Reposify

WHO PROTECTS THE PROTECTORS?

QUIS CUSTODIET IPSOS CUSTODES?

Cybersecurity Industry:

State of the External Attack Surface

2022

Table of Content

Introduction

Sprawling digital footprints create massive blind spots for IT and security teams

Modern business is online. Fast-paced growth involves a constant expansion of a company's digital footprint, creating major blind spots for security teams. **Organizations evolve in the cloud, form subsidiaries, are transitioning to hybrid workspaces and rely on third-party vendors more than ever before.** A study by the Enterprise Strategy Group (ESG) found that 70% of companies use more than 10 tools to manage security hygiene and posture. Digital footprints are sprawling and decentralized, making asset management far more difficult for IT and security teams.

Unknown assets are consistently ranked as modern businesses' main cyber vulnerability

The result is a complex and ever-growing attack surface that leaves companies vulnerable to cyber threat. **External attack surface management becomes extremely challenging for every industry, especially without proper visibility or control mechanisms in place.** This has reinforced the need for resilient, thorough cybersecurity posture. Eighty-six percent of organizations believe they follow best practices for security hygiene and posture management. However, 69% admit they have experienced at least one cyberattack that started through the exploit of an unknown or unmanaged internet-facing asset, according to the aforementioned ESG report.

Furthermore, a recent MIT Technology Review poll found that 51% of Asia-Pacific companies blame cyberattacks on unknown assets. In the same poll, 43% of respondents confirm more than half of their digital assets are stored in the cloud, while 67% of companies mark continuous asset monitoring as a cornerstone of a strong cybersecurity strategy.

Cybersecurity is essential for digital business; but are cybersecurity leaders practicing what they preach?

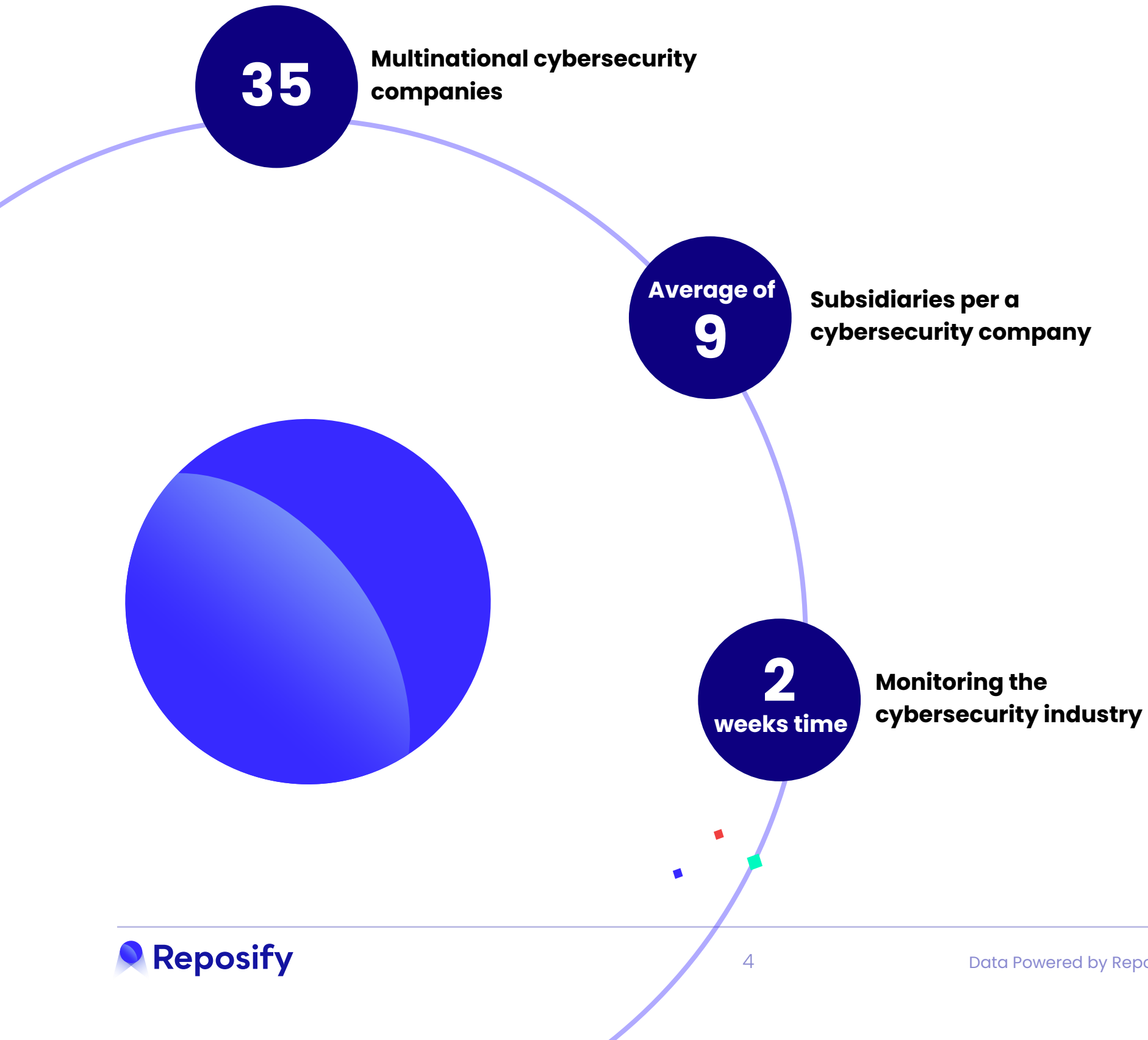
With nearly every industry at risk, are cybersecurity companies truly as cyber-secure as the world would like to think? Worldwide security and risk management spending exceeded $150bn USD in 2021. With every tool at their disposal, is the cybersecurity industry taking advantage of its know-how to protect itself? While it works to protect other vulnerable industries from cyberattack, the industry has forgotten to ask itself a critical question: **who protects the protectors?**

About this Report

Reposify's *Cybersecurity Industry: State of the External Attack Surface 2022* report examines the security posture of the cybersecurity industry, and delivers unique insight into the external attack surface of the world's leading cybersecurity companies.

This report presents information about prevalent exposures of services, sensitive platforms, CVEs and other security issues among **35 multinational cybersecurity companies,** and their **350+ subsidiaries,** with an average of **9 subsidiary companies per multinational firm.** The State of the External Attack Surface report identifies **high or critical issues** facing the cybersecurity industry today. Reposify's technology scans the internet 24/7 for known and unknown assets, indexing over 500 million assets each month. The technology preempts potential breaches by mapping the internet for any exposed assets: cloud services, external-facing on-premise infrastructures, IoT infrastructures, web assets, development tools and more.

The data in this report was derived from Reposify's external attack surface management (EASM) platform, and discovered a total of 258.2 million exposed assets during **a two-week window in January 2022.** At this same period of time, 35 cybersecurity companies were found to host over **200,000 exposed assets.**



Key Findings

97%

of security companies mapped **have exposed assets in Amazon Web Services** (AWS) cloud services.

91%

of web servers identified as **Nginx and Apache** hosted exposed assets.

86%

of security companies analyzed have **at least one sensitive remote access service** exposed to the internet.

51%

of security companies have **at least one exposed database** that could lead to potential leakage.

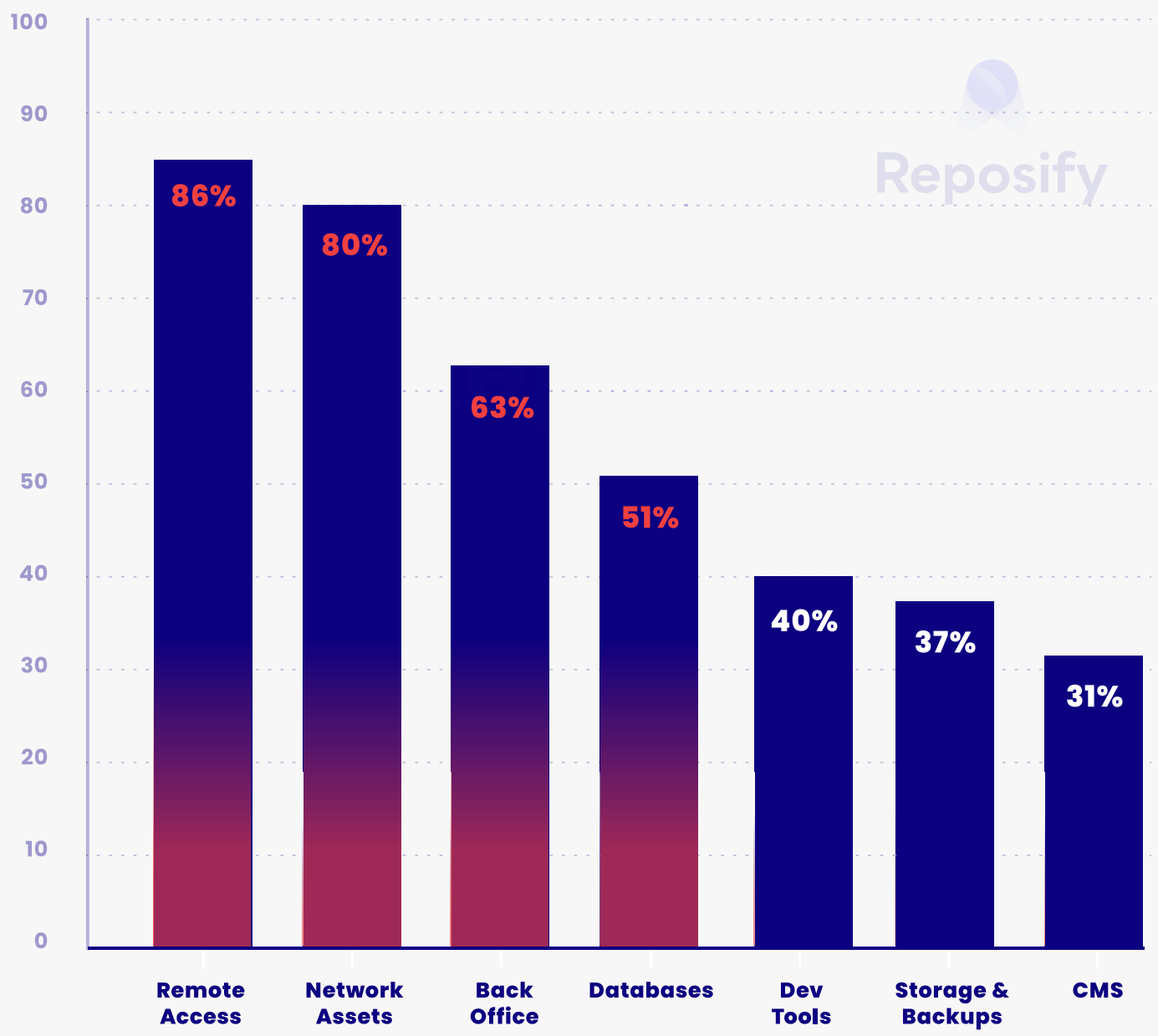
42% of the exposed assets discovered on the Reposify platform were identified with high-severity issues.

Exposed Services Overview

Reposify's EASM platform analyzed the prevalence of exposed sensitive services among cybersecurity companies. The results support a trend across several industries to better index their assets, particularly as digital transformation, work-from-home policies and an increased reliance on cloud services takes hold.

- **86%** of cybersecurity companies analyzed have at least one sensitive remote access service exposed to the internet; a trend that is only set to continue as work from home becomes the norm.
- **80%** of companies have exposed network assets; reflecting the impact of decentralized IT control.
- **63%** of companies have exposed back office internal networks demonstrating that even internal configurations are not immune to cyberattack.
- **51%** of companies have at least one exposed database that is sensitive to attack from malactors. As critical houses of a companies' sensitive information, these are attractive targets for hackers.
- **40%** of companies have exposed development tools, reinforcing the need for companies to continually update tools across the organization to help prevent attack.
- **37%** of companies have exposed storage and backup tools, should these be compromised, services may become unavailable, and permanent and private information may be lost.

Percent (%) of cybersecurity companies with exposed services (by platform category)

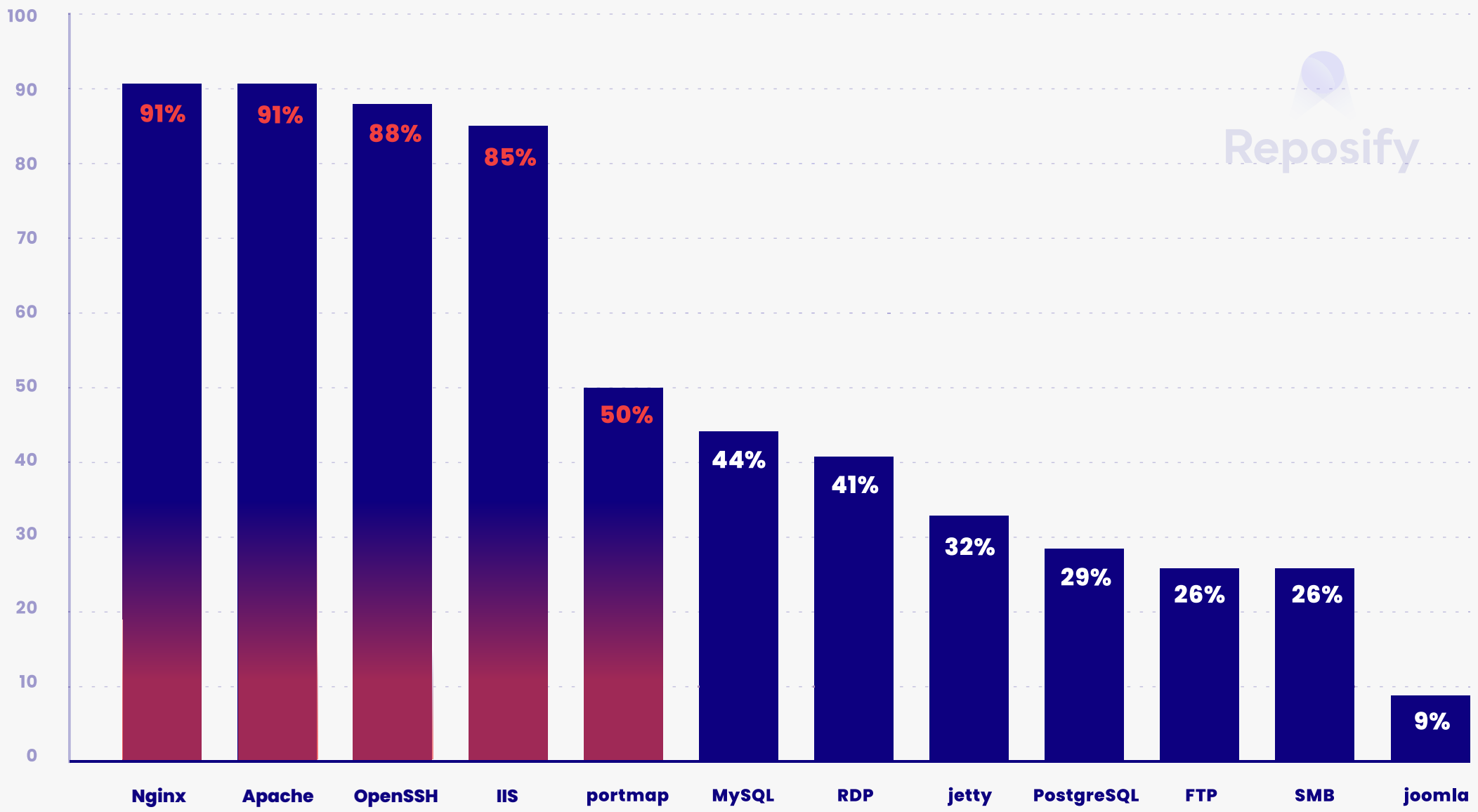


Sensitive Exposed Platforms

Sensitive exposed platforms span remote access platforms, development tools, storage and backups, remote communication tools among others. These asset categories are highly sensitive, and the consequence of a breach is severe - particularly in the case of the cybersecurity industry. Each vulnerability represents a possible entry point to an attacker; it's critical they be protected.

- 91% of web servers identified as **Nginx** and **Apache** hosted exposed assets.
- 88% of exposed platforms were accessible via **OpenSSH**. This is unique to the cybersecurity industry, compared to Reposify assessments of the financial sector and pharmaceutical industry.
- **IIS** followed closely with 85% of cybersecurity companies having a exposed asset on the platform.
- **Portmap**, an open network computing remote procedure call (ONC RPC), saw 50% of cybersecurity companies with exposed assets on the platform.

Percent (%) of cybersecurity companies with sensitive exposed platforms

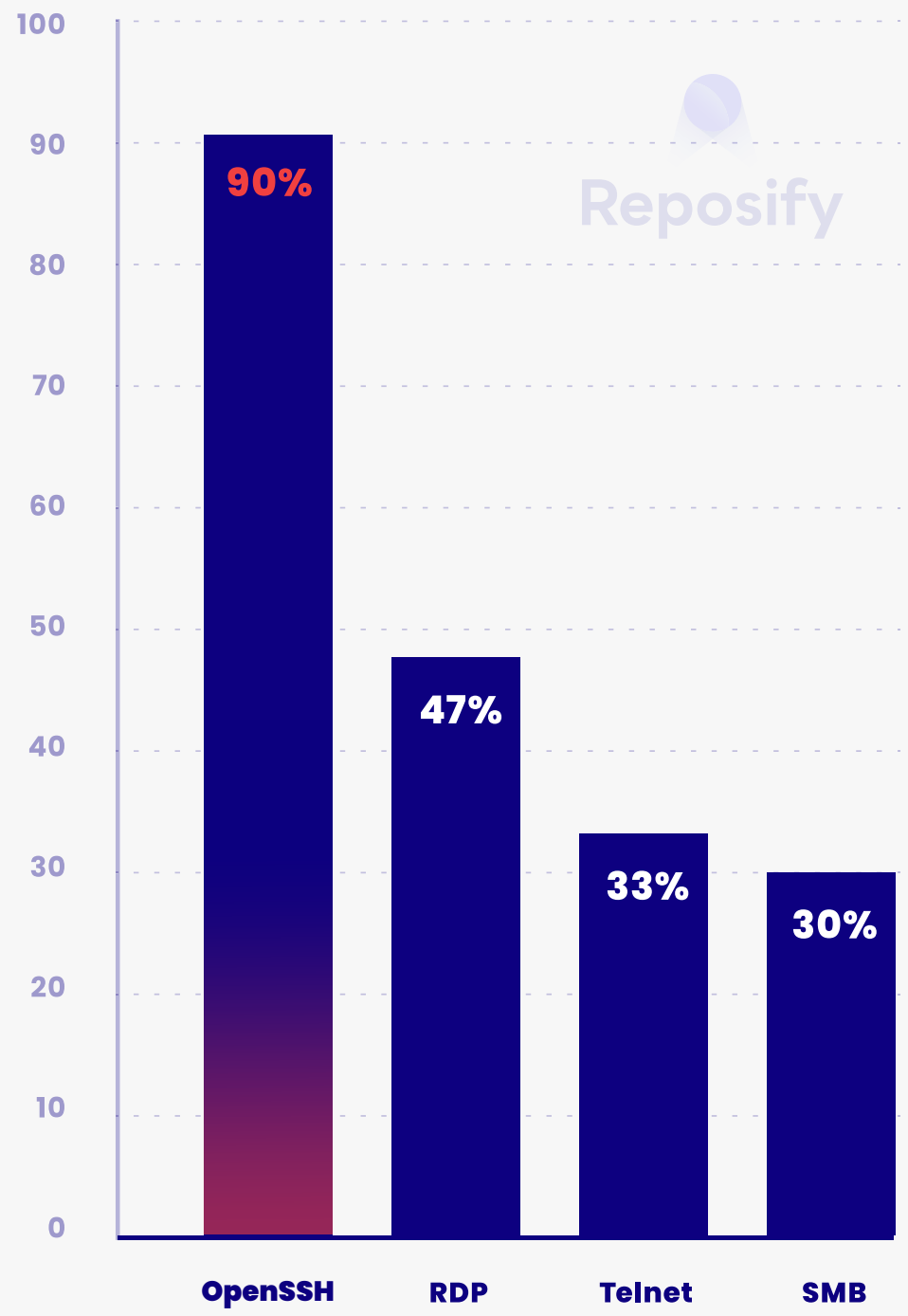


Exposed Remote Access Protocols

The demand for remote access platforms has skyrocketed as employees transition to the home environment in the aftermath of the COVID-19 pandemic, and many companies embrace global remote hiring practices. Findings in exposed remote access platforms for the cybersecurity industry mirror that of other industries – with similar figures cropping up in an examination of finance and pharmaceutical industry exposed remote access platforms.

- **OpenSSH** had nearly twice the amount (90%) of exposed assets compared to **RDP** (47%), whose number of exposed assets increased by 127% in the early months of the COVID-19 outbreak as employees transitioned to the home environment.
- **Telnet** (33%) and **service message block (SMB)** services (30%) follow for a near-tie in third place.

Percent (%) of security companies with exposed remote access protocols

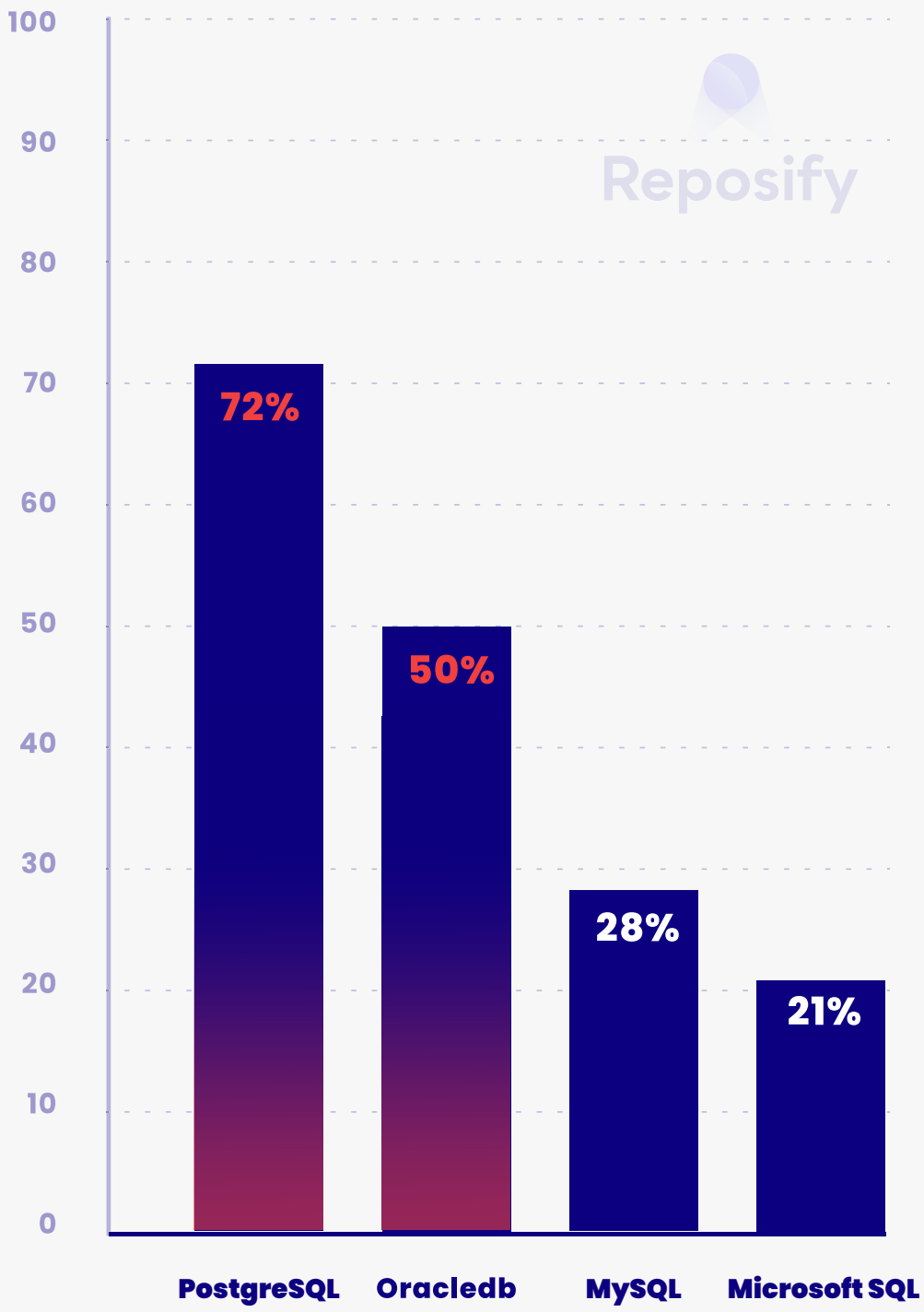


Exposed Databases

Databases are among the most vulnerable to cybersecurity threat. The Reposify platform identified over half (51%) of companies host an exposed database.

- Reposify has found that out of the companies identified as having exposed database, 72% have exposed **PostgreSQL** databases, followed by **Oracledb** with 50%.
- **MySQL** and **Microsoft SQL** are the least exposed database platforms - with 28% and 21% respectively.

Percent (%) of security companies with exposed databases



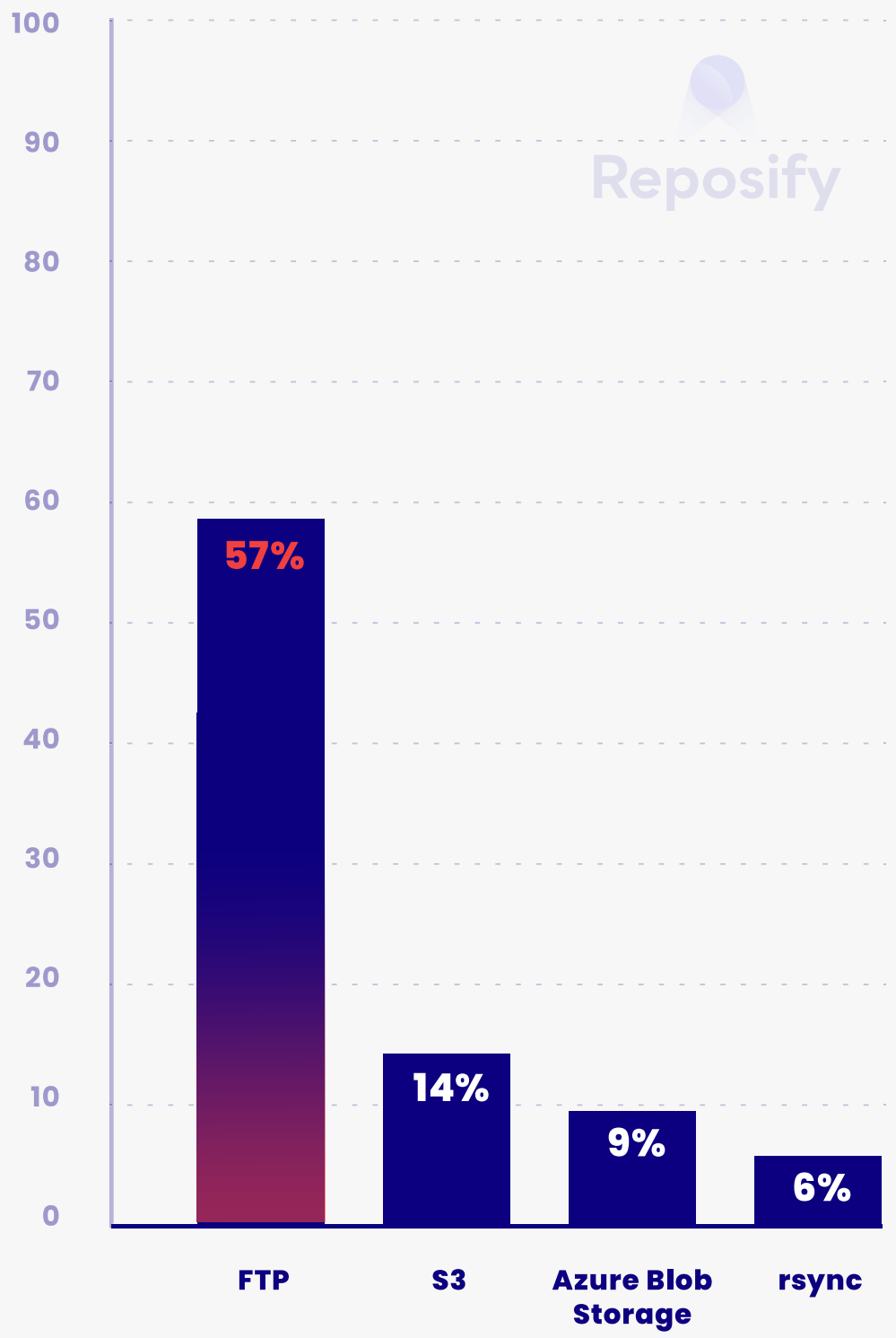
Exposed Storage & Backup Assets

FTPs are used for file sharing within external networks. Though FTPs are incredibly useful as a communication protocol, it's best practice to avoid use altogether as they lack built-in authentication. Reposify's research found that the majority of FTPs were either not behind a VPN or set up to allow for "anonymous authentication", which allows the user to login without a username or password for verification.

Though the number of cybersecurity companies with exposed assets in FTP storage is significantly lower than that of the financial and pharmaceutical industries, the patterns are not dissimilar as FTPs represent a majority of the risk across all industries, according to research by Reposify.

- Despite best practice to avoid them altogether, 57% of cybersecurity companies have exposed **FTP** services.
- Exposer were also found on **S3** (14%), **Azure Blob Storage** (9%) and **rsync** (6%) - but at a significantly lower rate than that of **FTPs**.

Percent (%) of companies with exposed storage & backup assets



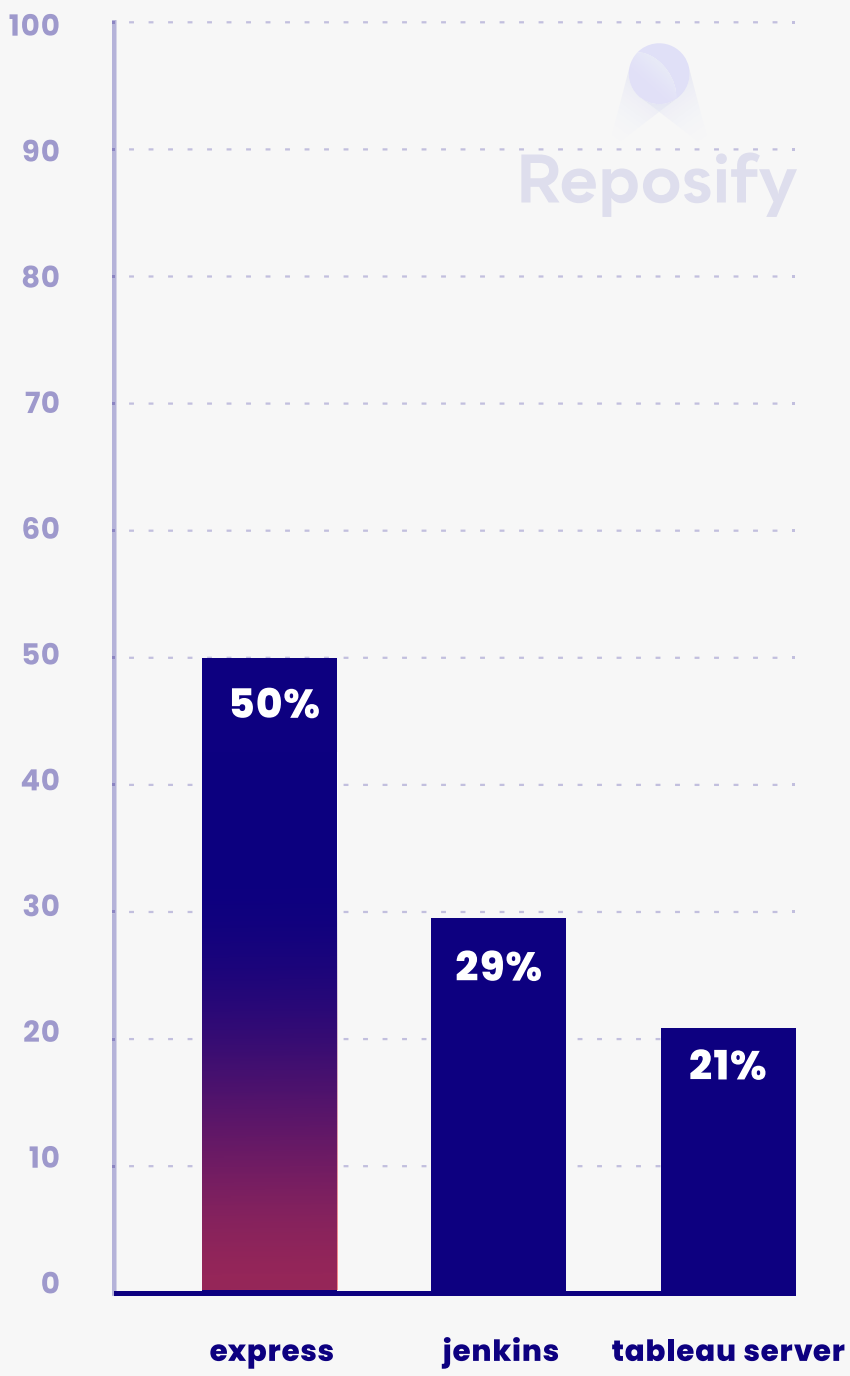
Exposed Development Tools

Development tools can become high risk assets if misconfigured, or failure to regularly update tools to the latest version. When left out of date, dev tools can easily leak information such as source code, business analytics, unprotected API endpoints and more.

The exposure of these tools is especially problematic as it can increase the probability of a supply chain attack. Malicious code can be added to an otherwise legitimate application, like SolarWinds, PHP related services, CodeDev and others.

- 50% of cybersecurity companies using **Express** had exposed development tools.
- **Tableau server** and **jenkins** saw 21% and 29% of companies with exposed development tools on their servers.

Percent (%) of companies with exposed Dev Tools

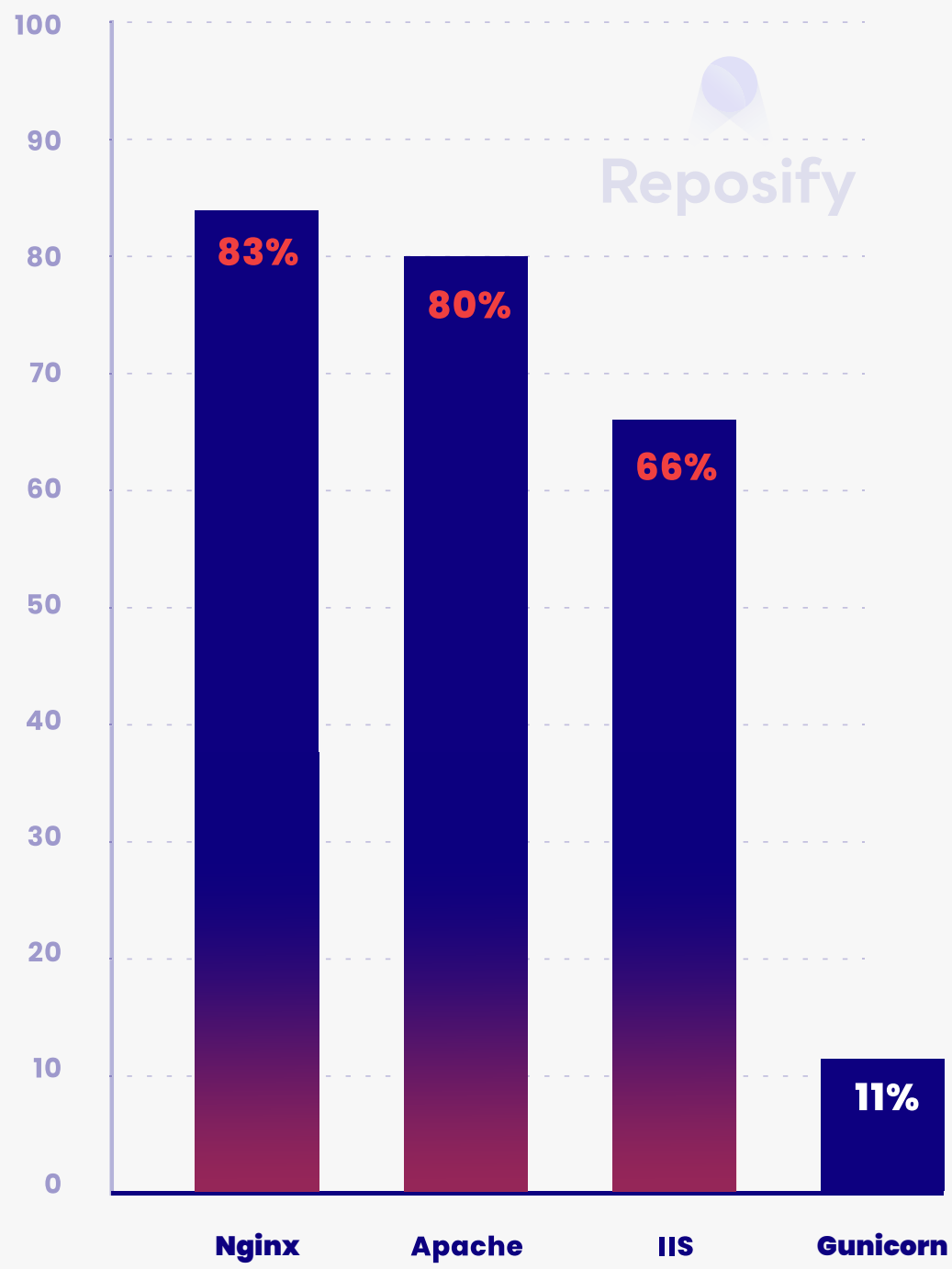


Exposed Web Servers

Web server vulnerabilities are continually changing. SQL Injection, Cross-Site Scripting (XSS), Distributed Denial of Service (DDoS) or Cross-Site Request Forgery (CSRF) are just a few methods attackers use to infiltrate web servers, but as digital solutions become more sophisticated, so will the means of attack.

- Reposify found that **Nginx** (83%) and **Apache** (80%) were the most common web servers with exposed assets.
- Closely following them was **internet information services (IIS)**, with 66% and **Gunicorn** with a significantly lower 11%.

Percent (%) of companies with exposed web servers - TOP 4 sensitive web servers



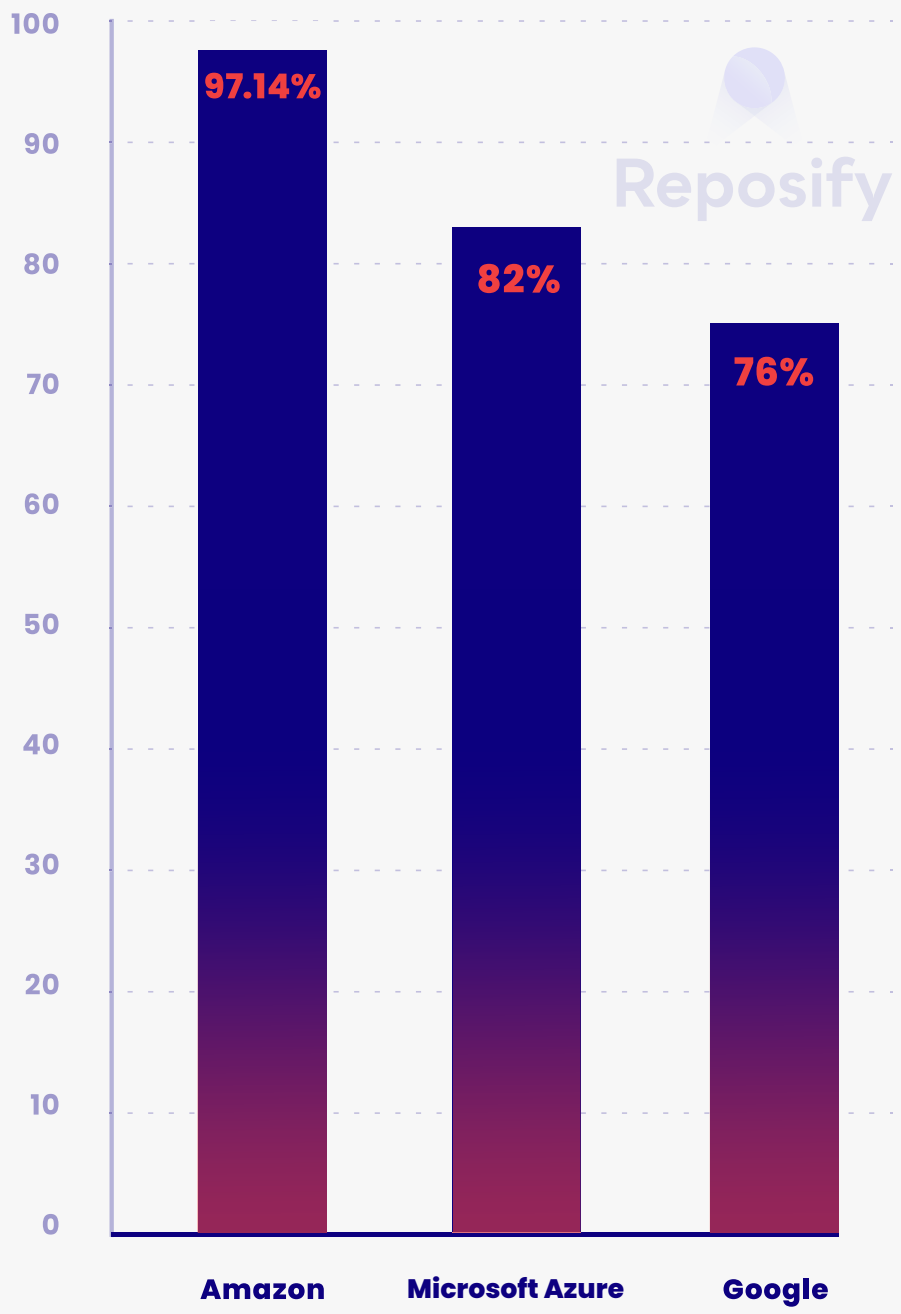
Common Cloud Providers with Exposed Assets

Though cloud computing has come under fire for its associated cybersecurity risks, the market is projected to hit $791.48bn USD by 2028, spurred on by demand for real-time information from any location, the integration of big data, AI and ML, and cloud-based solutions becoming the norm during the pandemic. Key players in the space include: AWS, Oracle, IBM and Microsoft Corporation, among others.

Reposify analyzed the top cloud providers to assess the number of cybersecurity companies with exposed assets in the cloud, with critical findings.

- Nearly all – 97.14% – of cybersecurity companies hosted exposed assets in **Amazon Web Services (AWS)** Cloud platform.
- **Microsoft Azure** followed with 82%, and **Google** coming in with 76%.

Percent (%) of companies with exposed cloud assets per each cloud provider

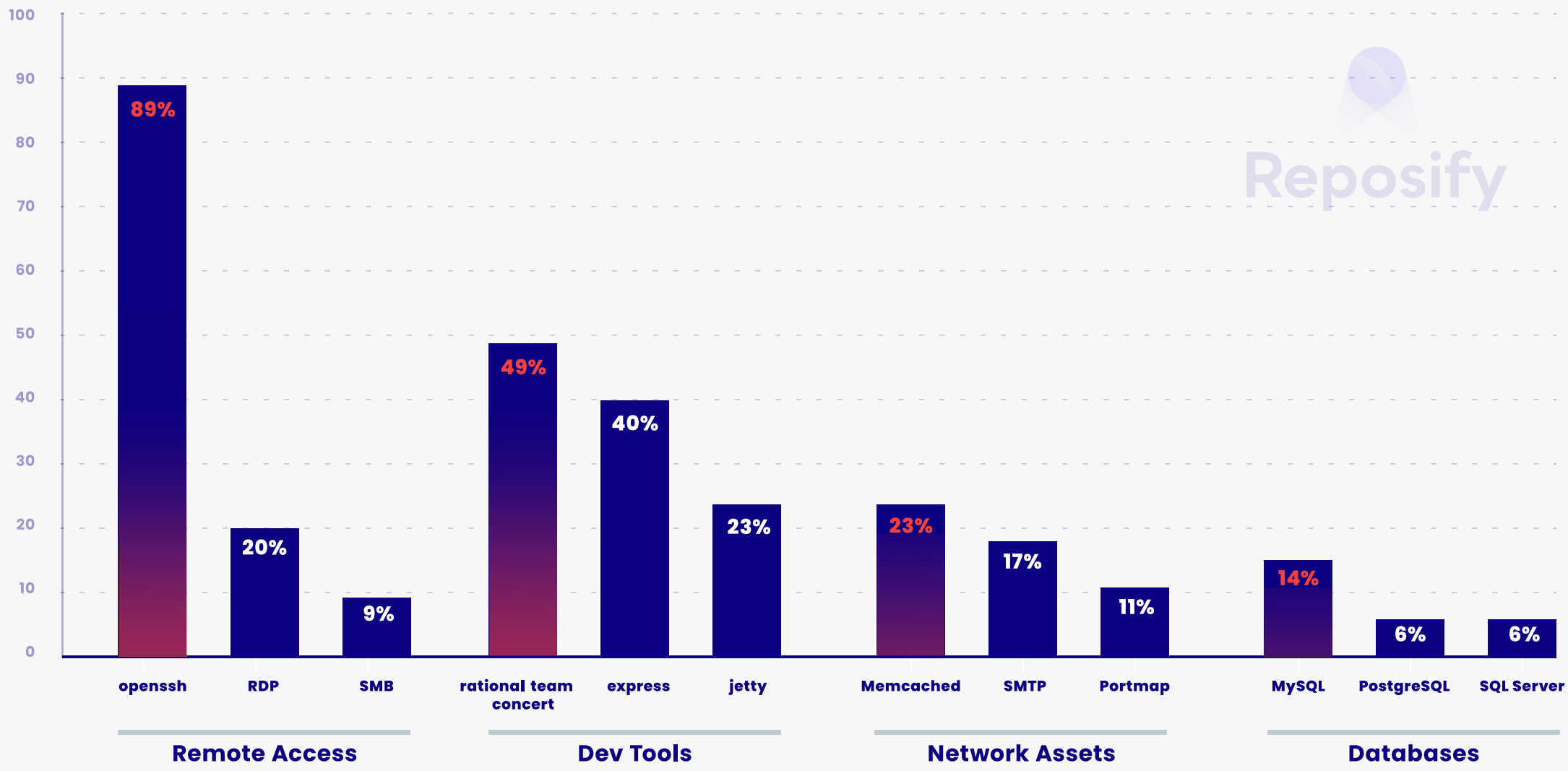


Common Exposed Services & Categories in Cloud Environments

Further analysis of the top three cloud providers with vulnerabilities revealed the most exposed asset categories and platforms. Reposify focused on the following categories: databases, development tools (eg. express, Jetty, RDi/IBM Rational), internal network assets (eg. memcheshed, portmap), remote access (eg. openSSH, RDP) and storage and backup (FTP).

- As seen in the exposed remote access category, **OpenSSH** saw 89% of cybersecurity companies with exposed assets. **RDP** and **SMB** followed with 20% and 9% respectively.
- Under network assets, **Memcached** saw 23% of companies hosting exposed assets, followed by **SMTP** at 17%, and **Portmap** with 11%.
- Development Tools on the cloud were also vulnerable, with **rational team concert** hosting 49% of exposed assets, express with 40% and **Jetty** with 23%.
- Finally, databases **MySQL** saw 14% of cybersecurity companies exposed, followed by **PostgreSQL** and **SQL** Server with 6% each.

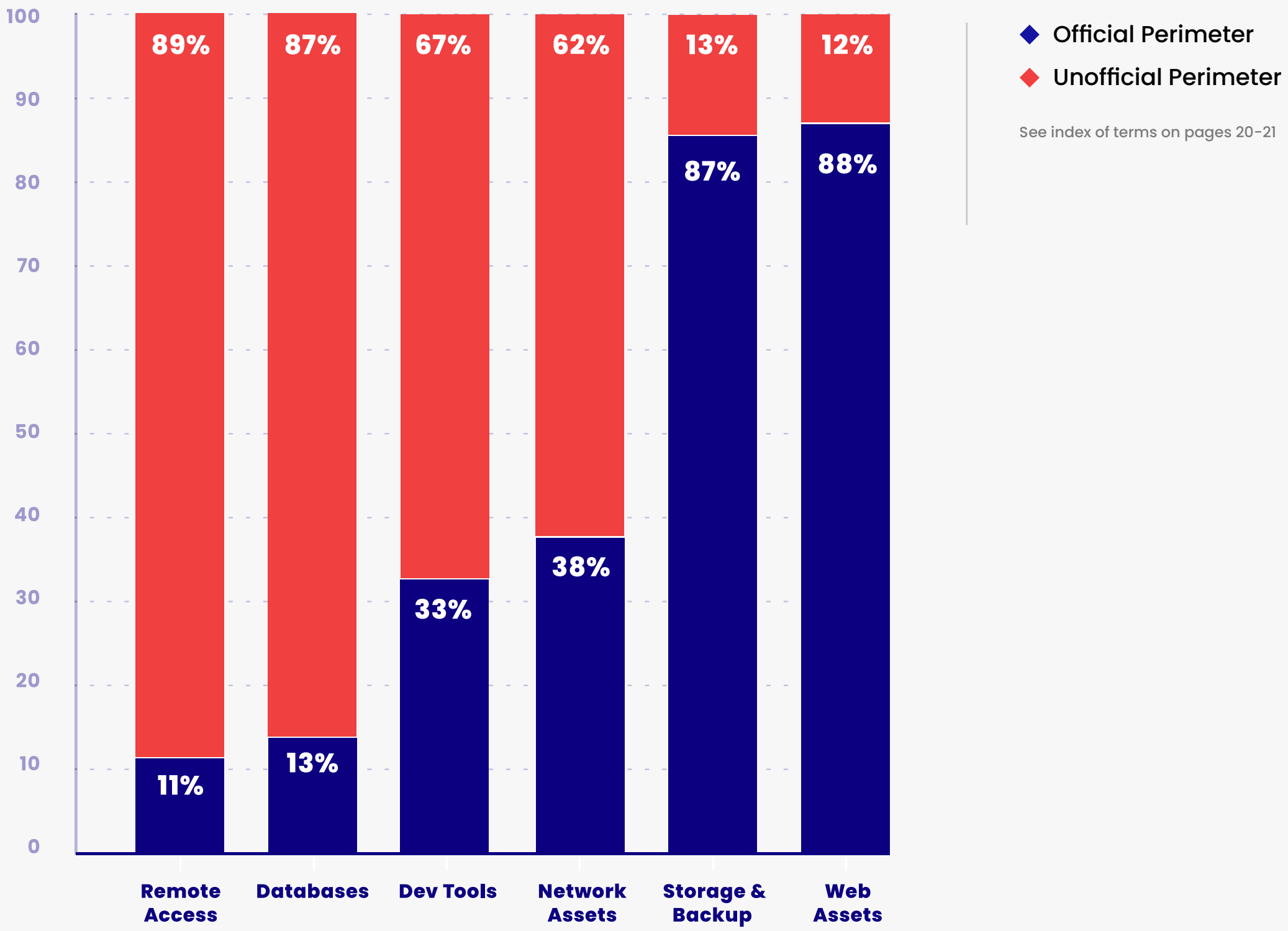
Percent (%) of companies with Exposed Services & Categories in Cloud Environments



Known vs. Unknown Exposures

To gauge companies' awareness of exposures, Reposify analyzed the distribution of services across the network perimeter using it's advanced artificial intelligence technology. This determines if services are attributed to known or unknown network perimeters. Services under known perimeters are likely to be on a security teams' radar, and therefore will be periodically monitored. Services under unknown perimeters are less likely to be known, and often represent shadow IT, unknown risks, or flag a possible backdoor malactors can use to access a company's assets.

Distribution of services across official & unofficial perimeter - selected asset categories



See index of terms on pages 20-21

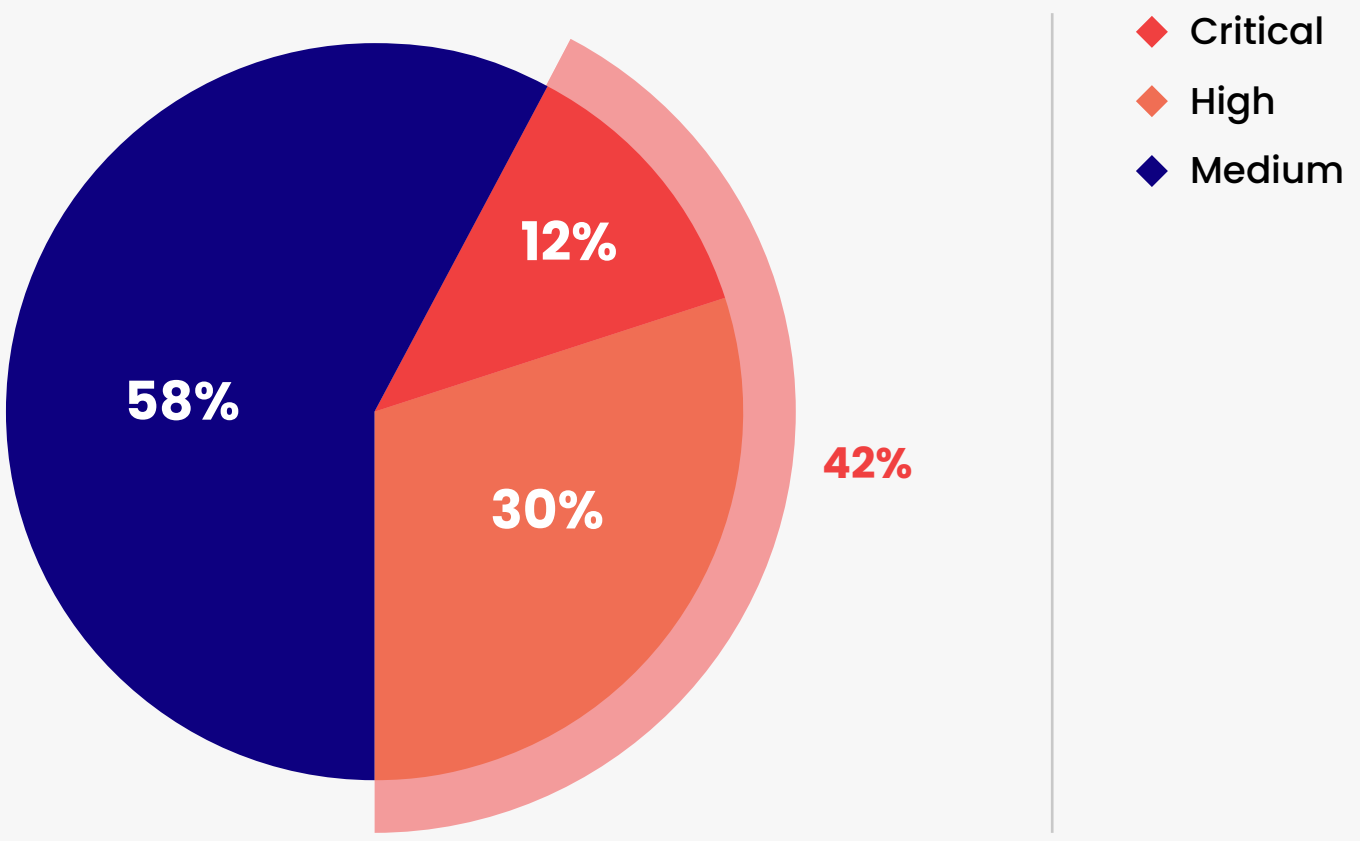
Risk Overview

Reposify's research team analyzed the prevalence of key risks which are visible from an external point of view, and could be leveraged by potential attackers. These risks include known vulnerabilities, like misconfigurations and human error.

Various security issues were identified – ranging from low- and medium-severity (eg. highly complex low exploitation probability or lower risk issues) to critical severity (eg. potential remote code execution). Reposify gathered data over a period of two weeks (January 2022) for this report, during which 258.2 million exposed assets were discovered across all industries.

30% of issues discovered by Reposify's platform were categorized as high severity, and 12% as critical severity. Meanwhile, 58% of issues discovered were categorized as medium severity.

All security issues discovered (by risk severity: medium, high-critical)

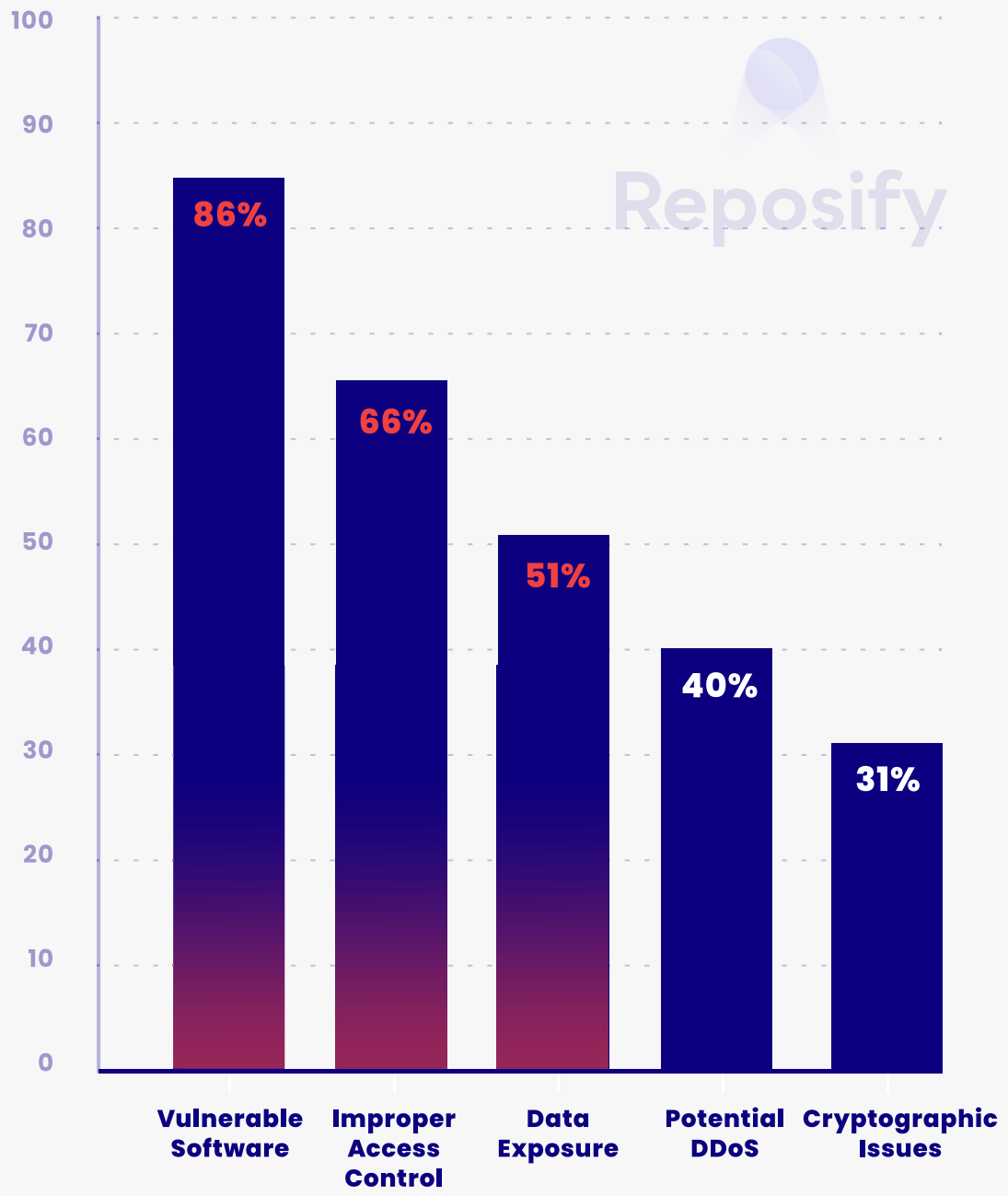


* Findings refer to actual systems with public IP exposed meaning having actual exploitation possibilities and it's distribution over the scanned systems/assets

High & Critical Security Issues

Reposify analyzed the number of services affected by security issues with high and critical CVSS scores. Vulnerable software and improper access control issues were the most common issue categories.

Percent (%) of security companies with open CVEs (per issue category)



Implications & Recommendations

The cybersecurity industry has done an incredible job of protecting its clients. Now, the industry must pay that same attention to themselves. Companies are embracing digital transformation, moving to cloud-based services, encouraging employees to work from home and often use mobile phones to access work email, documents and servers. These changes represent incredible opportunity - but also incredible risk as unknown assets multiply and hackers become more sophisticated in their methods of attack.

As analyzed in this report, exposed assets can be found across development tools, cloud service providers, web servers, databases and remote access platforms – all of which can be used by malactors as an entry point. **Cybersecurity companies must harden their security to make it more difficult for attackers to gain a foothold in their systems, beginning with a clear view of their external attack surfaces and continuous monitoring and elimination of risky attack vectors.**

External attack surface management (EASM) tools provide these services seamlessly. Defined in the Hype Cycle for Security Operations, 2021 Gartner Report as “the processes, technology and managed services deployed to discover internet-facing enterprise assets and systems and associated vulnerabilities.” EASM is the sum of all digital doorways into an enterprise, and is critical to any enterprise cybersecurity management strategy.

In addition to identifying known and unknown assets, EASM goes one step further by evaluating and analyzing assets to determine high risk or vulnerability, and prioritizing based on this risk assessment. Now, CISOs can use EASM for actionable insight to determine where further investment is needed to improve overall security posture.

In this report, Reposify uncovered that nearly 100% of companies analyzed host vulnerable assets on Amazon Web Services. Over half of security companies have at least one exposed database, which could lead to millions in damages and insurmountable data loss or leakage. Meanwhile, 86% of companies have exposed remote access services, reinforcing the need for more thorough cybersecurity management as the workforce shifts to the home environment. **Just one of these statistics is concerning enough – but the combination points to a sincere need for the industry to better practice what it preaches.**

About Reposify

Reposify is the leading External Attack Surface Management (EASM) provider. By mapping the web in real-time, 24/7, Reposify enables security teams to discover and eliminate unknown exposures and shadow IT risks across all environments with no agents or deployment required. Reposify delivers an up-to-date view of a company's exposed asset inventory, analyzes and prioritizes every asset and generates a plan with actionable insights so teams can resolve more issues in less time.

Leading enterprises worldwide use Reposify to protect their digital footprint and eliminate shadow IT risks in real-time.

Reposify is a Gartner Emerging Vendor in the EASM space.

Let's Connect:

www.reposify.com

info@reposify.com

Reposify

Appendix - Index of Terms

- **Attack Surface**

  Any software, application, or network has an attack surface which is the sum of all points where unauthorized users can try to access the data or steal it from that certain IT environment.

- **Cyber Risk**

  Cybersecurity risk is a potential exposure of an IT network or a system environment that can result in extensive harm to critical assets or loss of sensitive data within an organization's network.

- **External Attack Surface**

  The external surface is any exposed server or IoT device with a public-facing IP address, related to your organization that potential attackers could leverage to break into a network, gain access to corporate data and use your resources without authorization.

- **External Attack Surface Management**

  'EASM' solutions are specially designed for organizations to gain instant visibility into all of the IT network exposed assets and its security posture with real-time and ongoing discovery of unknown risks and exposures. EASM solutions provide the ability to get an always up-to-date view of all your assets allowing organizations to fully maximize the current tools used by the organization.

- **Known Assets**

  Assets an organization knows about, manages, and monitors on a daily basis. It includes servers, web-facing applications, and other services. These assets are usually used on a daily basis.

- **Official Perimeter**

  Official perimeter or registered perimeter is an IP address that is publicly known and registered to your organization's IT network. The official perimeter is part of an organization's asset inventory, which holds the current exposed services of a specific network.

- **Security Breach**

  Any incident that results in a sort of unauthorized access to network data, application, or device is called a security breach. This means that secure information can be intentionally or unintentionally accessed.

- **Shadow IT**

  Implemented resources or applications that are unknown or unapproved by the IT department within the organizations' network, is called Shadow IT. These assets refer to computer services, hardware devices, or cloud services of any kind that were installed inside the IT environment of an organization without the IT division knowing about its existence.

- **Unknown Assets**

  A major part of an organization's "unofficial perimeter". These assets are not part of the organization's formal external profile. Here you may find various test servers, IoT devices, login pages, and temporary services that are exposed either by accident, misconfiguration (often default settings), or by human error, for example, a user forgetting to take them down when deprecating or replacing them with newer services.

- **Unofficial Perimeter**

  Every exposed server and IoT device which are not being marked as official and recognized by an organization as official will be identified as part of its unofficial network perimeter. Inside the unofficial perimeter are assets like shadow IT-related services, phishing sites, and staging environments.

- **Vulnerability**

  Vulnerability refers to any weakness a computer system or a network has that can be exploited by hackers/ cybercriminals in order to gain illegitimate access and compromise sensitive data. Once organizations are familiar with its vulnerabilities, security teams must work fast to patch them or face potential cyberattacks.

- **Vulnerability Management**

  Vulnerability management is the process performed for identifying, classifying, prioritizing, and reporting security software vulnerabilities. Vulnerability management is a proactive approach of looking for weaknesses by scanning networks and identifying vulnerabilities and providing remediation suggestions to mitigate the potential of security breaches so organizations can stay ahead of attackers.