2023

UNIT 42
ATTACK SURFACE
THREAT REPORT

Lessons in Attack Surface Risk
Based on Observable Data

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Modern organizations are racing to update their enterprise network architectures to take advantage of Zero Trust security designs, cloud computing, software-as-a-service (SaaS) value delivery, and distributed workforces. This has fueled a dramatic increase of infrastructure, known and unknown, which in turn has greatly increased the complexity of securing their environments.

Exposures on publicly facing assets put them at risk of being compromised, and sometimes this leads to organizations becoming victims of opportunity as opposed to a targeted attack. Understanding what you need to protect is a precursor to any successful cybersecurity program — but companies and government agencies struggle to understand what they own and what services expose the most risk.

To put these sweeping changes into context and provide actionable intelligence, Unit 42 analyzed several petabytes of public internet data collected by Cortex Xpanse — the Palo Alto Networks attack surface management solution — in 2022 and 2023. This report outlines aggregate statistics about how attack surfaces worldwide are changing and drills down into particular risks that are most relevant to the market.

01

Key Findings

- **Constant change in the cloud creates new risk.** Cloud-based IT infrastructure is always in a state of flux. In a given month, an average of 20% of an organization's cloud attack surface will be taken offline and replaced with new or updated services. The deployment of these new services is generally responsible for nearly half of the organizations' new high or critical cloud exposures every month.

- **Remote access exposures are widespread.** Over 85% of organizations analyzed had Remote Desktop Protocol (RDP) internet-accessible for at least 25% of the month, leaving them open to ransomware attacks or unauthorized login attempts.

- **Cloud is the dominant attack surface.** A vast 80% of medium, high, or critical exposures belonging to the organizations analyzed were observed on assets hosted in the cloud.

Recommendations

Obtain continuous, comprehensive visibility
Maintain a complete and up-to-date inventory of your organization's assets both on-premises and in the cloud to ensure consistent application of governance policies.

Transform your vulnerability mindset
A lot of security breaches involve exposures due to issues such as misconfigured services, misconfigured firewalls, or even known vulnerabilities. Legacy vulnerability management processes fail to identify many of these issues, much less assist your organization in resolving them.

Enable your team to respond quickly to emerging threats
When critical vulnerabilities arise, quickly understand your risk exposure for patch prioritization and mitigation of unpatchable end-of-life services.
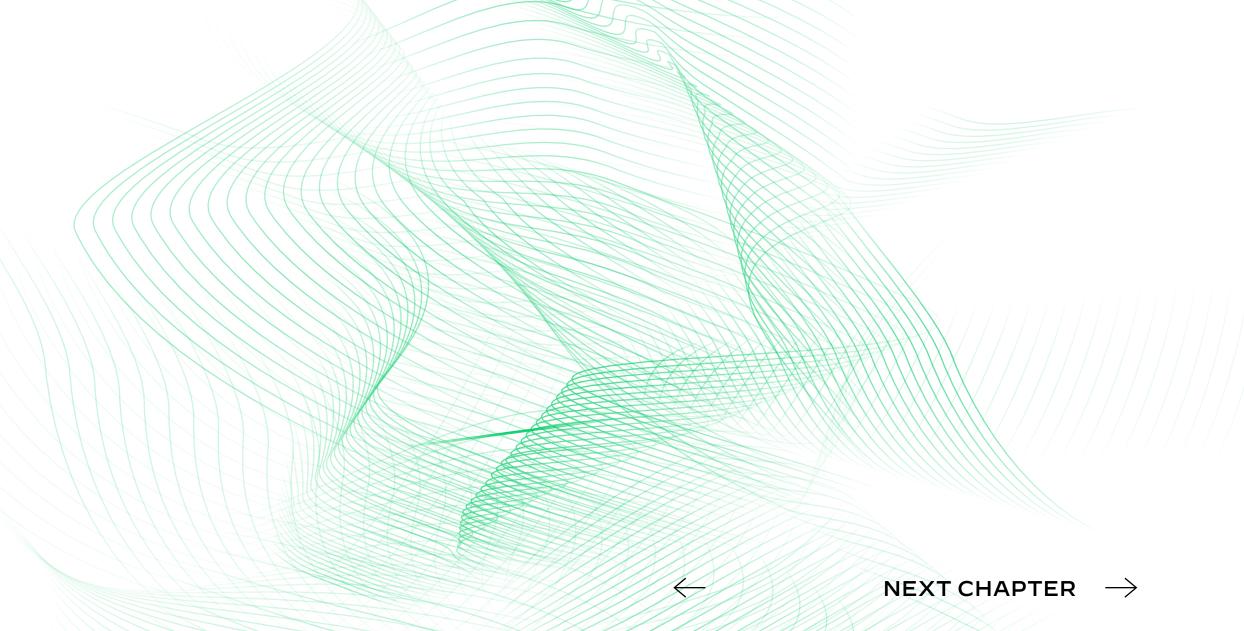
Monitor remote access services
Monitor all remote access points and usage to eliminate the risk of unauthorized logins.

Manage your attack surface at machine speed
Attackers are utilizing automation to move at machine speed. It's critical that your organization is able to move at machine speed as well by leveraging attack surface management tools which provide proactive prioritization and enable automatic remediation of common exposures.

Your security teams face challenges in attack surface management, including understanding current threats, maintaining a comprehensive asset inventory to avoid unknown risks, and quickly addressing all risks on those assets. Any exposure or vulnerability in an internet-accessible system gives attackers an opportunity to harm your organization, causing downtime, data loss, financial setbacks, and potential brand reputation damage. By actively managing your attack surface, you proactively and automatically mitigate risks, staying a step ahead.

ATTACKERS MOVE AT MACHINE SPEED

Attack surfaces are constantly changing, making it difficult for security teams to secure them. Defenders must remain vigilant as every configuration change, new cloud instance, and vulnerability disclosure present an opportunity for attackers.

Today's attackers have the ability to scan the entire IPv4 address space for vulnerable targets in minutes.

As we will explore in this report, attackers have been observed exploiting vulnerabilities in the wild within hours of their public disclosure. According to **previous research**, we found that on average, an organization takes more than three weeks to investigate and remediate a critical exposure.[1] Even the largest, most-sophisticated, and best-resourced security teams struggle to remediate critical exposures as quickly as attackers can test and field new capabilities.

02

Exploit Intelligence Confirms the Need for Rapid Response

Unit 42 analyzed 30 Common Vulnerabilities and Exposures (CVEs) from May 2022 to May 2023 to characterize how quickly adversaries were able to begin exploiting them. Researchers selected these CVEs based on threat intelligence about exploitation activity. Figure 1 shows the selected CVEs. **Notably, three of the 30 vulnerabilities were exploited within hours of the CVE public disclosure.** Nineteen of the 30 vulnerabilities were exploited within 12 weeks of the public disclosure, highlighting the risks associated with incomplete and inconsistent patching programs.
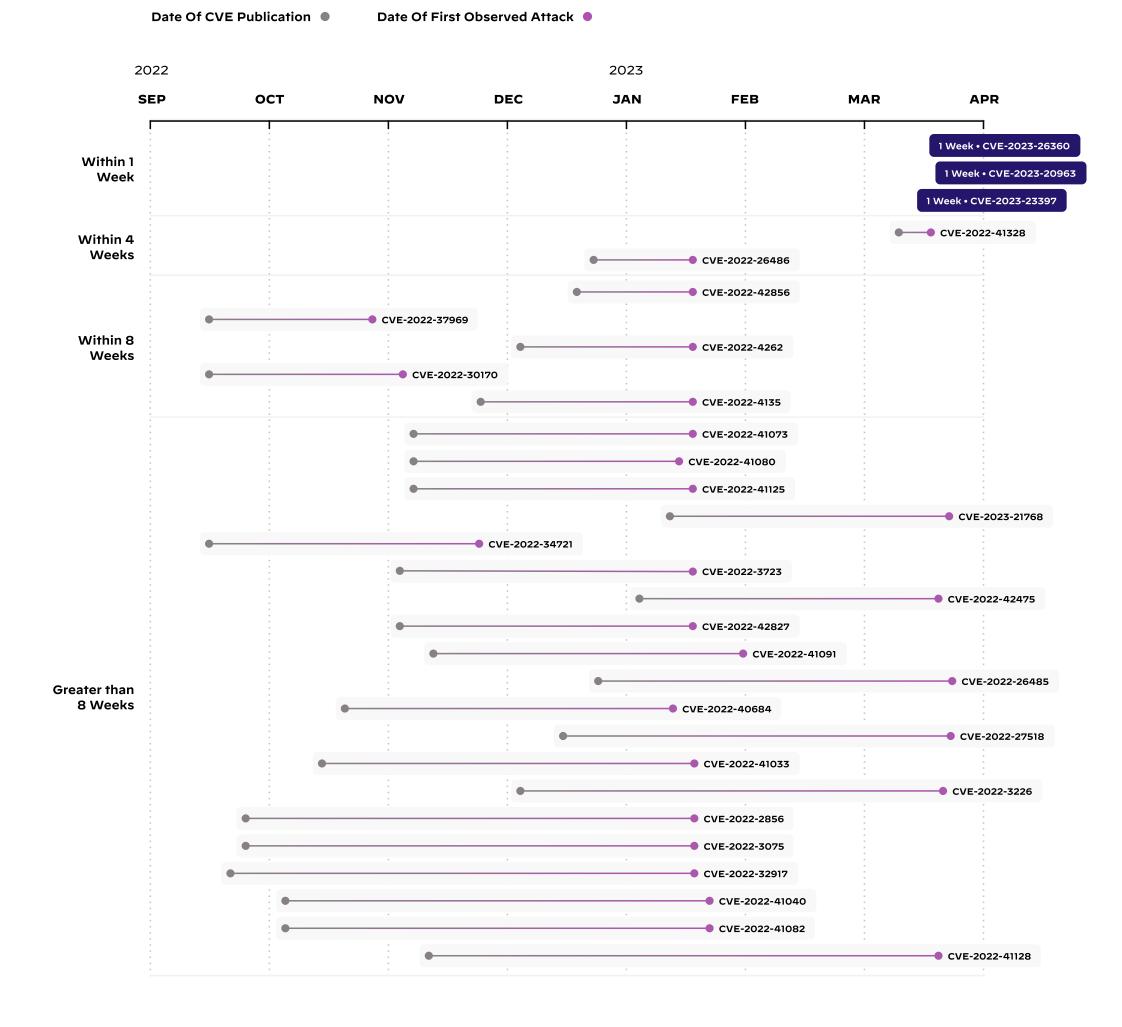
Date Of CVE Publication ●   Date Of First Observed Attack ●

Figure 1: Time elapsed before the first reported attack against 30 vulnerabilities exploited by a known threat actor in the last 12 months

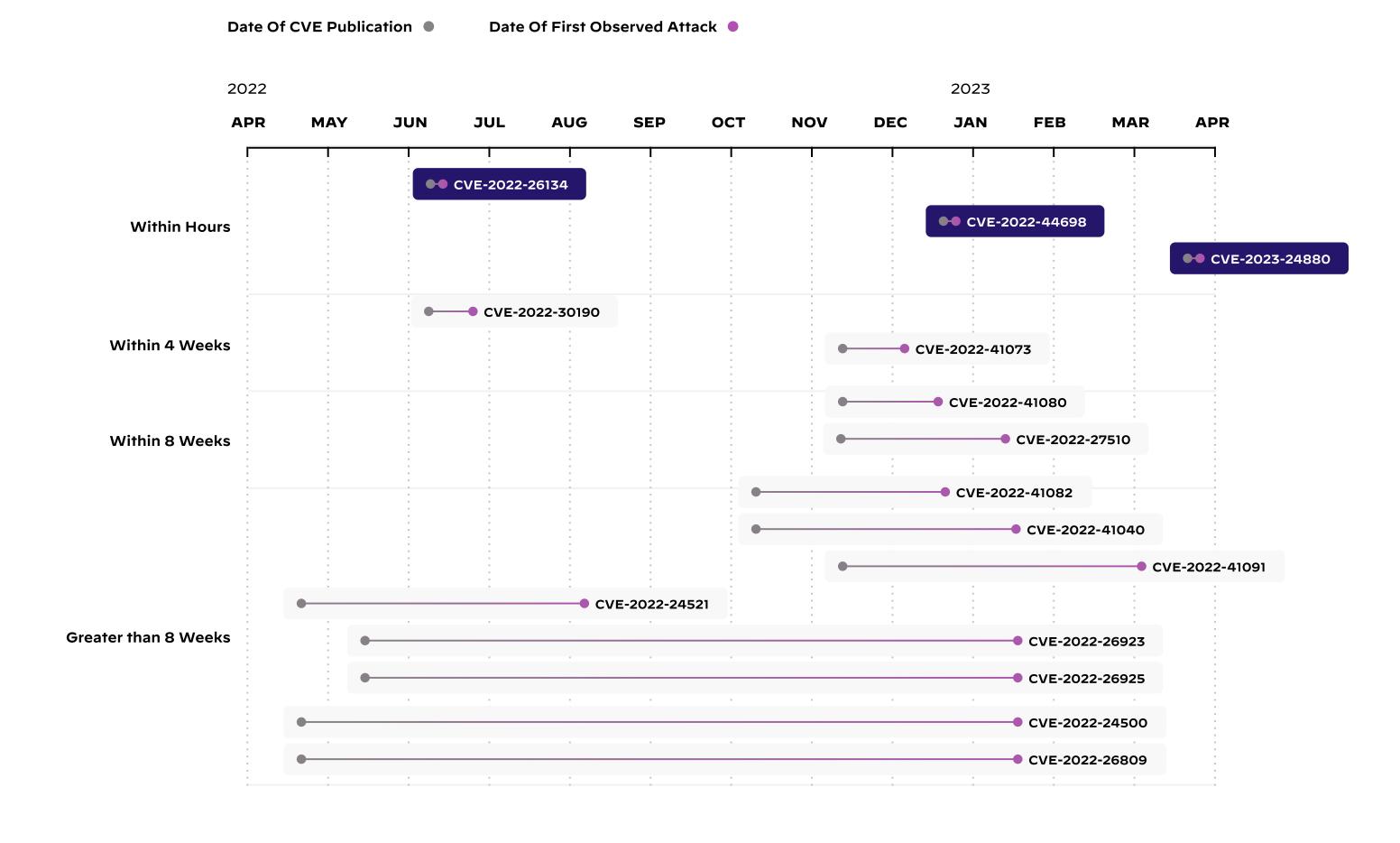**Date Of CVE Publication** ●   **Date Of First Observed Attack** ●

Figure 2: Time elapsed before the first reported ransomware attack against 15 RCE vulnerabilities by a known threat actor in the last 12 months

Ransomware Threat Actors Exploit Critical Vulnerabilities Within Hours of Publication

Unit 42 analyzed 15 remote code execution (RCE) vulnerabilities actively used by ransomware operators (shown in figure 2). These CVEs were selected based on intelligence information about the threat actor group and their active exploitation within 12 months of publication. **Threat actors targeted three of these critical RCE vulnerabilities within hours of disclosure**, and six of the vulnerabilities were exploited within eight weeks of publication.

TOP ATTACK SURFACE EXPOSURES

There are two broad categories of risks associated with the compromise of an internet-accessible asset for an organization:

1. Risks related to attacker actions taken on a compromised device that can directly harm the organization:

   - Examples include exfiltration of sensitive documents stored on an internet-accessible corporate laptop, ransomware attacks that disrupt payments processing, and physical damage from a compromised building control or industrial control system.

2. Risks related to how an attacker can leverage unauthorized access on a compromised attack surface asset to gain further unauthorized access to other organizational IT resources, including those not directly accessible over the public internet:

   - Examples include moving laterally across an internal subnet to exfiltrate data from a critical datastore, compromising virtual private network (VPN) infrastructure to access and infect source code repositories in supply chain attacks, and using a compromised IP security camera to record employees physically entering login credentials.

In general, when a device is compromised on the attack surface, it can pose both kinds of risks to organizations. Unit 42 categorized these risks according to the business function of a device, which relates strongly to the nature and severity of risk its compromise could pose to an organization. The total risk an attack surface poses to an organization is thus related to the volume of exposed assets vulnerable to compromise, the consequence of those assets being compromised, and the duration of time those assets are exposed relative to the time it takes attacker groups to find and exploit them.

03

Web framework takeover exposures, as mentioned in figure 3, make up 22% of exposures observed across the 250 organizations; attackers actively seek out and target websites running vulnerable software because they are so prevalent. The most common exposure types were insecure versions of Apache web servers, insecure versions of PHP, and insecure versions of jQuery.

Remote access services account for 20% of exposures. These exposures include services like RDP, Secure Shell (SSH), or virtual network computing (VNC). When compromised, these services allow attackers to gain unauthorized access to an organization's network or systems, potentially leading to financial losses, reputational damage, or other consequences. In addition, RDP has been shown to be a leading vector for business interruption via ransomware.

Web Framework Takeover
22.8%

Remote Access Services
20.1%

Unencrypted Logins and Text Protocols
2.1%

IOT, Embedded Devices, and OT
3.6%

Weak or Insecure Cryptography
5.5%

Unpatched, Misconfigured, and End of Life (EoL)
5.5%

Databases
9.5%

File Sharing
12.1%

IT Security and Networking Infrastructure
17.1%
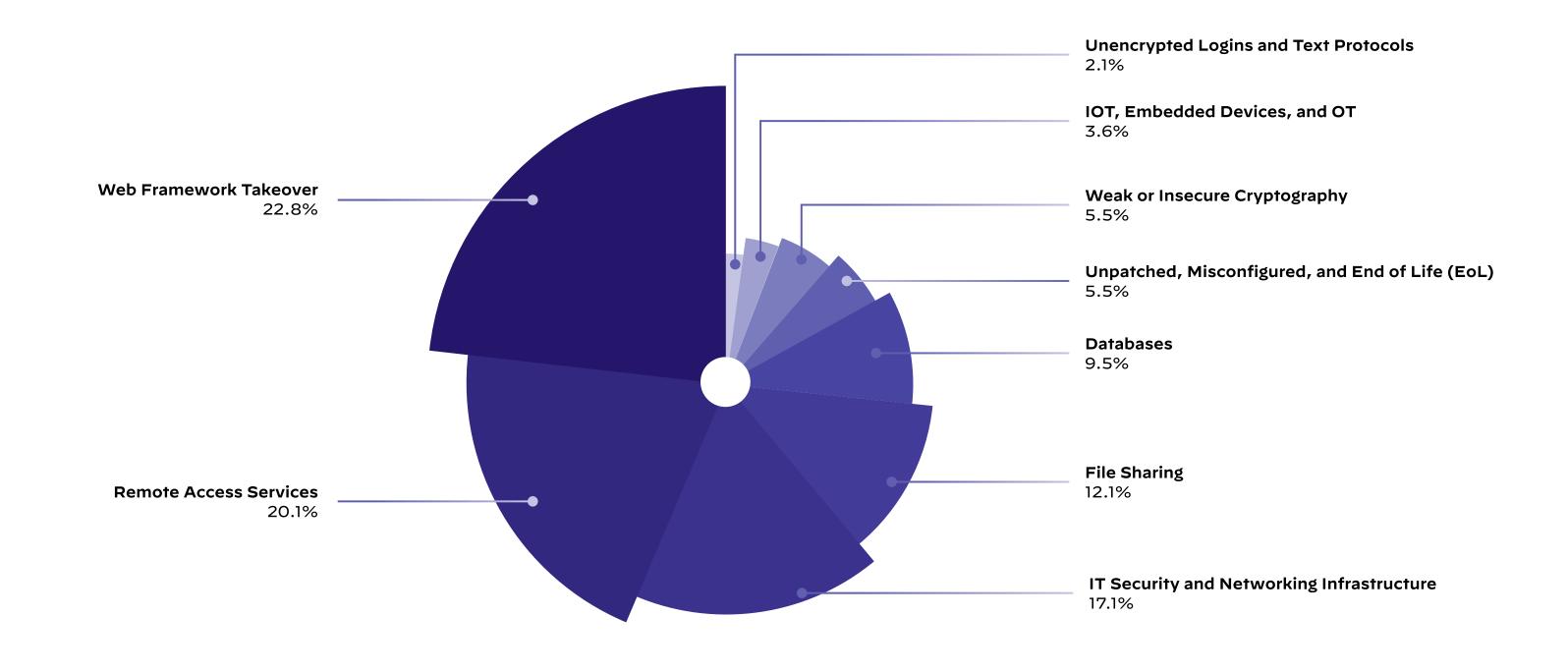
Figure 3: Distribution of exposure categories observed across the 250 organizations in the last 12 months

IT and networking infrastructure exposures comprise 17% of exposures that Unit 42 observed. Exposures in this category include application-layer protocols like Simple Network Management Protocol (SNMP), NetBIOS, Point-to-Point Tunneling Protocol (PPTP), and internet-accessible administrative login pages of routers, firewalls, VPNs, and other core networking and security appliances. Compromise of these assets can have substantial consequences for organizations, including the compromise of core business functions and applications, and the data they contain.

File sharing exposures account for 12% of exposures and pose significant risks to organizations, including data breaches. Examples of insecure file sharing include publicly accessible file-sharing services, FTP, and misconfigured cloud storage. Compromise of these systems allows attackers not only access to the data stored on them but also all future data sent through them.

Database exposures and vulnerabilities make up 9% of exposures observed across the 250 organizations. Exposing a database with sensitive information directly to the internet can dramatically increase the probability that your organization experiences a data breach.

Unit 42 also observed other types of exposures, including:

- Unpatched, misconfigured, and EoL systems

- Weak or insecure cryptography

- IoT, embedded devices, and operational technologies (OT)

- Unencrypted logins and text protocols

- Development infrastructure

- Business operations applications

- Medical systems

REMOTE ACCESS EXPOSURES LEAD TO RANSOMWARE

According to the **2022 Unit 42 Incident Response Report**, the top suspected means of initial access for ransomware cases investigated by Unit 42 are software vulnerabilities (48%), followed by brute-force credential attacks (20%).[2] The heavy use of software vulnerabilities matches the opportunistic behavior of ransomware actors, who typically scan the internet at scale for vulnerabilities and weak points. This approach, along with brute-force credential attacks, focused on RDP.

04

NEXT CHAPTER →

Remote access services can be essential in today's hybrid work environment, but their misconfiguration can pose significant risks.

Figure 4 reveals that RDP is the most prevalent remote access service worldwide, accounting for over 40% of the exposed remote access services. The prevalence of remote access exposures on the overall public internet remains even when we focus on enterprise networks: 85% of organizations analyzed in this report had at least one internet-accessible RDP instance online during the month.
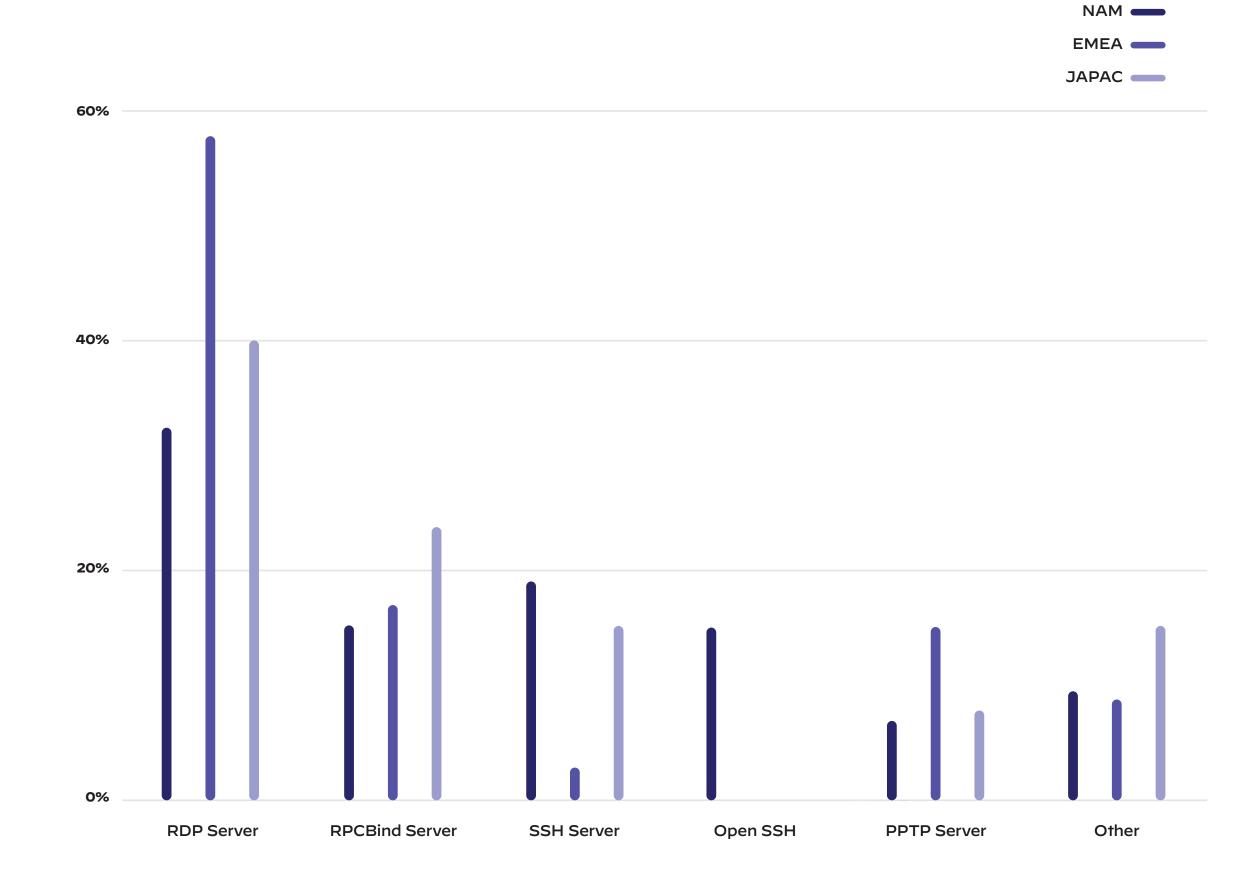

Figure 4: Top five most common exposed remote access services by geography in the last 12 monthss

NEXT CHAPTER →

Industry	Median number of unique RDP instances exposed to the internet over the last 12 months*	Median number of days an RDP instance was active and exposed to the internet in any given month*
High Technology	55	9
Manufacturing	54	9
Professional and Legal Services	92	4
Financial Services	55	30
Insurance	43	9
Healthcare	25	14
Wholesale and Retail	27	8
National Government	111	10
State and Local Government	46	30

* Note: Medians are calculated across organizations in each industry.

Table 1: The Frequency and Duration of RDP Exposures for the Median Large Organization in Each Industry

Unit 42 found that the average national government organization had internet-accessible RDP exposures for 10 distinct days in a month, providing attackers with ample opportunity to gain unauthorized access. The average professional services organization had RDP exposed for a shorter duration but tended to have more distinct instances of RDP exposed.

Eight of the nine industries that Unit 42 studied had internet-accessible RDP vulnerable to brute-force attacks for at least 25% of the month. The median financial services and state or local government organizations had RDP exposures for the entire month.

Across over 600 incident response cases, the **2022 Unit 42 Incident Response Report** found that 50% of targeted organizations lacked multifactor authentication (MFA) on key internet-facing systems. The prevalence of RDP exposures in each industry studied in this report, combined with the rarity of compensating controls like MFA, make it likely that ransomware attacks will continue for the foreseeable future.

CLOUD DYNAMISM IS STRAINING SECURITY CONTROLS

To assess the dynamic nature of modern IT environments, Unit 42 studied the composition of new and existing services running in different cloud providers used by an organization over a period of six months.

05

Cloud-based IT infrastructure is always in a state of flux— on average over 20% of externally accessible cloud services change every month across the 250 organizations, as illustrated in figure 5.

Without continuous visibility, it is easy to lose track of accidental misconfigurations and the steady spread of shadow IT within an organization.
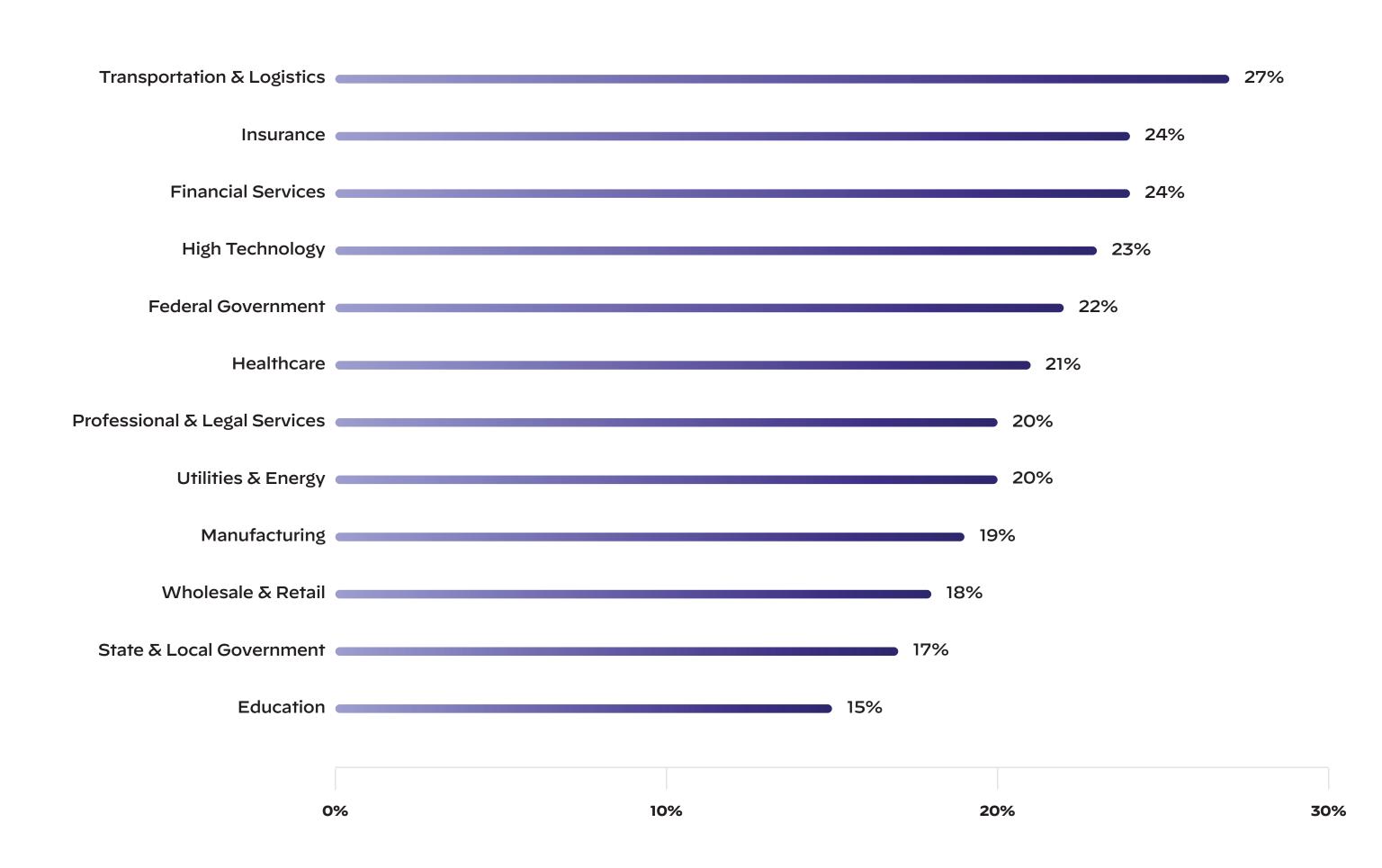
Industry	Percentage
Transportation & Logistics	27%
Insurance	24%
Financial Services	24%
High Technology	23%
Federal Government	22%
Healthcare	21%
Professional & Legal Services	20%
Utilities & Energy	20%
Manufacturing	19%
Wholesale & Retail	18%
State & Local Government	17%
Education	15%

Figure 5: Median proportion of new services introduced by a typical company in each industry during a given month

NEXT CHAPTER →

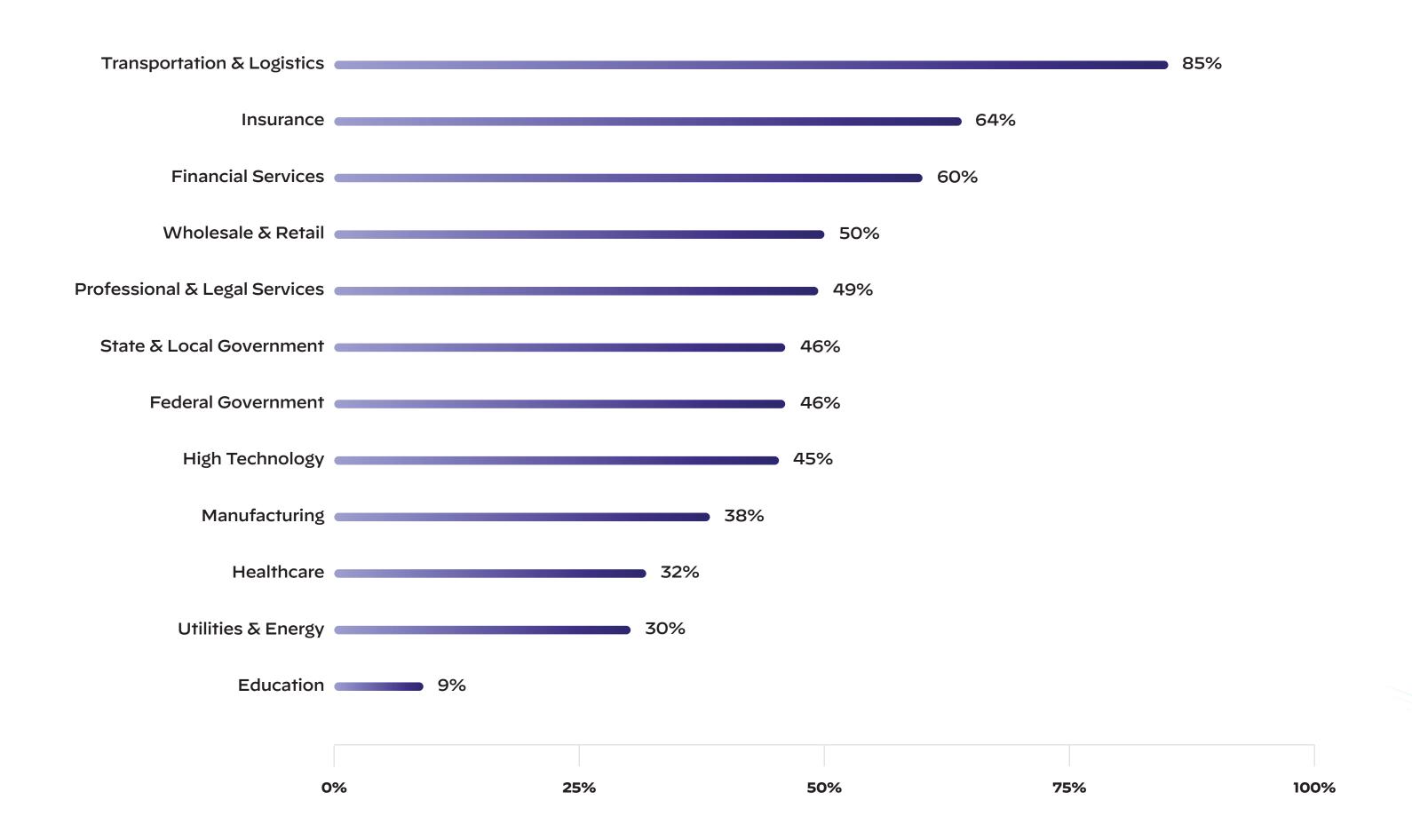| Industry	
Transportation & Logistics	85%
Insurance	64%
Financial Services	60%
Wholesale & Retail	50%
Professional & Legal Services	49%
State & Local Government	46%
Federal Government	46%
High Technology	45%
Manufacturing	38%
Healthcare	32%
Utilities & Energy	30%
Education	9%

Figure 6: Median proportion of cloud-hosted exposures that are high risk observed on a typical company's attack surface in each industry during a given month

Upon discovering that one out of every five cloud-based systems in an organization changes every month, Unit 42 investigated the impact on the number of new security risks introduced within an organization.

Figure 6 shows that, for most organizations, over 45% of their high-risk, cloud-hosted exposures in a month were observed on new services that were not present on their organization's attack surface in the prior month. Thus, the creation of new, publicly accessible cloud services, both intended and unauthorized, accounts for nearly half of all high-criticality exposures at a given time.

NEXT CHAPTER

CLOUD EXPOSURES DOMINATE MOST ORGANIZATIONS' SECURITY RISKS

Cloud deployments offer cost savings and operational efficiencies, but organizations must also be aware of security risks and take appropriate measures to secure their cloud environments.

06

NEXT CHAPTER →

According to our analysis,
80% of security exposures were
observed in cloud environments,
as shown in figure 7.

This higher distribution of exposures in the cloud can
be attributed to frequent misconfigurations, shared
responsibilities, shadow IT, inherent connection to the
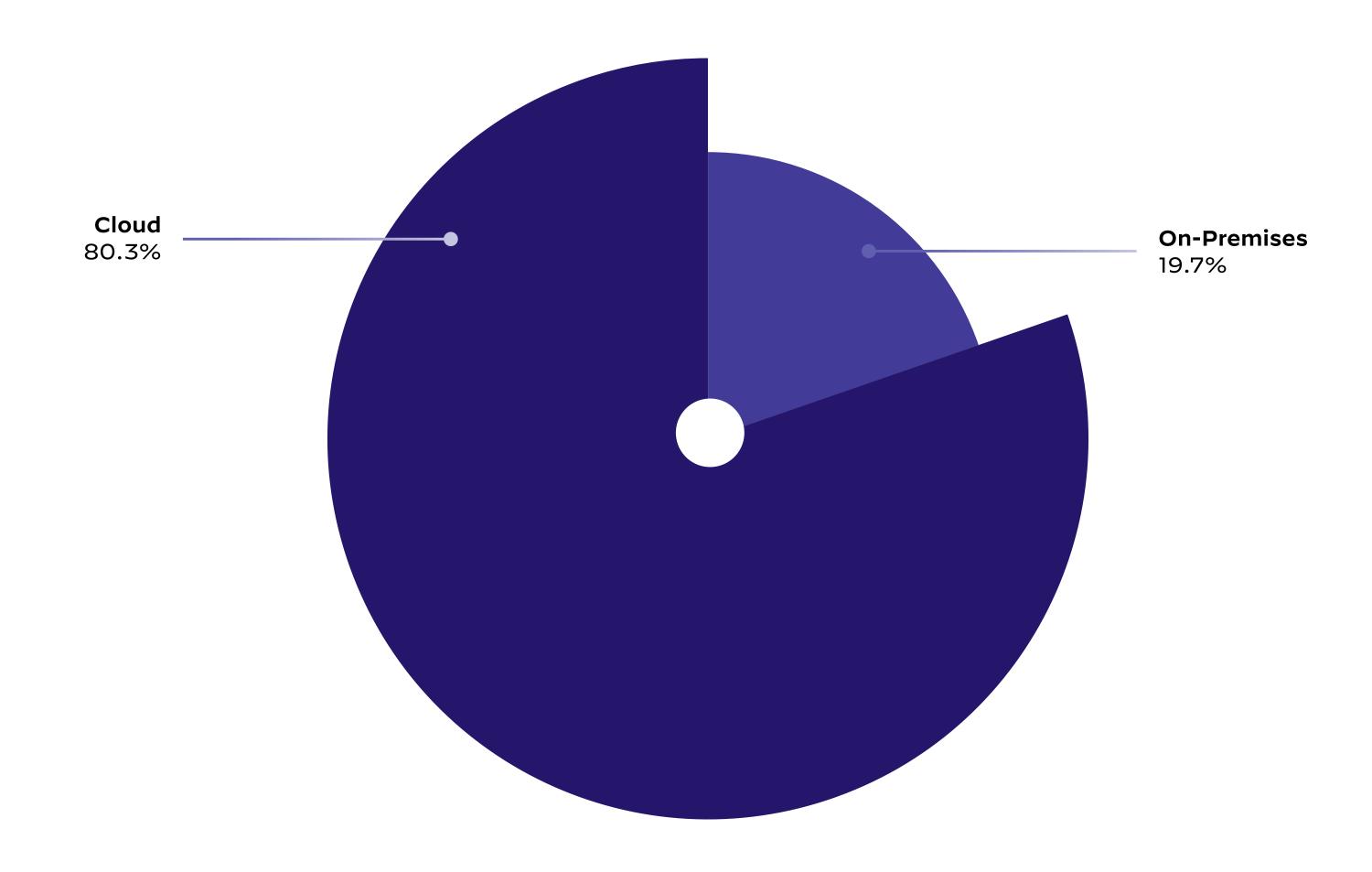internet, and lack of visibility into cloud assets.

Cloud
80.3%

On-Premises
19.7%

Figure 7: Distribution of exposures (Critical, High, Medium) in the cloud versus on-premises in 2022
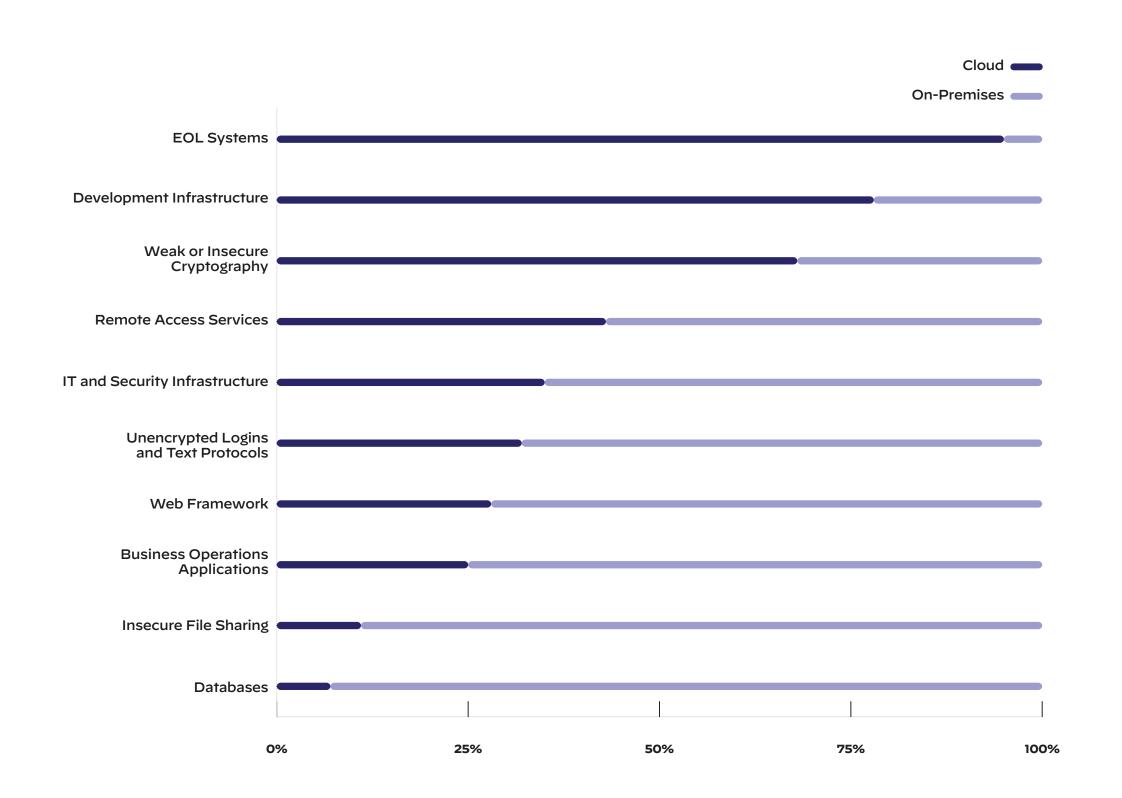
NEXT CHAPTER

Figure 8: Distribution of different categories of Exposures (Critical, High, Medium) in the Cloud vs. On-Premises in the last 12 months

As seen in figure 8, nearly 95% of EoL software systems exposed on the public internet of the organizations measured were found in cloud environments.

This suggests that organizations might be slower to retire outdated systems that are publicly accessible in cloud environments than on-premises ones, and also that it is comparatively easier for developers to create and deploy large volumes of new services with substantially outdated software in the cloud.

Similarly, over 75% of publicly accessible software development infrastructure exposures were found in the cloud, making them attractive targets for attackers.

Common exposures that are found primarily on-premises may inadvertently increase:

- 67% of unencrypted logins and text protocol exposures

- 89% of insecure file-sharingfile sharing exposures

- 93% of internet-exposed databases

While these exposures are being found primarily on-premises, organizations should be cognizant of these exposures when migrating sensitive data to the cloud.

Any of these exposures being accessible over the public internet is a cause for concern since they can act as a toehold for attackers to gain unauthorized access to an organization's network and access sensitive data.

INDUSTRY ATTACK SURFACE BREAKDOWN

Last year, Palo Alto Networks published the **2022 Cortex Xpanse Attack Surface Threat Report**,[4] which included a study of attack surface exposures in different industry verticals. In this year's report, Unit 42 provides an update for each sector, showing the frequency of exposures and explaining the potential consequence of a successful attack.
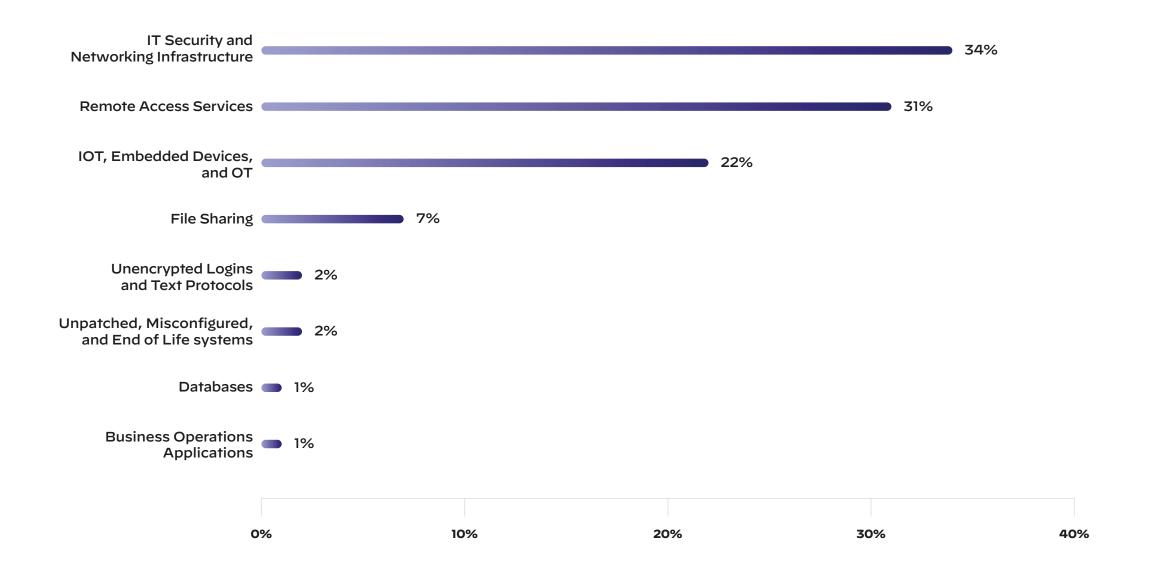
07

Figure 9: Median distribution of top exposures in the high-tech industry in 2022

High Technology

Unit 42 observed that high-tech companies are unintentionally exposing several login and/or admin pages of critical IT as well as security infrastructure, such as routers, switches, and firewalls, as shown in figure 9. If these assets are exploited successfully, attackers would have the same ability to control the environment as a member of an IT team. Compounding the risk, credential reuse is common on IT and security infrastructure, which means that attacks can be heavily automated and don't require an unpatched vulnerability to succeed.

Additionally, these companies rely heavily on remote access services, which amount to 31% of all the exposures for a typical company in this industry. This can be a significant attack vector due to accidental misconfigurations or inadequate

security practices. Insecure implementation of SSH servers is the leading contributor to remote access exposures in this industry.

High-tech companies are generally stronger at keeping publicly accessible web servers up to date. This is likely due to a correlation between having a strong digital presence related to revenue-generating operations and their security departments having better inventories of intentionally public-facing assets. Unfortunately, this does not extend to assets deployed as shadow IT or IoT devices with no associated DNS.

NEXT CHAPTER →

National Governments

The top exposures for national governments are related to data security and IT infrastructure. As shown in figure 10, file sharing and database exposures account for over 46% of all the exposures in a typical national government organization. Misconfigured critical IT systems and internet-accessible login and/or admin pages of routers, firewalls, VPNs, etc., were some of the common exposures found under this category.

Insecure file sharing and databases are one of the most significant attack surface risks in national governments, above the rates for other organizations.
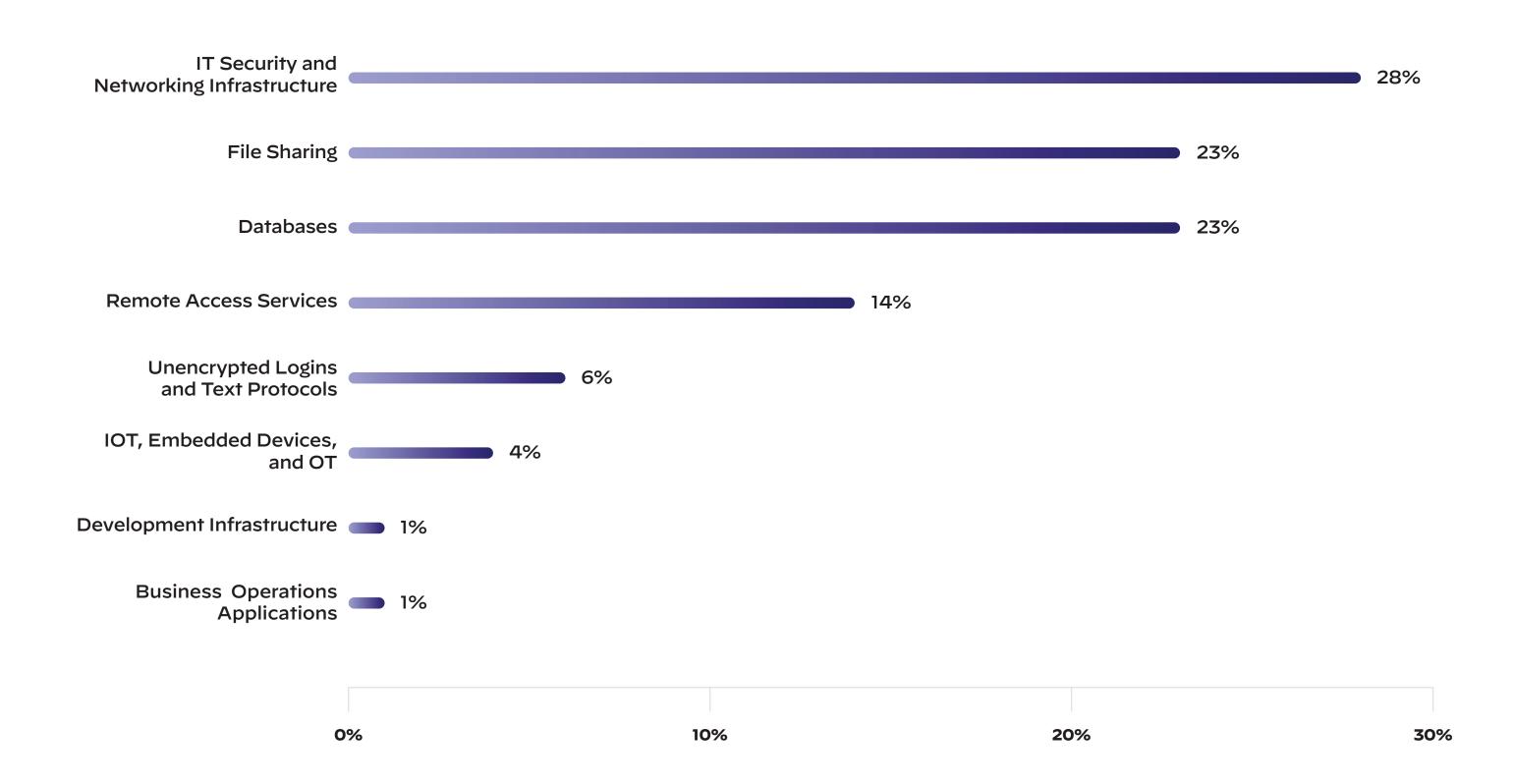
IT Security and Networking Infrastructure — 28%
File Sharing — 23%
Databases — 23%
Remote Access Services — 14%
Unencrypted Logins and Text Protocols — 6%
IOT, Embedded Devices, and OT — 4%
Development Infrastructure — 1%
Business Operations Applications — 1%

0%   10%   20%   30%

Figure 10: Median distribution of top exposures in national governments in 2022

NEXT CHAPTER →

Professional and
Legal Services

Unencrypted FTP servers are ubiquitous in professional and legal services organizations, as shown in figure 11, opening several avenues for data compromise. Additionally, the improper use of cloud-based data storage and analysis systems for business information processing, visualization, and analytics leads to accidental exposures that provide opportunities for attackers to steal critical information.

The higher rates of file-sharing exposures for this sector are especially concerning. As part of business operations, these organizations must send and receive large volumes of files from clients, necessitating a large number of file-transfer services to run their business. However, the sensitive nature of the files exchanged, combined with the number of exposed systems, makes targeting these systems especially valuable to attackers.
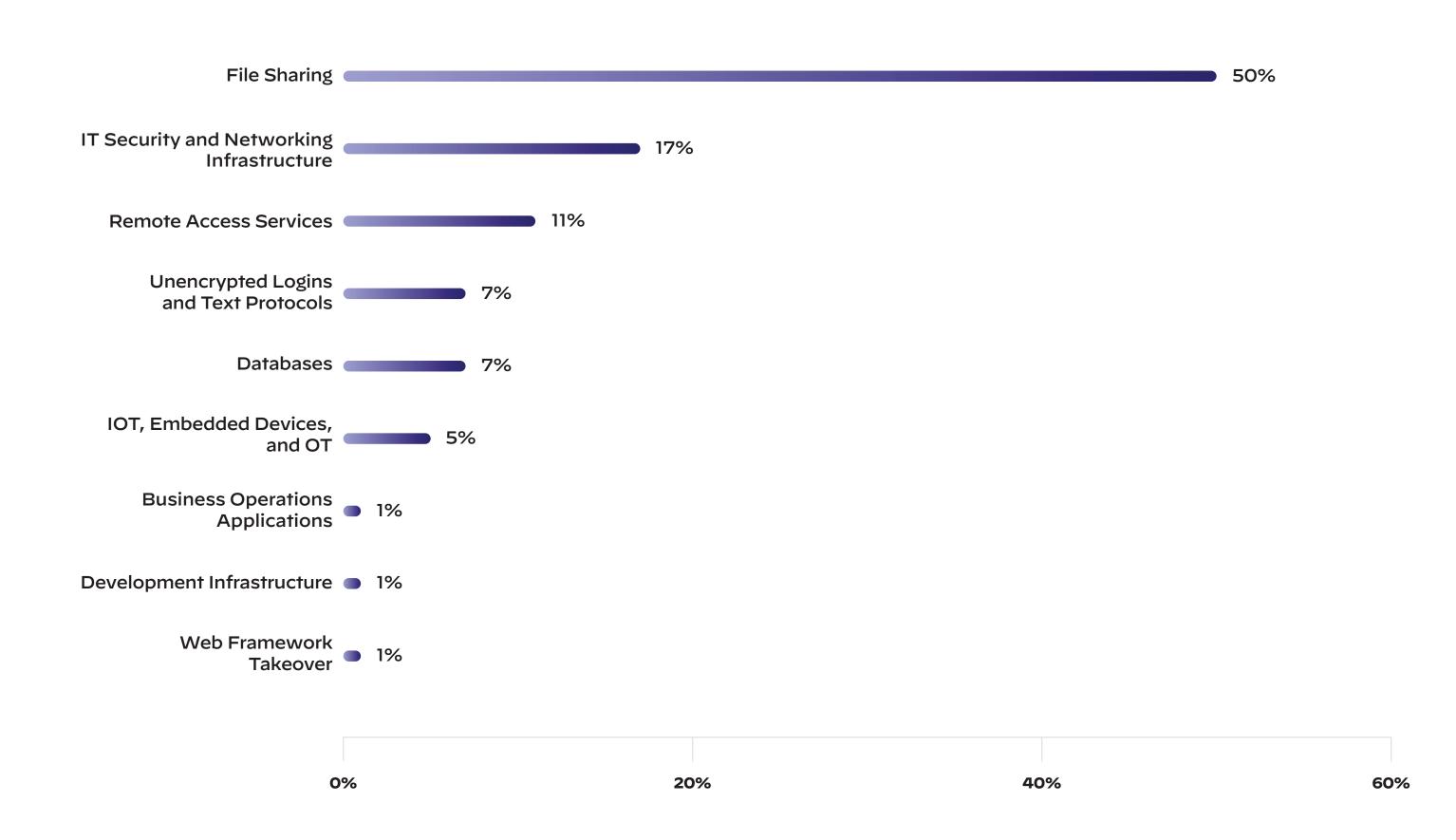
Category	Percentage
File Sharing	50%
IT Security and Networking Infrastructure	17%
Remote Access Services	11%
Unencrypted Logins and Text Protocols	7%
Databases	7%
IOT, Embedded Devices, and OT	5%
Business Operations Applications	1%
Development Infrastructure	1%
Web Framework Takeover	1%

Figure 11: Median distribution of top exposures in the professional services industry in 2022

NEXT CHAPTER →

Healthcare

As healthcare companies undergo digital transformations, it is essential that they keep sensitive data, like protected health information (PHI), secure. The high rate of publicly exposed development environments, which are often misconfigured and vulnerable, gives attackers an opportunity to establish a foothold in the organization's network. This access can lead to data breaches, unauthorized access, or even medical device failures, as shown in figure 12.
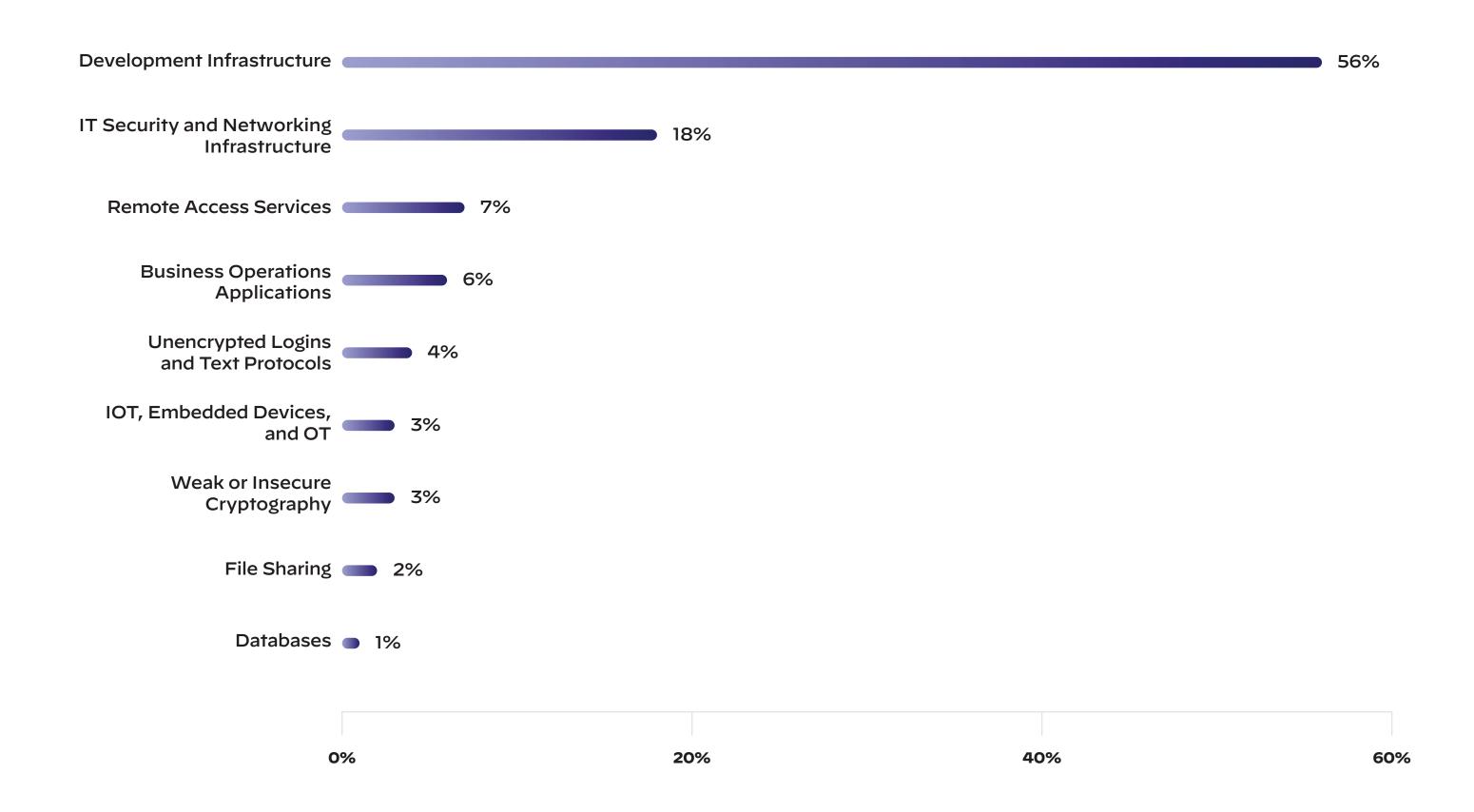
Development Infrastructure — 56%

IT Security and Networking Infrastructure — 18%

Remote Access Services — 7%

Business Operations Applications — 6%

Unencrypted Logins and Text Protocols — 4%

IOT, Embedded Devices, and OT — 3%

Weak or Insecure Cryptography — 3%

File Sharing — 2%

Databases — 1%

0%   20%   40%   60%

Figure 12: Median distribution of top exposures in the healthcare industry in 2022

Utilities and Energy

Internet-accessible IT infrastructure control panels account for nearly one out of two exposures in the utilities and energy sector, as shown in figure 13. RDP servers make up 11% of the exposures and are the leading cause of remote access exposures in this sector.

Particularly concerning is the elevated risk of IT networking systems that would allow attackers more direct access to the core, internal networks of these organizations. Even if the attackers are unable to cross to OT networks from IT networks, business interruptions on IT networks can still result in overall power and energy service disruption to the individuals and businesses that these organizations serve.
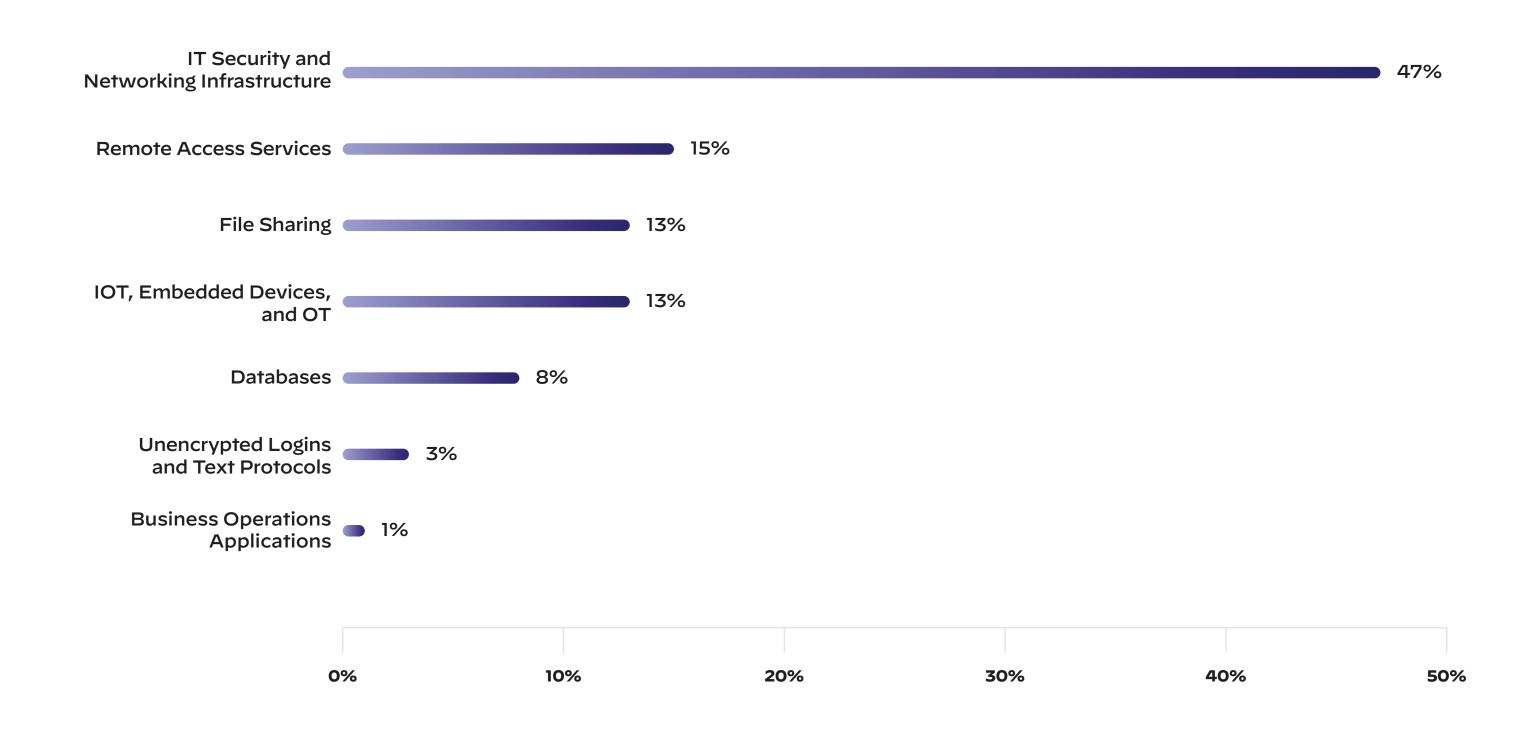

Figure 13: Median distribution of top exposures in the utilities and energy industry in 2022

NEXT CHAPTER →

Manufacturing

The most prevalent risks observed on the attack surface of manufacturing companies were IT, security, and networking infrastructure. By compromising core networks, attackers could cause significant operational disruptions, leading to production downtime, loss of revenue, andreputational damage with long-lasting effects.
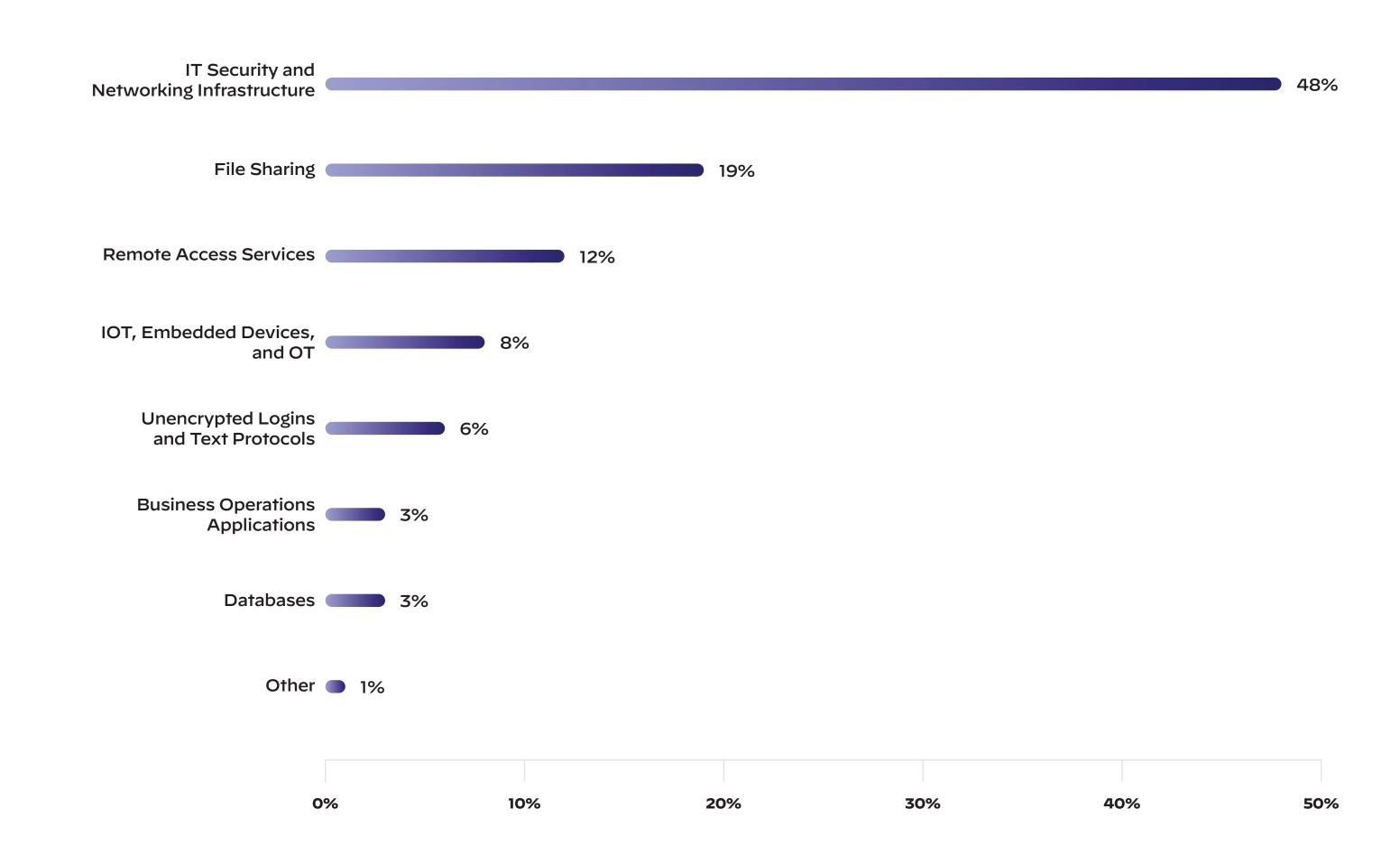
IT Security and Networking Infrastructure — 48%
File Sharing — 19%
Remote Access Services — 12%
IOT, Embedded Devices, and OT — 8%
Unencrypted Logins and Text Protocols — 6%
Business Operations Applications — 3%
Databases — 3%
Other — 1%

0%   10%   20%   30%   40%   50%

Figure 14: Median distribution of top exposures in the manufacturing industry in 2022

NEXT CHAPTER →

Education

Educational institutions were most likely to expose IT, security, and networking infrastructure, followed by file-sharing services and remote access services. Unit 42 also observed business operations applications and IoT at a higher rate than other sectors. Risky exposures like these can lead to a serious data breach, such as:

- The theft of sensitive personal, academic, and financial information.

- The disruption of essential educational services.

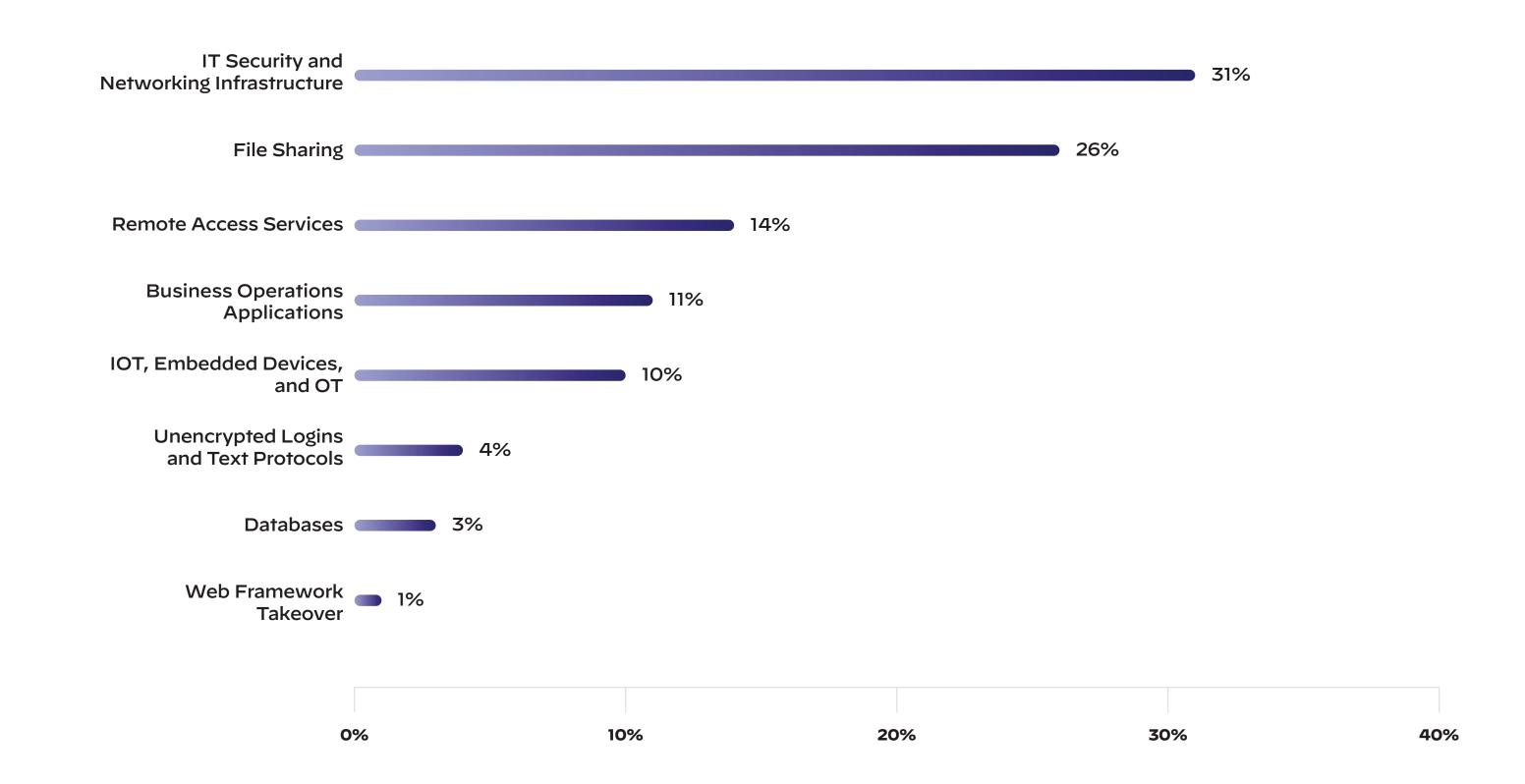- Financial losses from investigation, restoration, and potential fines due to breaches.

Category	Value
IT Security and Networking Infrastructure	31%
File Sharing	26%
Remote Access Services	14%
Business Operations Applications	11%
IOT, Embedded Devices, and OT	10%
Unencrypted Logins and Text Protocols	4%
Databases	3%
Web Framework Takeover	1%

Figure 15: Median distribution of top exposures in the education industry in 2022

NEXT CHAPTER →

US State and Local Governments

In a **Palo Alto Networks–sponsored survey** of IT leaders from US state and local governments, nearly one-third of respondents did not know whether remote work had impacted their organization.[5] Unit 42 found that remote access services are responsible for 24% of remote access risks in state and local governments, as shown in figure 16. Many state and local governments also exposed IT, networking, and security infrastructure and file-sharing services.

State and local governments should secure their networks due to the critical importance of the data and services they handle. These systems frequently house sensitive information, such as citizens' personal data, infrastructure details, and financial records. If compromised, this can result in breaches of privacy, identity theft, and significant financial and reputation damage. Further consequences could include the disruption of critical public services, ranging from emergency response to utility provisioning.
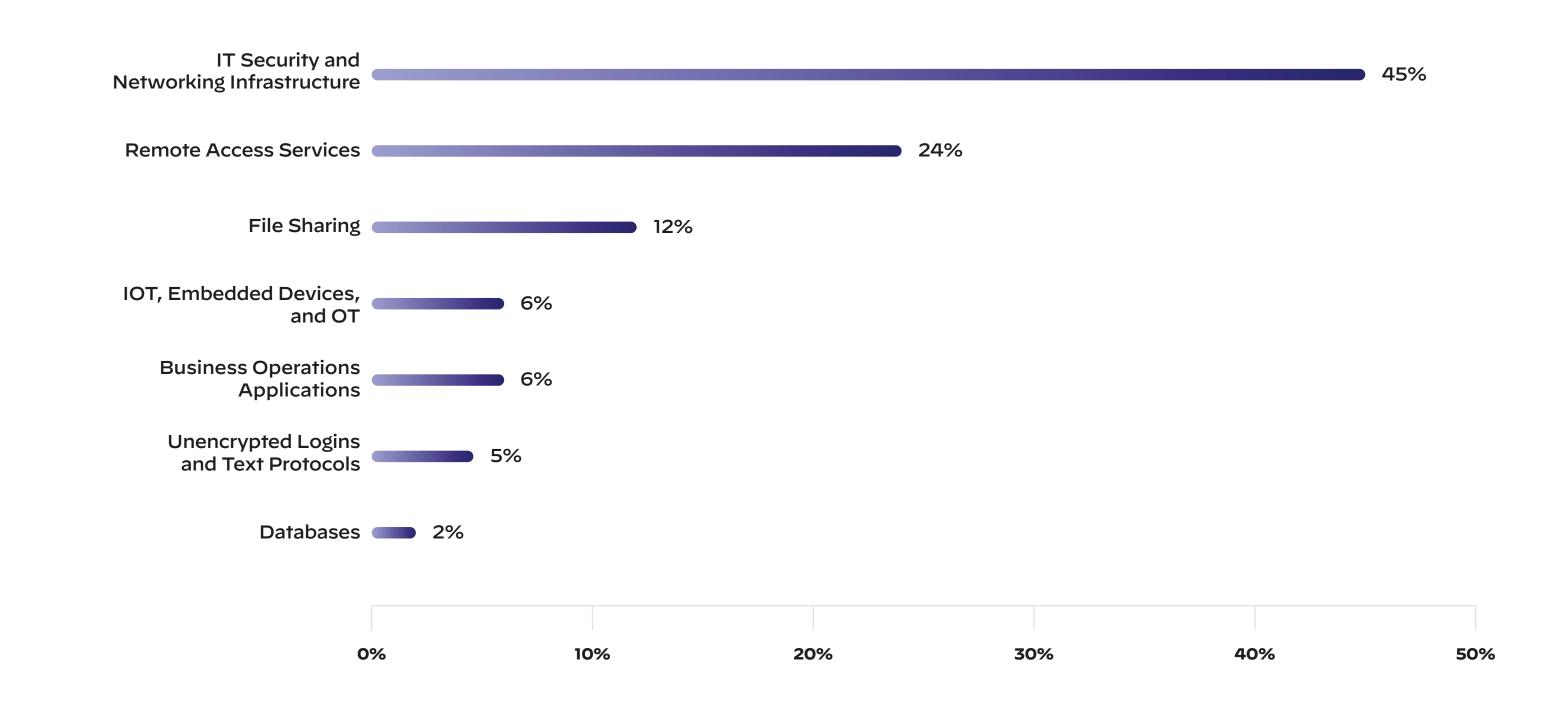
Figure 16: Median distribution of top exposures in state and local government in 2022

Transportation and Logistics

Compromise of remote access services, which make up 13% of all the exposures in this industry, as shown in figure 17, can lead to disruptions in transportation networks, delays in delivery schedules, and potential theft or manipulation of sensitive data. Database exposures are responsible for one out of every four critical issues in a logistics company.

These exposures can result in unauthorized access to sensitive information, including shipping manifests, customer contacts, and operational data that can lead to potential theft or manipulation of sensitive cargo data. Additionally, this industry also relies on outdated and unencrypted FTP servers (7% of all exposures are legacy FTP servers) to share data, which provides attackers with several opportunities for data theft.
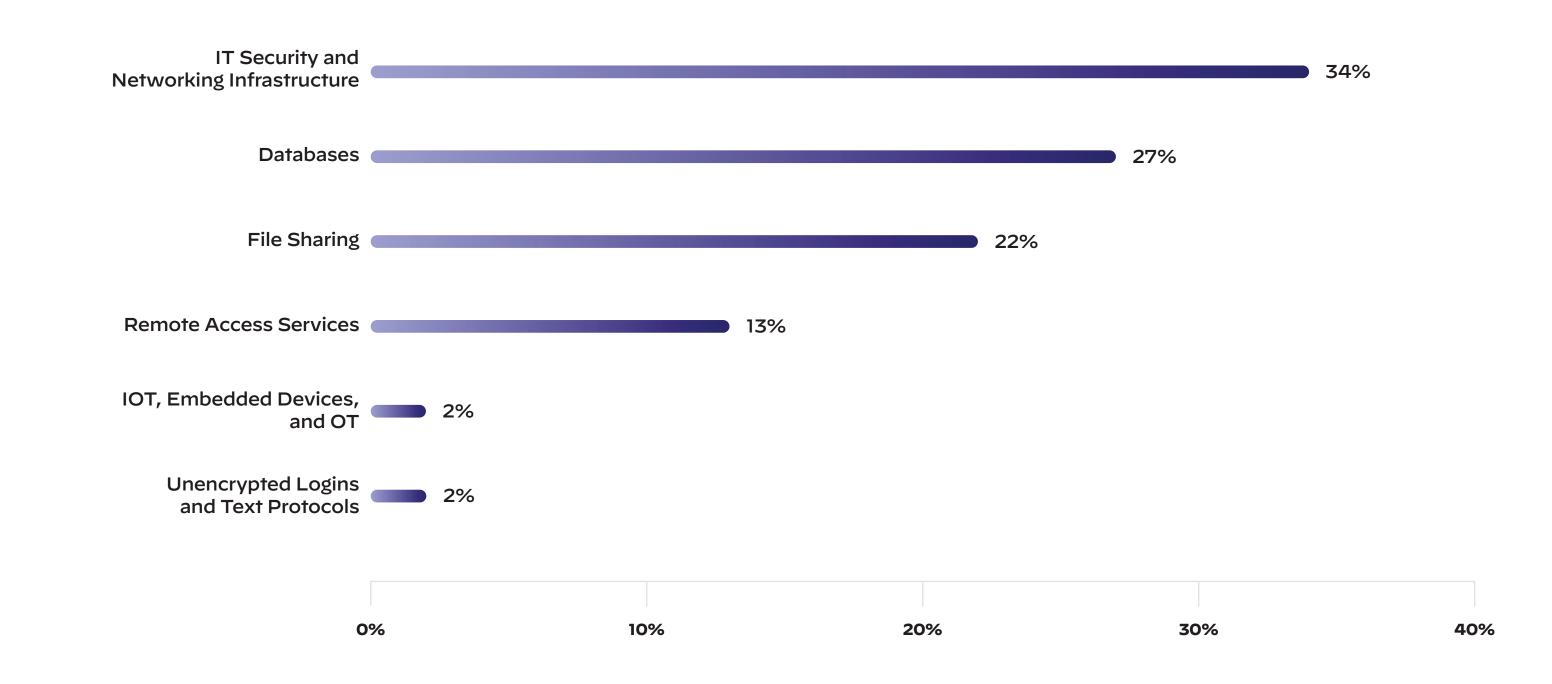

Figure 17: Median distribution of top exposures in the transport and logistics industry in 2022

Finance

Financial institutions most frequently expose file-sharing services, followed by IT, security, networking infrastructure, and remote access services. Financial institutions must prioritize network security due to the sensitive nature of the data they handle and the potential consequences of a breach. These institutions are custodians of vast amounts of personal and financial data, and any compromise can lead to substantial monetary loss, identity theft, fraud, and a loss of customer trust that can be irreparable.

Moreover, as financial systems interconnect globally, a security breach can have systemic implications, potentially destabilizing the financial ecosystem. Hence, robust cybersecurity measures are paramount in protecting the integrity and confidentiality of data, ensuring the continuity of services, maintaining customer trust, and upholding the overall stability of the financial system.
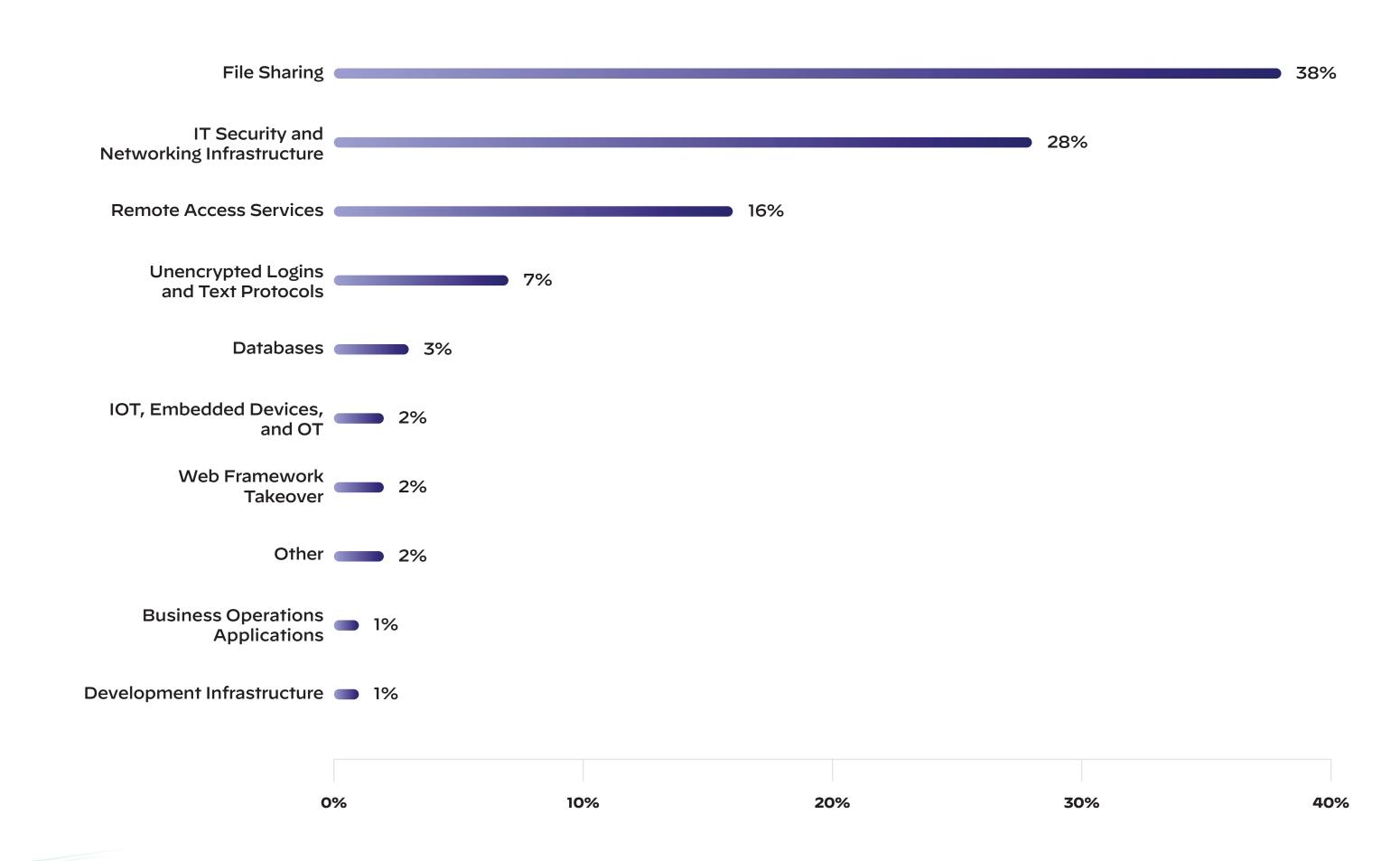

Figure 18: Median distribution of top exposures in the finance industry in 2022

NEXT CHAPTER →

Wholesale and Retail

Wholesale and retail organizations had a remarkably high proportion of remote access services, which are likely exposed to help organizations efficiently manage the IT at a large number of distinct physical locations. Misconfigured remote access services carry substantial risk since they give attackers an opportunity to gain unauthorized access to the organization's network.

Securing network infrastructure is of paramount importance for retail businesses due to the sensitive nature of the data they handle and the potential impact on their operations. Retailers collect and store vast amounts of customer data, including personal and financial information.

A security breach can lead to significant data loss, fraud, and a breach of customer trust that can damage the brand's reputation. Additionally, retailers rely heavily on IT systems for inventory management, sales processing, and other critical operations. A disruption due to a cyberattack can lead to substantial financial losses and operational inefficiencies.
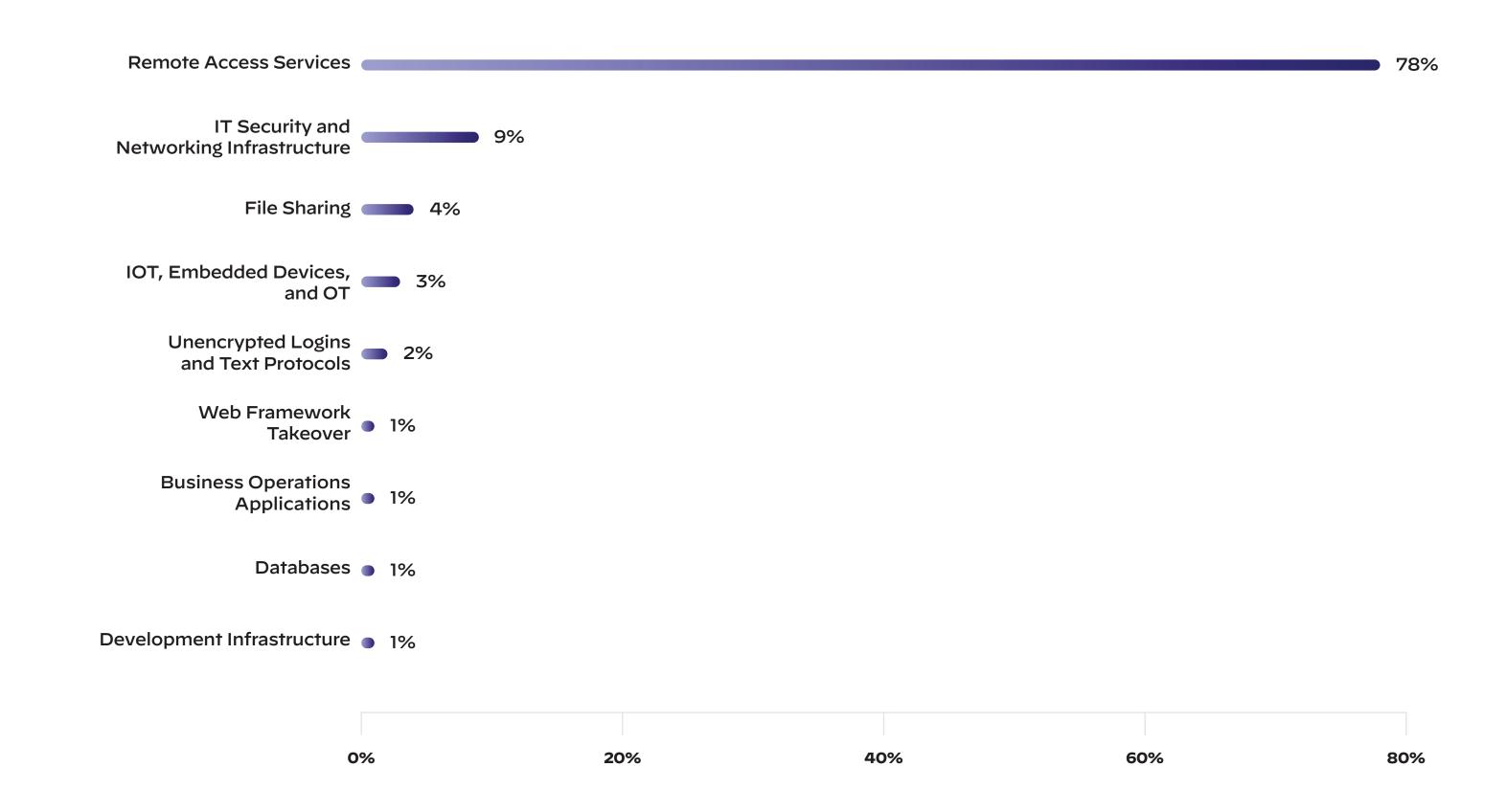
Category	Percentage
Remote Access Services	78%
IT Security and Networking Infrastructure	9%
File Sharing	4%
IOT, Embedded Devices, and OT	3%
Unencrypted Logins and Text Protocols	2%
Web Framework Takeover	1%
Business Operations Applications	1%
Databases	1%
Development Infrastructure	1%

Figure 19: Median distribution of top exposures in the wholesale and retail industry in 2022
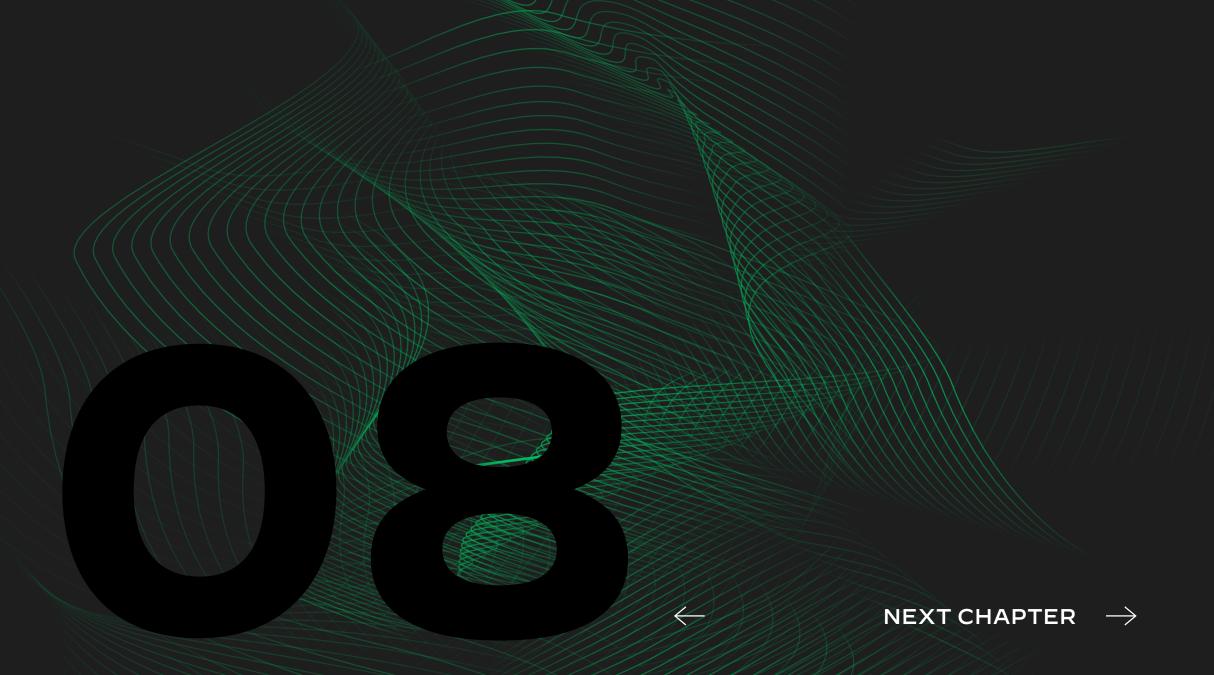
CONCLUSION

Organizations across all industries face significant challenges and risks due to growing attack surfaces. Modern threat actors are experts at exploiting the path of least resistance to gain access to victims' environments.

To manage and secure their attack surfaces, organizations must adopt a proactive and holistic approach. This involves continuous visibility and prioritizing remediation to maintain control over their internet-facing infrastructure.

By implementing the recommendations outlined in the report, organizations can actively manage their attack surfaces and keep their organization safe. The following section provides detailed recommendations to help organizations strengthen their cybersecurity posture and actively manage their dynamic attack surfaces.

08

Recommendations

Attackers are using automation and opportunity at scale, and defenders must do the same to be convergent with the threats they face. Here are our recommendations:

Gain continuous visibility over all assets

Ensure that your organization has a comprehensive, real-time understanding of all internet-accessible assets, including cloud-based systems and services, to effectively manage your attack surface. This is important to maintain even as that attack surface changes every day. Cortex Xpanse helps your organization actively discover, learn about, and respond to risks in all connected systems and exposed services.

Prioritize remediation

Focus on addressing the most critical vulnerabilities and exposures, such as those with a high Common Vulnerability Scoring System (**CVSS**) score, which accounts for severity, and an Exploit Prediction Scoring System (**EPSS**) score, which accounts for likelihood, to reduce the likelihood of successful cyberattacks.

Get the help you need

If attack surface management is new to your organization, or you'd like help with improving your program, a Unit 42 Attack Surface Assessment can jump-start your journey.

Secure remote access services

Implement strong authentication methods, such as MFA, and monitor remote access services for signs of unauthorized access or brute-force attacks. Our Prisma Access solutions can help enable Zero Trust Network Access and provide other SASE capabilities your organization needs.

Address cloud misconfigurations

Regularly review and update cloud configurations to ensure they align with best practices and address any potential security risks. Prisma Cloud helps security and DevOps teams collaborate and drive secure cloud-native application development and deployment. This is a great way for security and DevOps teams to build a working relationship that's good for everyone.

Monitor for emerging threats

Stay informed about new vulnerabilities, exploits, and threat actors. Continuously assess your organization's attack surface for potential risks. Follow the **Unit 42 blog** for our insights, and if you'd like a consulting relationship, **consider a services retainer** for threat landscape briefings and incident response services.

09

METHODOLOGY

Unit 42 and Cortex Xpanse collected petabytes of information on internet-accessible exposures across 250 organizations in 2022 and 2023. While Unit 42 used the data to analyze issues associated with these exposures, the research team used the last six months of 2022 to study the nature of the change of cloud services and the associated risks they create in a typical organization across industries because six months yielded sufficient data for computation.

For each industry category, the research team included data from at least five large organizations in that industry. Cortex Xpanse was used to classify a system as on-premises or cloud, depending on a variety of factors. To do this work with speed, precision, and scale, the research team leveraged a machine learning model for the accurate attribution of assets to different organizations. The model was supervised by a team of attack surface analysts that support Cortex Xpanse.

To map the timeline of the attack, the research team combined our data with third-party data for the "time elapsed before attack" analysis.

The datasets used for this were from March 31, 2022, to March 31, 2023.

The research team only accounted for exposures where the product or vendor or the Common Platform Enumeration (CPE) could be inferred, and the data points were consistent across the fingerprinting source and the vulnerabilities data source. To identify the steady median for analysis, the research team used a rolling 10-day median, which eliminated any outlier bias in our VPN device observations.

For delineation between cloud and on-premises assets, on-premises assets of an organization are publicly accessible systems and services owned by an organization with statically assigned IP addresses, and cloud assets are publicly accessible systems and services leased by an organization in dynamic IP space, not including multitenant, SaaS-delivered services.

10

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats so organizations can embrace technology with confidence. We provide next-generation cybersecurity to thousands of customers globally, across all sectors.

Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

For more information, visit
www.paloaltonetworks.com

About Cortex Xpanse

Cortex® Xpanse™ is an active attack surface management solution that helps your organization actively discover, learn about, and respond to unknown risks in all connected systems and internet-accessible services.

Cortex Xpanse protects the U.S. Department of Defense, all six branches of the U.S. military, several federal agencies, and several large enterprises like Accenture, AT&T, American Express, AIG, Pfizer, and over 200 others.

For more information, visit
www.paloaltonetworks.com/cortex/cortex-xpanse

About the Unit 42 Attack Surface Assessment

The Unit 42 Attack Surface Assessment helps you identify and manage exposure, mitigate risk, and bolster your security posture now and in the future. This assessment provides an expert view of your internet-connected assets with prioritized recommendations to improve your defenses so you can remediate issues before they can be exploited.

With our security expertise and Cortex Xpanse data, you will find previously unknown assets, including shadow IT infrastructure, to identify vulnerabilities and security gaps. You get recommendations tailored to your specific business and security concerns.

Identifying and remediating issues in your attack surface can reduce insurance premiums and show measurable progress to regulators, board members, and other stakeholders. If your organization needs help with starting or advancing your attack surface management program, the **Unit 42 Attack Surface Assessment** can help.[6]

About Unit 42

Palo Alto Networks Unit 42™ brings together world-renowned threat researchers, elite incident responders, and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against real-world threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster.

Visit **paloaltonetworks.com/unit42**

3000 Tannery Way
Santa Clara, CA 95054

Main   +1.408.753.4000
Sales   +1.866.320.4788
Support   +1.866.898.9087

References:
1. *2021 Cortex Xpanse Attack Surface Threat Report*, Palo Alto Networks, May 10, 2021. 2. *2022 Unit 42 Incident Response Report*, Palo Alto Networks, July 26, 2022. 3. Ibid.
4. *2022 Cortex Xpanse Attack Surface Threat Report*, Palo Alto Networks, July 19, 2022. 5. *Smart Investments for Getting Ahead of Ransomware*, Center for Digital Government, February 2022.
6. "Unit 42 Attack Surface Assessment" datasheet, Palo Alto Networks, January 31, 2023.