate sources to deceive recipients into taking action that compromise security.

Account takeover being the highest vulnerability finding underscores the importance of API authentication methods in API development. These mechanisms verify the identity of users or applications accessing APIs, ensuring only authorized parties can interact with them and their resources. Authentication is crucial for preventing unauthorized access and protecting sensitive data.

API authentication methods may include:

API Keys: Unique tokens used by developers or applications to access an API, included in requests as headers or query parameters, which the server validates for authorization.

Basic Authentication: This involves sending credentials using secure connections (HTTPS) alongside the base64-encoded format.

OAuth: An authorization framework that lets third-party applications access resources on behalf of a user without revealing the user's credentials.

OBSERVATIONS

For years, APIs operated behind the scenes, serving as the invisible link that enabled communication between software applications. Historically, they were the unsung heroes of technology—crucial yet largely unrecognized. However, that has changed dramatically. APIs have surged in prominence, becoming central to driving innovation and competition across global organizations. As their visibility has grown, so too has their appeal to cybercriminals, drawn by the vast amounts of sensitive data exchanged through them.

With the advent of cloud computing, microservices, mobile technologies, and the Internet of Things (IoT), APIs have become indispensable. This increased reliance underscores the need for stringent security measures, including robust authentication, effective detection, meticulous input validation, rate limiting to avoid service disruptions, and the use of API gateways and security solutions.

Ongoing API discovery and continuous security testing, including penetration testing, are essential for uncovering vulnerabilities and implementing proactive security measures against emerging threats.

RECOMMENDATIONS

Depending upon whether the API is in development or already deployed in use, there are several recommendations to keep your APIs secure.

- **Penetration Testing as a Service (PTaaS):** PTaaS will test the running API with malicious inputs to identify vulnerabilities by simulating attacks, including testing RESTful APIs.
- **Manual Pentesting:** Human-driven experts can conduct manual penetration testing to help identify vulnerabilities left undetected by automation.
- **Static Application Security Testing (SAST):** SAST provides static code analysis to identify vulnerabilities in the source code of APIs.
- **Fuzz Testing for APIs or Fuzzing:** A software testing technique used to discover vulnerabilities in APIs. Pentesting is a fuzz testing method used to discover unexpected behaviors and vulnerabilities by sending malformed or random data to the target system.

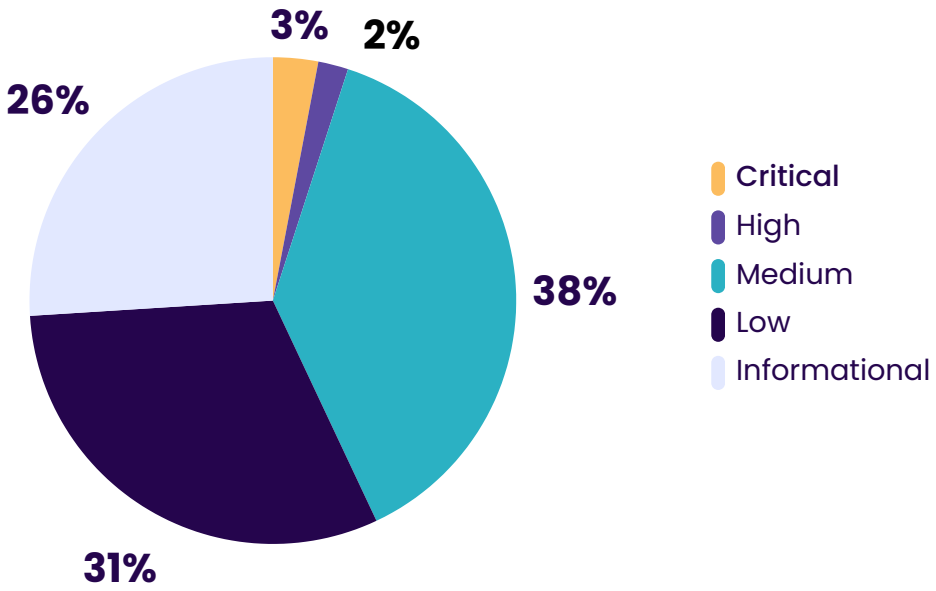
MOBILE

Mobile applications play a pivotal role in the modern enterprise allowing businesses to engage directly with their customers, providing a convenient platform for users to access services, make purchases, and interact with the brand.

Mobile apps extend an organization's reach beyond traditional channels. Today, Forbes estimates that approximately **62%** of businesses already use mobile apps or are in the process of developing one. Among these businesses, **50%** use their apps for support and engagement, **30%** for revenue generation**,** and **20%** for branding**.** Additionally, a recent techjury survey revealed that **64%** of working adults use their personal smartphones for business-related purposes. With over **3.8 billion smartphone users worldwide**, the use of mobile apps, and the security of the sensitive data that is exchanged, exponentially increases the attack surface.

Mobile applications(Android and iOS) represent almost 3% of overall risk of all assets tested in the data set.

Overall Risk Severities Mobile (Android + iOS)



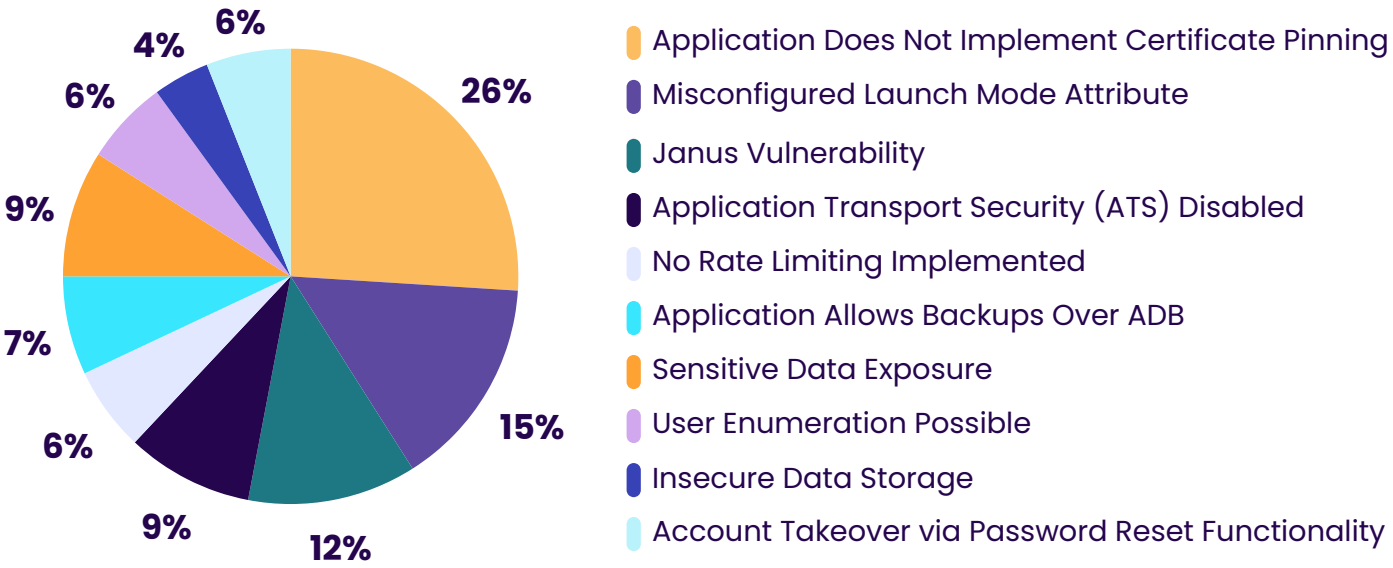
Risk Severity Analysis:

The 2024 report data reveals distribution of risk findings in both Android and iOS mobile applications with Critical Findings at 3%, which is a 300% increase from 2023 findings, High (2%) increasing from 2023, Medium findings decreased to 38% vs. over 50% in 2023, followed by Low (31%) severity findings.

Top 10 Vulnerabilities Mobile Applications

There was virtually no difference in our mobile findings in 2024 in comparison to 2023, with the Top 5 vulnerability types actually decreasing slightly in our 2024 report data. The new entry to the Top 10 is "**Account takeover via password reset functionality**" accounting for 4% of the mobile vulnerabilities. It is remarkable that this vulnerability was not in the Top 10 in 2023 and is no surprise that it appears in 2024 and isn't more prevalent.

This vulnerability has gained more visibility due to a combination of evolving threat landscapes, changes in user behavior, and advancements in attack techniques. Earlier, security professionals may have focused more on other significant vulnerabilities such as insecure data storage, insufficient encryption (which does not appear in Top 10) and unprotected communication channels.



However, with the growing number of online accounts and mobile applications, the digital footprint of users has expanded, providing attackers with more opportunities to target password reset mechanisms. Unfortunately, users still reuse passwords across multiple platforms or choose weak passwords, contributing to guess or brute-force password reset options.

The **#1 vulnerability** remains **"application does not implement certificate pinning" (26%)** accounting for almost one-third of this type of vulnerability found in both Android and iOS. There is still widespread misunderstanding and misimplementation with certificate pinning, which involves linking specific certificates to specific endpoints within an application. Because this requires detailed knowledge and careful implementation, developers can find this process complex and opt to bypass it.

State of Mobile Security

In 2024, mobile application security continues to be a critical concern as new threats evolve.

71% of organizations have increased the frequency of push updates to mobile applications, occurring once per week or more, thus expanding the attack surface.

74% of DevOps teams rely on documentation to catalog their applications and APIs, with **68%** using spreadsheets.

61% of security teams rank prioritizing mobile issues among their top three challenges, with **22%** citing it as their top.

Security teams use over **25 tools** for detecting threats but struggle to prioritize effectively.

Top 3 Industries Impacted

Manufacturing: Due to supply chain attacks

Healthcare: Frequent targets due to patient data

Finance: High-value targets due to potential for financial gain

OBSERVATIONS

The importance of mobile applications cannot be under-estimated as they provide direct customer engagement, personalized experiences, and significant revenue. However, maintaining visibility and managing APIs remains a challenge, with 57% of security professionals reporting difficulties in gaining full visibility into their mobile apps.

Ensuring security across diverse devices and OS versions adds complexity to safeguarding mobile apps. The use of third-party libraries and SDKs can also introduce vulnerabilities if not properly vetted and updated.

Differences in vulnerability prevalence exist between Android and iOS apps. Both suffer from the lack of certificate pinning (the top vulnerability finding in our 2024 report), but it is more prevalent in Android due to its open ecosystem and diverse development practices. Android's open nature presents more opportunities for security lapses compared to the controlled environment of iOS.

The benefits of mobile apps are far-reaching. Robust mobile apps can enhance operational efficiency and provide critical differentiation for businesses. Therefore, safeguarding mobile apps is crucial for organizations in 2024.

RECOMMENDATIONS

- **Software Development Life Cycle (SDLC):** Continuous security testing across the SDLC is important for all applications. Pentesting across the different phases of the SDLC can be extremely helpful to uncover vulnerabilities, keep app dependencies up to date, and help to prevent common attacks such as SQL injection, XSS, and buffer overflow.
- **Continuous Pentesting:** Conduct automated security audits and vulnerability assessments to identify and prioritize security issues, and perform periodic pentesting to simulate attacks to uncover and remediate these vulnerabilities.
- **Secure Coding Practice:** Integrate continuous security testing into the development lifecycle, adopting secure coding standards and practices, and providing ongoing security training for developers is recommended. Follow the principle of least privilege and create the minimum permissions necessary for the app to function.

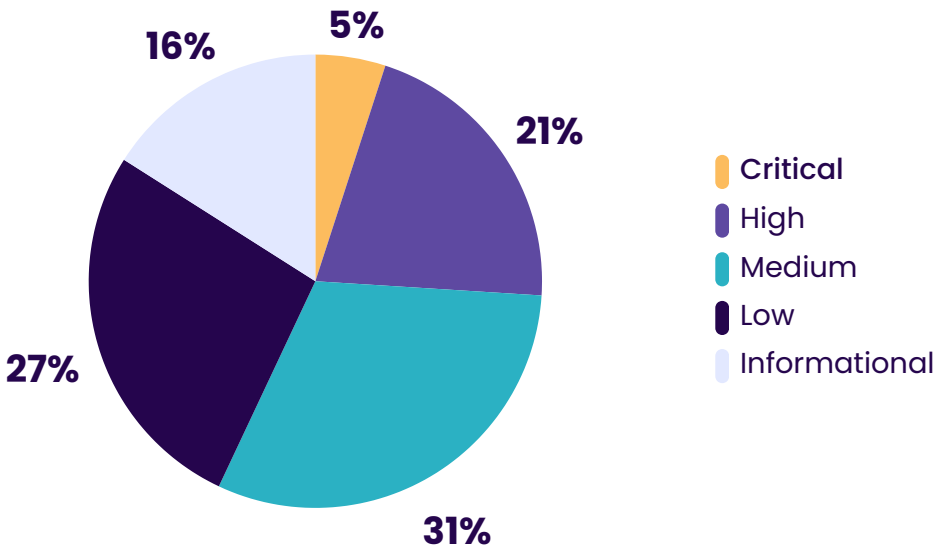
CLOUD

Cloud security is no longer just an IT concern. It's a business imperative. Adversaries are more sophisticated than ever and the stakes have never been higher.

Cloud intrusions have surged by **75%** in the past year from 2023 to 2024 and attackers are becoming increasingly skilled at exploiting cloud environments. It is estimated that is takes an average of just **62 minutes** to spread from an initially compromised host to another within the cloud environment, with the **fastest attacks** doing so in a mere **two minutes**, according to CrowdStrike's 2024 Global Threat Report.

According to our 2024 report findings, **Cloud** represents **7% o**f overall assets tested with **almost two-thirds of risk severities** ranging from **medium to critical.**

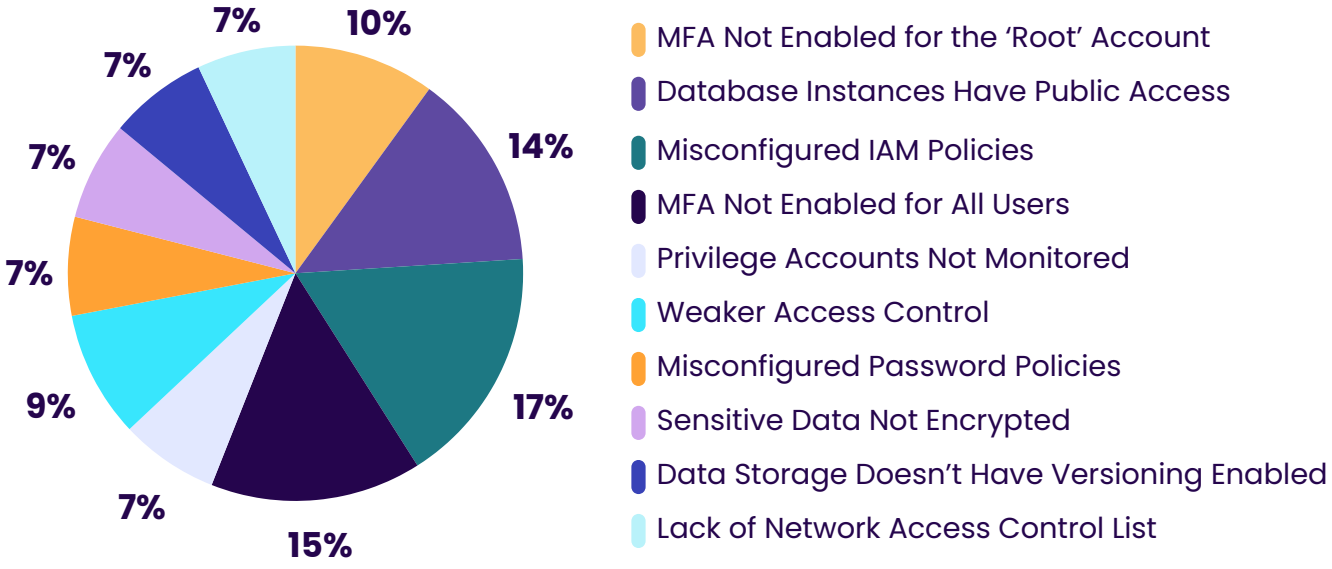
Overall Risk Severities Cloud



Risk Severity Analysis:
The 2024 data shows a distribution of risk findings with almost one-third of risks found in Critical (5%) and High (21%). This represents an increase in Critical severities by 66.7% from 2023. The remaining two thirds of risk findings fall in Medium (31%), Low (27%) and Informational (16%). The Medium risk severities are important and should be validated, and prioritized for mitigation after the Critical and High risks are further investigated and issues are fixed.

Top 10 Cloud Misconfigurations

The Top 10 cloud types of misconfigurations did not change in 2024; however, the prevalence of the **Top 5 misconfigurations increased by a total of almost 10%** vs. 2023. MFA not enabled for all users increased by 5%, database instances that have public access increased by 3%, and misconfigured IAM policies increased by 5%, as well.



One of the many reasons we are seeing a higher inrease in Critical to High vulnerability severity is simply the scale and complexity of cloud environments. Often involving numerous interconnected services, applications, and resources, this complexity increases the likelihood of misconfigurations and security gaps that can be exploited.

Cloud environments are also highly dynamic, with frequent changes and updates that can introduce new vulnerabilities or exacerbate existing ones. And because there is a shared responsibility model in the cloud, it can lead to misunderstandings about who is responsible for securing different parts of the infrastructure, resulting in critical security tasks being overlooked.

Lastly, cloud environments often host sensitive data and critical applications, making them attractive targets for attackers. The potential impact of a breach can be significant, leading to the classification of vulnerabilities as High or Critical. Many organizations rely heavily on cloud services for their core business operations, so vulnerabilities can have severe consequences on business continuity and security.

State of Cloud Security

According to Mordor Intelligence Cloud Computing Market Report (2024-2029), the average number of cloud providers per enterprise has decreased from **2.26 to 2.02** in 2024, reflecting a trend towards consolidation.

Over **60%** of organizations use more than **25 SaaS applications,** with **30%** using more than 50.

Human error continues to be the leading cause of data breaches, with **44%** of organizations experiencing a breach due to a misconfiguration.

Security for **IaaS and PaaS** environments is at the top of investment priorities in 2024, with **33%** of organizations focused on these areas.

Top Industries Impacted

Cloud misconfigurations impact various industries, including:

Healthcare: 31% of healthcare organizations experience a cloud misconfiguration

Finance: 30% of FSIs

Retail: 26% of retail

Technology: 23% of technology firms

OBSERVATIONS

In 2024, cloud security remains a dynamic and evolving field, reflecting both advancements in technology and the growing sophistication of cyber threats.

More organizations are migrating to multi-cloud and hybrid cloud environments , which adds complexity to security management. New vulnerability and attack vectors are constantly emerging, such as those related to misconfigured cloud services, inadequate access controls, all appearing in the Top 10 misconfigurations of this report.

In 2024 we saw increased security and regulations around cloud security, with standards and compliance requirements evolving to address new risks and threats. See Page 38 for more information regarding the new compliance changes. To adjust to these new regulations, we are seeing cloud service providers (CSPs) enhance their security offerings.

Organizations are turning to non-traditional and innovative security solutions to help them secure their cloud environments. This includes cloud security posture management (CSPM) tools, cloud workload protection platforms, (including VMs, containers, and serverless) as well as implementing more best practices for cloud security.

RECOMMENDATIONS

- **Leverage Automation and Continuous Security Testing:** Utilize automation such as Attack Surface Management (ASM) for continuous security monitoring to safeguard cloud assets. Penetration testing can also be automated to continuously identify and mitigate vulnerabilities, improve incident response, and conduct compliance checks to improve efficiency and reduce human error.
- **Invest in Cloud Security:** Organizations need to prioritize investment in cloud security by performing regular security audits and vulnerability assessments to identify and address potential weaknesses. These should be ongoing assessments, and not periodic or point-in-time as the cloud threat landscape is always changing.
- **Understand Your Shared Responsibility:** Ensure that your security team fully understands their responsibility vs. the CSP should a breach occur. Develop an incident reponse plan that is regularly reviewed with your CSPs and agree upon security measures and responsibilities to take quick and efficient action.

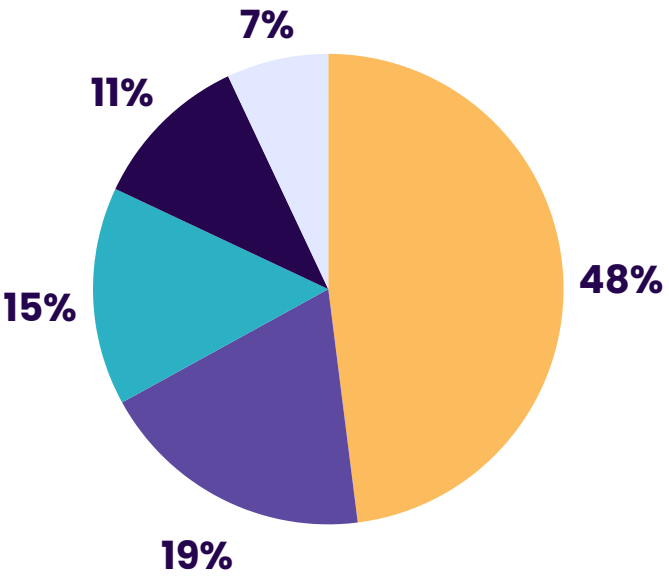
INDUSTRY OVERVIEW

Enterprises in all industry sectors are beginning to take advantage of offensive security strategies as part of proactive security processes focused on identifying and monitoring potential attacker entry points before an attack occurs.

It is important to note that sectors like Computer Software & Technology have witnessed a significant increase in cyber threats in 2024. These were characterized by a wide range of sophisticated attacks from such notable threat actors as Midnight Blizzard (aka Nobelium, APT29, Cozy Bear), LockBit Ransomware Group, Muddy Water APT Groups, Killnet 2.0 Hacker Group, and others.

The healthcare sector also experienced some of the largest breaches in U.S. history, including the UnitedHealth ransomware attack and the unauthorized access to Kaiser Foundation Health Plan patient data. UnitedHealth's Change Healthcare key operations were disrupted by a cyberattack affecting 100% of billing and insurance claims for over 5,000 hospitals, networks, and providers. Kaiser reported 13.4 million of its members' information was taken in a data breach due to unauthorized access in its network after the company shared patient information with third-party advertisers.

Offensive security solutions like continuous security testing and red teaming exercises can identify potential risks and map critical attacker entry points to thwart attack like those mentioned above.

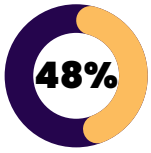


Top 5 Most Impacted Industries with Highest Findings

- Computer Software & Technology
- Professional Services
- Banking & Finance
- Healthcare
- Retail & eCommerce

INDUSTRY INSIGHTS

Different industries, from finance to healthcare to technology, rely on pentesting to safeguard their unique and critical systems, ensuring robust security against evolving threats.

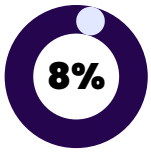


It has been a tough year so far in 2024 for the **Computer Software & Technology** industry, which has been besieged by an escalation in cyber incidents targeting technology infrastructure. BreachLock clientele in this sector saw a high number of severe vulnerabilities with 15% of findings categorized as Critical to High.

Professional Services is defined as consumer services, HR, law and legal, as well as staffing and recruitment. It is not surprising that this sector saw vulnerabilities across severity, especially in law and legal which hold sensitive client information. Findings included Critical (2%) to High (5%) with over one-third falling into Medium (34%) severity, which is considerable and worth prioritizing for further investigation.

The **Financial Services** sector saw the 2nd highest number of vulnerabilities along with healthcare. Findings include Critical (3%), High (10%), and Medium (34%). As a high-value target, there is increased focus by these institutions on regulatory compliance (PCI DSS).

Healthcare organizations saw some of the largest breaches in the U.S. in 2024, including UnitedHealth and Kaiser. Healthcare continues to be reliant on pentesting to protect PHI with HIPAA compliance other regulations as driving forces. Healthcare had the 2nd largest total of Critical and High findings across sectors at 4% and 9%, respectively.



Retail and eCommerce continue to see the value in pentesting as they this sector remains vulnerable to attacks due to high transaction volume and sensitive customer data such as credit card information. This sector was #1 in highest number of findings in Critical (4%) and High (15%).

Insights and Recommendations

Cybersecurity incidents are increasing, often due to organizations' failure to incorporate security by design. While investments in technology challenge our ability to ensure resilience to future disruptions, we must address the risks and vulnerabilities introduced by the most recent transformations with offensive security solutions before an attack occurs.

- Invest in and build trust in new technologies across the organization early.
- Provide a clear picture of current cyber risk posture and capabilities.
- Sustain compliance with regulatory requirements.
- Evolve with new cyber threats by aligning your security and business objectives.
- Enhance the efficiency, effectiveness, and timeliness of incident response.

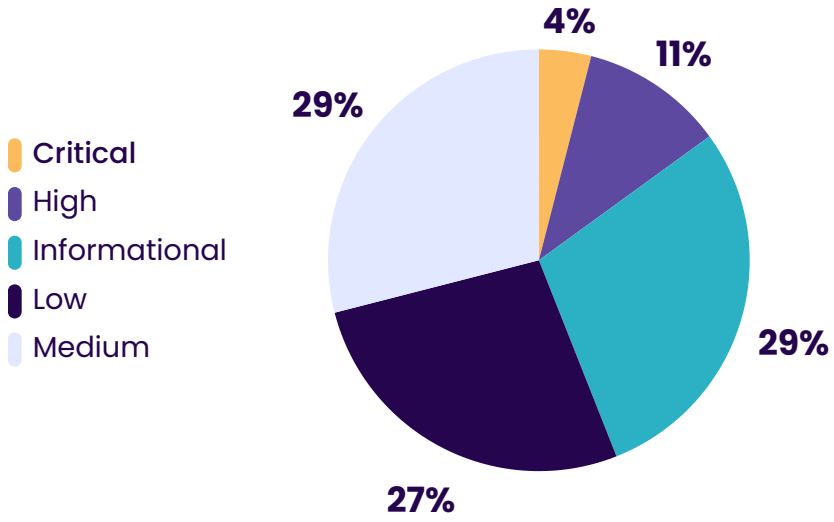
COMPUTER SOFTWARE & TECHNOLOGY

Computer software and technology companies handle and store a wide range of data including customer information, operational data, intellectual property, and security data like logs and incident response reports. They often work with Managed Service Providers (MSPs) to manage IT infrastructure and improve operational efficiency.

MSPs monitor networks, manage backups, deploy and manage endpoint security, leverage cloud services for scalability, and some offer SOC services for threat detection and response.

As a result it is no surprise that computer software and technology companies remain prime targets by cyber criminals. A successful attack can access valuable customer data and have severe consequences, affecting thousands if not millions of customers.

Severity of Findings

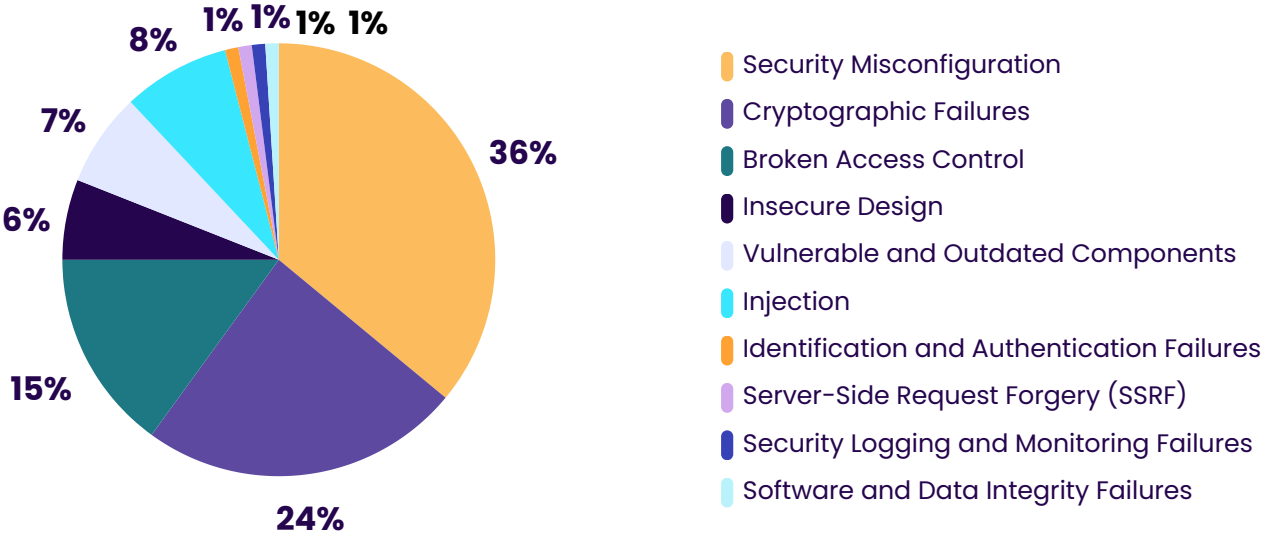


Risk Severity Analysis:

The 2024 data reveals an almost three-fold increase in Critical (4%) and High (11%) severity findings combined compared to 2023. This is followed by a total of 56% of findings falling into Medium (29%) and Low (27%) which is a decrease from 2023, but certainly worth noting as these account for over half of the findings.

OWASP Top 10

Top 3 Risks on OWASP Top 10: When mapped to OWASP Top 10, the report data corresponds with the top 3 categories resulting in Critical and High vulnerabilities.



State of Cyber Security
Computer Software & Technology

Malicious actors are now targeting a wider range of victims. According to research by McKinsey, there's a growing number of attacks on small and midsize businesses. These attacks can be far more damaging proportionally, as the victims are unable to pay ransoms and may lack resources to recover damaged data.

Computer software and technology companies, including MSPs, must consider how to protect customer data against increasingly sophisticated and persistent attackers why complying with stringent regulatory requirements.

This industry sector cannot take network security for granted and it is vital that their data as well as sensitive customer information is protected.

OBSERVATIONS

As previously mentioned in this report, 2024 has been unprecedented in the scale of attacks wielded at the technology sector. Cybercriminals are using more advanced tactics, including AI-driven attacks and sophisticated phishing schemes, making it harder to defend against breaches.

It is known that the expansion of cloud services, IoT devices, and continued remote work has significantly increased the attack surface and the propensity of potential threats.

In review of the top three risks affecting the computer and software technology sector, security misconfigurations, cryptographic failures, and broken access controls retain a disproportionate number accounting for 75% of overall vulnerabilities. That is remarkable. All three of these exposures share common characteristics including complex and varied settings in software and hardware, human error, and mistakes in defining and enforcing security policies for configuration of access controls.

The reason for the prevalence of these three vulnerabilities can be attributed to the fact that they are easier to detect compared to others. But also it reflects the impact and shift to cloud computing and DevOps practices emphasizing speed and agility, sometimes at the expense of security.

RECOMMENDATIONS

Based on our data findings, Computer Software & Technology organizations should consider the following best practices:

- **Continuous Network Security:** Continuous security testing of both internal and external networks includes securing all servers and virtual machines, paying particular attention to cloud service administrative accounts.
- **Regular Security Audits:** Scheduling regular audits to identify any compromised accounts used to gain access to the network via the cloud, and close doors to and from would be attackers. Secure and protect all internet-facing services.
- **Vendor Management:** Trusted third-party vendors are often seen as a potential risk. Vet them carefully to confirm their compliance with relevant regulatory requirements. Pentest any connected systems and SaaS providers, and review their security plan to ensure that they meet your organizations security and regulatory standards.

BANKING & FINANCIAL SERVICES

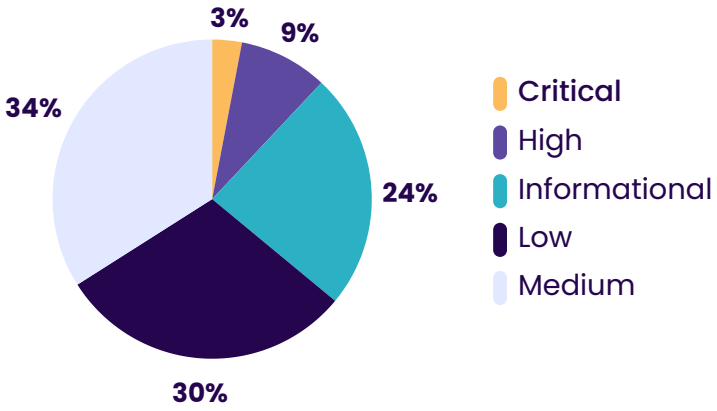
Most Financial Service Institutions (FSIs) have migrated to Open Banking to provide more competitive, new, and innovative services to banking customers such as wealth management, high-yield savings accounts, or Buy Now, Pay Later (BNPL) options. This banking practice allows third-party financial service providers open access to consumer banking, transactions, and other financial data from banks and non-bank financial institutions through the use of APIs. However, Open Banking raises the potential for both promising gains and grave risks to consumers as more of their data is shared more widely.

As data is shared with third-party providers, unauthorized access has become a reality and hackers are exploiting vulnerabilities in the APIs, exposing sensitive customer data. Upon analyzing the 2024 report and industry data, APIs remain an attractive target for attackers with a **71.43% increase** in Critical and High severities. FSIs must remain vigilant in protecting consumer information and investing in new secuirity technologies that can help them adjust this aggressive landscape.

Severity of Findings

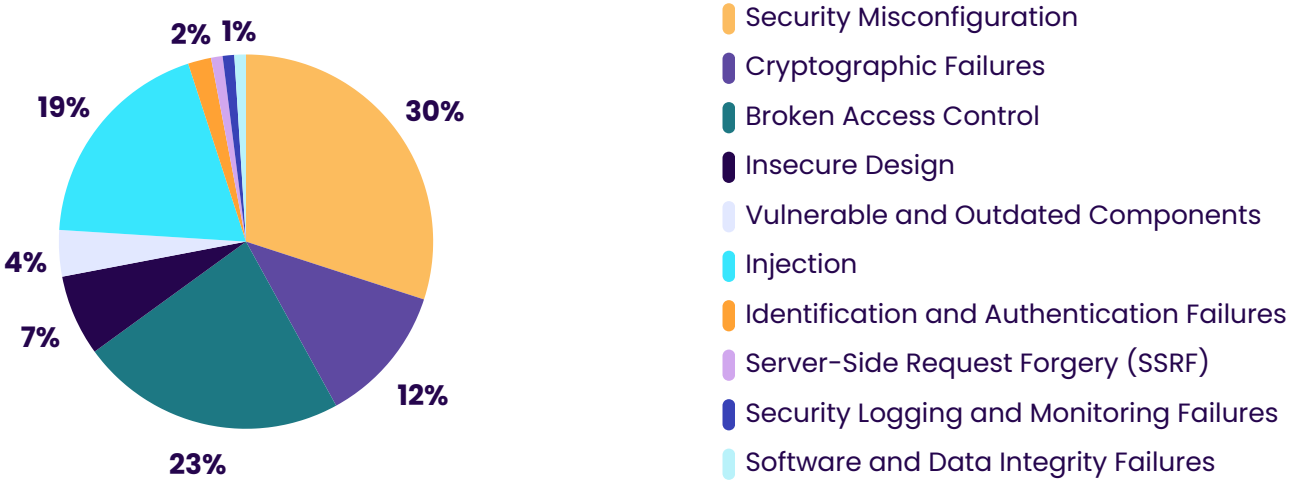
Risk Severity Analysis:

The report data reveals a **71.43%** increase of in Critical (3%) and High (9%) severities in 2024 vs. 2023. The remaining severity findings are also extremely significant with Medium (34%) findings representing over one-third and Low (30%) while Informational (34%) constituting over half of the severity findings.



OWASP Top 10

Top 3 Risks on OWASP Top 10: When mapped to OWASP Top 10, the report data corresponds with the reports top 3 categories in Critical and High vulnerabilities.



State of Cyber Security
Financial Services

In 2024, the financial services sector continues to face significant security challenges. Increased regulatory scrutiny, adoption of advanced technology lke AI and machine learning, and the exponential growth of data, FSIs are prioritizing data privacy and protection to maintain customer trust and comply with regulations.

Despite this, there were two major financial breaches in 2024 including the FinTech ransomware disaster at Evolve Bank & Trust, where LockBit 3.0, a ransomware-as-a-service group posted customer information on their web forum for extortion.

The other major attack was at Wells Fargo due to a data breach through a third-party vendor, resulting in the unauthorized disclosure of customer data.

OBSERVATIONS

While Open Banking fosters financial transparency and a competitive market, it also expands the threat landscape for financial institutions greatly. One of the primary concerns is the potential for data breaches as customer data is shared across various platforms, increasing the attack surface for cybercriminals. The APIs themselves can be a target; if not properly secured, they can become entry points for unauthorized access. Moreover, ensuring that third-party providers adhere to stringent security protocols is challenging, as their security practices may not always align with those of the financial institutions, leading to potential inconsistencies and gaps in protection.

The complexity of managing these risks is further compounded by regulatory compliance requirements, which vary across regions and jurisdictions. Financial institutions must implement robust security measures, conduct thorough due diligence on third-party partnerships (TTPs), and maintain rigorous continuous monitoring to mitigate these risks effectively.

FSIs are under heightened scrutiny by regulators to enhance their security measure and ensure compliance with new standards in 2024, which are outlined on Page 38.

RECOMMENDATIONS

Based on our data findings, here are a few recommendations that are suggested for the financial sector:

- **Secure APIs:** Ensure third-party APIs are secure with strong encryption (e.g., TLS/SSL) to protect data in transit. Regularly conduct penetration testing to identify and mitigate vulnerabilities in API endpoints. Implement rate limiting and anomaly detection to prevent abuse.

- **Third-Party Risk Management**: Conduct thorough due diligence and regular assessments of third-party providers to ensure they adhere to stringent security practices. Establish clear contractual agreements outlining security expectations and responsibilities.

- **Implement Secure Protocols:** Use OAuth 2.0 or similar secure protocols for authorization, ensuring that only authorized third-party providers can access specific data based on user consent.

HEALTHCARE

As healthcare providers adopt advanced technologies for life saving services, new medical IoT devices, or for electronic health records (EHRs) to improve patient care, they knowingly expand their digital footprint, making them prime targets for cyberattacks.

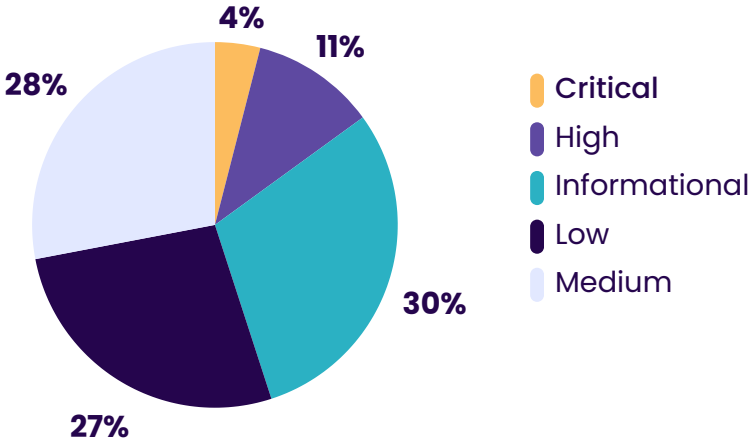
Ransomware attacks, data breaches, and phishing schemes are becoming alarmingly common, often leading to the unauthorized access and exploitation of sensitive patient information. The interconnected nature of modern healthcare systems means that a single vulnerability can have far-reaching consequences, potentially disrupting critical medical services and endangering lives.

As a result, the healthcare sector must prioritize robust security measures, continuous security testing and monitoring, and staff training to safeguard against these evolving threats to ensure the resilience of their operations in the face of persistent cyber risks.

Severity of Findings

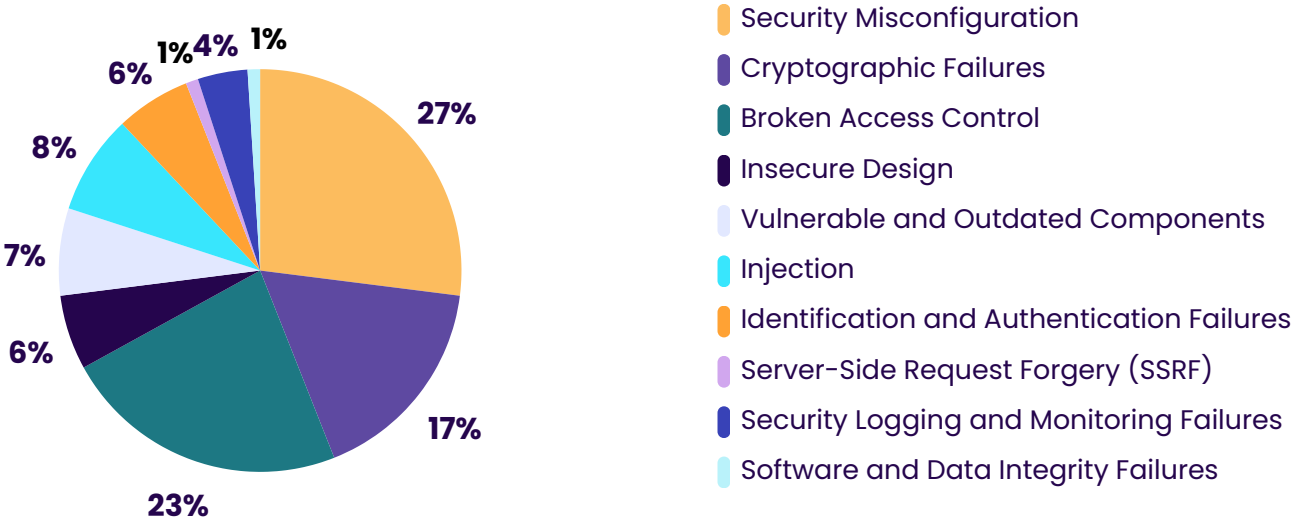
Risk Severity Analysis:

Report findings show an **85.71%** increase in Critical (4%) and High (9%) in severity findings vs. 2023. Medium severities significantly decreased from 25% in 2024 compared to 40% in 2023. Low (27%) findings also decreased with Informational accounting for slightly over one-third of findings.



OWASP Top 10

Top 3 Risks on OWASP Top 10: When mapped to OWASP Top 10, the report data corresponds with the top 3 categories resulting in Critical and High vulnerabilities.



State of Cyber Security
Healthcare

In May 2024, there were **51 data breaches** in healthcare in the U.S. Most notably in the February attack on United Health-owned Change Healthcare, resulting in a paid $22M ransom to a Russian cybercrime group, and the May ransomware attack on Ascension health system, impacting their emergency care services.

Across these breaches, **8.5 million individuals** had their PHI compromised. While associated businesses account for only **23.5%** of the breaches, they were responsible for **65.5%** of the breached healthcare records.

In Q1, **222 breaches** were registered, representing a **41% increase** versus the same period last year.

The overall impact is **11.6 million people** had their data exposed in 79 reported breaches affecting 500 or more individuals in 2024.

OBSERVATIONS

The report data shows that the top vulnerabilities for healthcare organizations align with OWASP Top 10. Security misconfigurations, broken access controls, and cryptographic failures all can result in unauthorized data access, data corruption or deletion, and access to even administrative operations.

An injection vulnerability finding worth mentioning, as injection appears in Critical/High report findings, is Cross-Site Scripting (XSS). Although not mentioned directly, an XSS attack can work in several ways, exploiting vulnerabilities in web applications used by healthcare providers, patients, and administrative staff. The attacker can craft a malicious script, typically in JavaScript, designed to execute in the victim's browser to steal cookies, capturing keystrokes, and redirecting users to phishing sites.

All of these vulnerabilities are particularly critical to healthcare operations due to the highly sensitive nature of the data involved and the potential for widespread disruption. For example, healthcare organizations store vasts amount of patient health information (PHI) including medical histories, diagnoses, treatment plans, and insurance details. Exposure of this data can lead to identify theft, fraud, and significant privacy violations in accordance with HIPAA.

RECOMMENDATIONS

Based on our data findings, here are a few recommendations that are suggested to to mitigate the top vulnerabilities:

- **Regular Security Audits:** Conduct frequent, if not, continuous security assessments to identify and address vulnerabilities in systems and applications.
- **Continuous Security Testing:** Ensure you are continuously testing and monitoring your systems, including IoT devices, to ensure security controls are effective.
- **Prioritize Medium and Low-Risk Findings:** Allocate resources to address these findings as they comprise a significant portion of total findings to reduce overall risk exposure to the organization.
- **Compliance Requirements:** Enforce all systems and processes are HIPAA compliant by implementing safeguards to protect the confidentiality, integrity, and availability of electronic health records (EHI).

PROFFESIONAL SERVICES

For this report, Professional Services includes organizations like consumer services, human resources, law practices, legal services, and staffing and recruitment. Professional Services replaces the IT Services & Consulting sector from our 2023 report as one of the Top 5 industries with the highest number of risk findings in 2024.

Professional services organizations face significant security challenges due to the sensitive data they handle, the complexity of attacks, and growing regulatory demands.

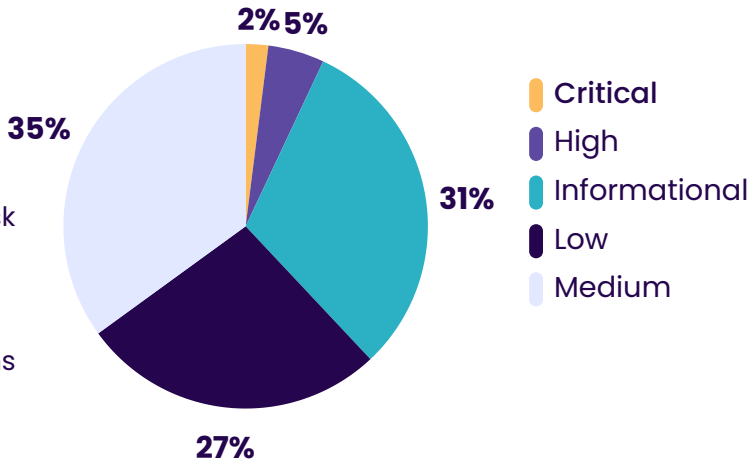
Human resources manage personal and financial employee information, including Social Security numbers and health records. Law practices handle confidential client data and intellectual property, while staffing and recruitment agencies process resumes, background checks, and employment histories.

Attackers target consumer services for payment card data and personal information through phishing, ransomware, and malware. Law practices attract sophisticated attacks aimed at accessing sensitive legal information, often through targeted spear-phishing campaigns.

Severity of Findings

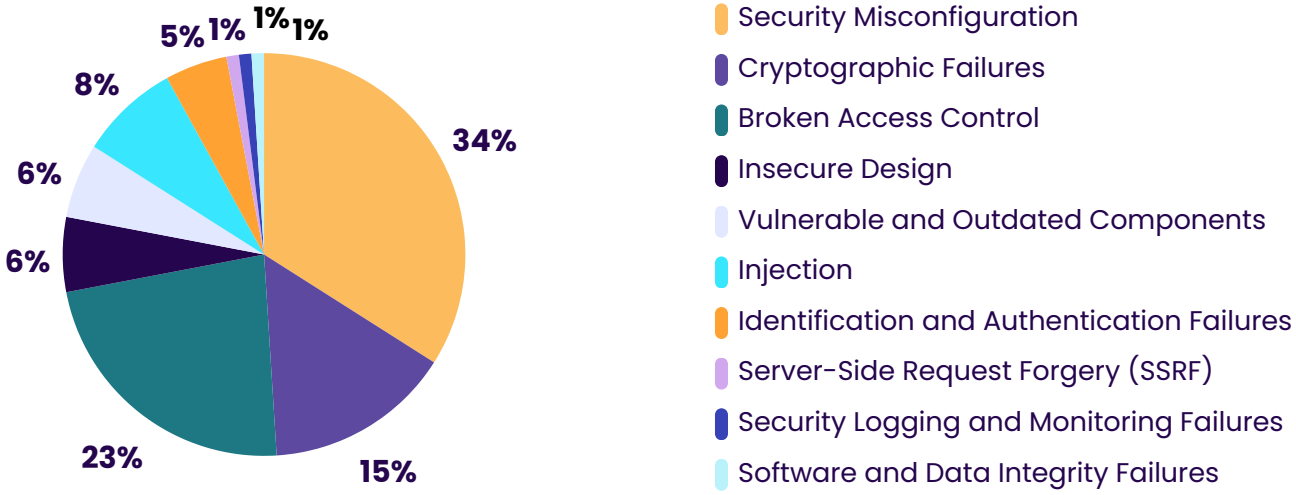
Risk Severity Analysis:

As a newcomer to this report, severity findings were aggregated across those types of segments tested. Critical to High risk findings total 7%. This is considerably less than the remainder with Medium (35%) accounting for over one-third of findings, which if not analyzed could lead to problems down the road. Low findings accounted for 27% with Informational at 31%.



OWASP Top 10

Top 3 Risks on OWASP Top 10: When mapped to OWASP Top 10, the report data corresponds with the top 3 categories resulting in Critical and High vulnerabilities.



State of Cyber Security
Professional Services

Consumer services is a broad category of different types of service organizations. and each face varying cybersecurity challenges. Let's look at some of the top challenges facing the consumer services sector.

Regulatory Compliance
Organizations must comply with various data protection regulations such as GDPR, PCI DSS, CCPA, and industry-specific standards requiring stringent data protection measures and regular audits.

Insider Threats
The risk of data breaches within these organizations, whether intentional or not, pose significant challenges, especially in environments where there is high turnover.

Third-Party Risks
Reliance on third-party vendors for various service introduce risk if vendors do not maintain robust security measures.

OBSERVATIONS

The top 3 risks that appear on the OWASP Top 10 include security misconfigurations, broken access controls, and cryptographic failures. We see the same risks across several industries in 2024. As these three risks have been explained previously, let's look at some additional challenges affecting the consumer services sector:

Advance Persistent Threats (APTs): Attackers use sophisticate APTs to gain long-term access to networks, particularly in law practices where the data can be highly valuable over time.

Phishing & Social Engineering: All consumer service sectors face phishing attacks aimed at stealing credentials or deploying malware.

Data Encyrption and Secure Communication: Ensuring data is encyrpted both in transit and at rest is vital, especially for legal and HR services where confidentiality is essential.

Incident Response & Recovery: Consumer services organizations are not known to have the latest technology, and when it comes to protecting data, this sector may be less sophisticated than other sectors such as financial services. Using offensive security tools that can help maintain system updates or enhance IR plans can help to improve IR preparedness.

RECOMMENDATIONS

Based on our data findings, here are a few recommendations that are suggested to to mitigate the top risks:

- ☑ **Regular Updates and Patch Management:** Ensure that all systems and software are kept up to date with the latest security patches and software updates. Implement automation such as continuous scanning to help stream-line this process and reduce the risk of human error.
- ☑ **Network Segmentation:** Segment the network to isolate critical systems from less secure and outdated components, limiting the ability of attackers to move laterally within the network and access sensitive systems.
- ☑ **Regular Seurity Assessments and Audits:** Conduct periodic security assessments and vulnerability scans to identify and address potential weaknesses. Use these assessments to inform and prioritize remediation efforts.

RETAIL & eCOMMERCE

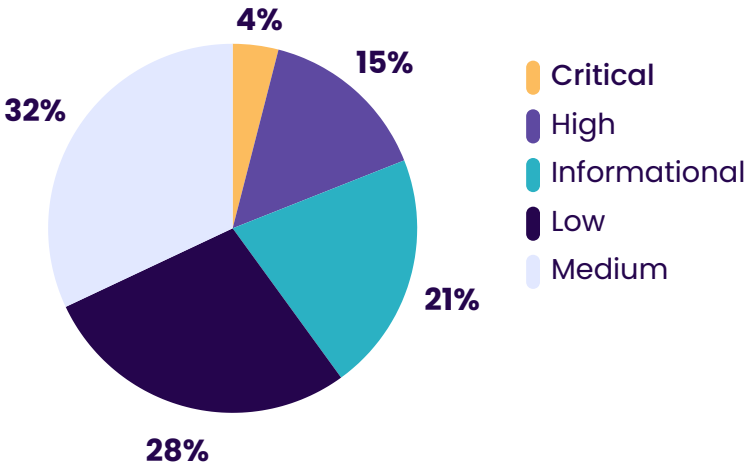
Due to the high volume of transactions and interactions with customers, it can be challenging for retail organizations to monitor and secure all activities effectively. Retailers handle vast amounts of sensitive customer data, including payment card information, and application data that includes name, address, and social security numbers. This makes retail prime targets for attackers who would like nothing more than to hold this data for ransom or face the risk of deliberate leakage on the Dark Web..

The retail environment includes the integration of multiple access points (online, point-of-sale (POS), mobile apps, web, and third-party vendors) to create a complex network that can be harder to secure. Dependence on third-party services for payment processing, logistics, and other functions can introduce vulnerabilities if those vendors are not adequately vetted to ensure their software and systems are secure.

Severity of Findings

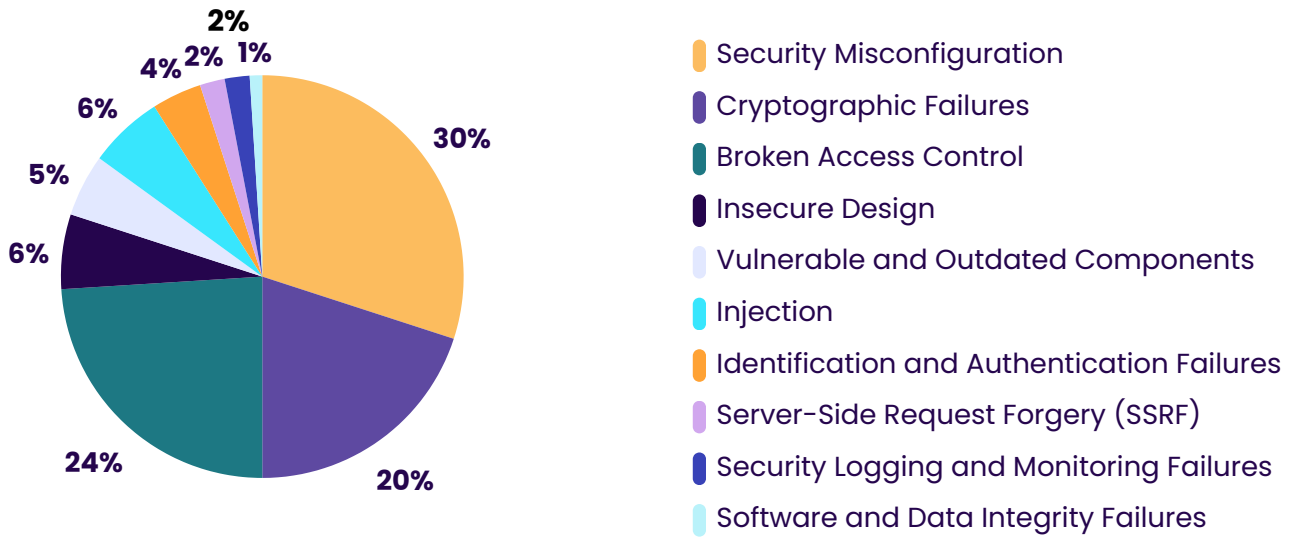
Risk Severity Analysis:

In 2024, report data found that Critical (4%) and High (15%) risk findings decreased by almost 30%, which is significant. Medium (32%) severities were relatively the same and Low (28%) findings increased slightly alongside Informational (21%) findings. Although these last findings do not have any current material impact, these constitute almost one-third of findings that could potential lay the foundation for future attacks.



OWASP Top 10

Top 3 Risks on OWASP Top 10: When mapped to OWASP Top 10, the report data corresponds with the top 3 categories resulting in Critical and High vulnerabilities.



State of Cyber Security

Retail & eCommerce

In 2024, the retail sector faces evolving cyber threats that demand vigilance and proactive security measures.

45% of retail encountered a ransomware attack in 2024, a decline from previous years. **92%** of victims faced attempts to compromise backups during attacks, with **47% succeeding.** And, **56% of ransomware incidents** resulted in data encryption, lower than the global average.

The mean cost to recover from a ransomware attack in the retail sector increased to **$2.73M with 60% paying an average $950K of the ransom** to retrieve data, decreasing by 68% from $3M.

Retail companies are increasingly mentioning cybersecurity in their SEC filings, reflecting heightened awareness.

OBSERVATIONS

Based on the data observations, the report's top 3 Critical and High vulnerabilities include security misconfigurations, cryptographic failures, and broken access controls. As these are similar findings, let's look at how retailers are using technology to expand their consumer reach and the risks involved.

Web Applications: By deploying web applications, retailers are reaching global audiences, offering products to customers who many not have access to physical stores or simply prefer online shopping. It is well established that brick and mortar stores are decreasing dramatically year over year. However, with web applications and the use of data analytics, retailers can provide personalized services and offers, enhancing customer satisfaction and loyalty.

Mobile Applications: Mobile apps allow customers to shop anytime and anywhere, increasing sales opportunities. Features like push notifications, loyalty programs, and mobile-exclusive discounts keep customers engaged and returning.

Custom Services: Offering subscription boxes or recurring delivery services for regular purchases, or IoT try-ons using AR and VR technologies, allow customers to virtually try on products, all of which enhance the online shopping experience.

However, with all of these retail enhancement and services comes an expanded attack surface and attacker playground.

RECOMMENDATIONS

- **Secure Coding Practices:** Conduct continuous scanning during the software development lifecycle, including penetration testing to secure code and ensure that vulnerabilities are addressed during the development process.
- **Input Validation and Sanitization:** Ensure all user inputs are validated and sanitized. Use allowlists and escape special characters to prevent malicous code execution.
- **Application Security:** Conduct regular and continuous pentesting for both web and mobile applications that store sensitive information to keep a pulse on security weaknesses, and need for updates and patches.
- **Third-Party API Assessments**: Conduct thorough due diligence and regular assessments of third-party apps and APIs used to connect different services. Pentesting can identify vulnerabilities if proper authentication and authorization is not enforced.

INDUSTRY IMPACT OF NEW 2024 CYBERSECURITY REGULATIONS

In 2024 we saw an onslaught of new and more stringent cybersecurity regulations that were enacted affecting all industries. But arguably the most impactful change has been the new Securities and Exchange Commission (SEC) Disclosure Rules Act. Enacted in July 2023, it was only in 2024 that we began to see the effect that these rules had on major domestic and global companies who experienced significant breaches that were immediately disclosed to the SEC and made public.

Let's review a number of new regulations and the reverberation it has had across industries in the U.S., UK, and Europe.

SEC Cybersecurity Disclosure Rules: In July 2023, the U.S. SEC adopted new rules that require domestic registrants and foreign private issuers (FPIs) to disclose cyber incidents within four business days in addition to submitting disclosure forms regarding the incident. These rules require publicly traded companies to disclose cybersecurity risks and incidents that are material to investors. This impacts organizations by necessitating transparency about their cybersecurity posture and any breaches that may affect the value of the company.

PSTI Act (Product Security and Telecoms Infrastructure Act): The PSTI legislation is a UK regulatory framework to enhance the security of consumer internet-connect devices. Affecting primarily the manufacturing industry, PSTI sets out minimum security standards that manufacturers must adhere to, ensuring that devices are protected against cyber threats and vulnerabilities. This includes internet or network connectivity from smartphones to game consoles to connected refrigerators.

DORA (Digital Operational Resilience Act): DORA is focused on the financial sector and emphasizes the need for robust digital operational resilience. A unified set of rules, including conducting continuous vulnerability assessments, is aimed at consolidating EU cyber-security regulations to strengthen the IT security of EU financial entities ensuring resilience of the EU's financial sector.

NIS2 (Network and Information Systems Directive 2): NIS2 sets out measures to boost the overall level of cybersecurity and resilience of network and information systems within the EU. Organizations are required to implement risk management practices and report significant cyber incidents.

CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act of 2022): CIRCIA affects U.S. organizations by requiring them to report cyber incidents and ransomware attacks. This regulation aims to improve the nation's cybersecurity through collaboration between the private sector and federal agencies.

EU CRA (European Union Cyber Resilience Act): Although still a proposal, the EU CRA is expected to impact organizations by setting cybersecurity requirements for digital products and ancillary services. Organizations need to ensure that their digital tools comply with these new standards.

CONCLUSION

The annual BreachLock Penetration Testing Intelligence Reports have become important to help enterprises and their security teams keep a pulse on the most prevalent vulnerabilities and potential changes to the threat landscape.
It also helps us as a security provider to better understand what is keeping our customers up at night, and to continue to develop innovative solutions to align with their needs and growing attack surface.

In 2024, we have seen an increase of Critical and High severity findings across assets and industries versus 2023. This comes as no surprise as the attack surface expands and attacks become more and more sophisticated. Zero-day attacks have now become the "norm." This is why Offensive Security solutions like Penetration Testing as a Service (PTaaS) and continuous pentesting are so important.

"We need to take the fight back to the attackers."

A proactive and continuous security testing approach signals to attackers that we will find vulnerabilities before they do. Organizations should invest in offensive security solutions to identify potential threats using real-world attack techniques to mitigate vulnerabilities before an actual attack occurs.

At BreachLock, we believe adopting an offensive mindset helps us outsmart the attackers. Our technology provides a centralized approach to visualize risk, understand vulnerabilities, and identify multiple attack routes to critical entry points. We aim to stop attackers and take the fight back to them!

breachlock

BreachLock is a global leader in Continuous Attack Surface Discovery and Penetration Testing. Continuously discover, prioritize, and mitigate exposures with evidence-backed Attack Surface Management, Penetration Testing, and Red Teaming.

Elevate your defense strategy with an attacker's view that goes beyond common vulnerabilities and exposures. Each risk we uncover is backed by validated evidence. We test your entire attack surface and help you mitigate your next cyber breach before it occurs.

Know Your Risk. Contact BreachLock today!

BreachLock Inc.
1345 Avenue of the Americas
33rd Fl., Office #96, New York, NY. 10105

BreachLock NL B.V.
Kon. Wilhelminaplein 1, Tower 4
1062 - HG Amsterdam

hello@breachlock.com

Sources:
Forbes.com: The Future of Busienss Is Mobile: How to Drive ROI Growth with Mobile Apps in 2024
techjury Survey: 17 App Revenue Statistics - Mobile is Changing the Game in 2024
ISACA.org: Securing the Futre: Enhancing Cybersecurity in 2024 and Beyond
Forrester, The Attack Surface Management Solutions Landscape, Q2 2024
Forrester, The External Attack Surface Management Landscape, Q1 2023
Mordor Intelligence, Cloud Computing Markt Report (2024-2029)
Gartner Hype Cycle for Application Security, 2024
Gartner Hype Cycle for Security Operations, 2024
Gov.UK, Cyber security breaches survey 2024
Synopsys 2023 Software Vulnerability Snapshot
IBM Cost of Data Breach Report 2024
CrowdStrike 2024 Global Threat Report
2024 Verizon DBIR Report