The Top 5 Most

Common Third-Party Cyber Gaps

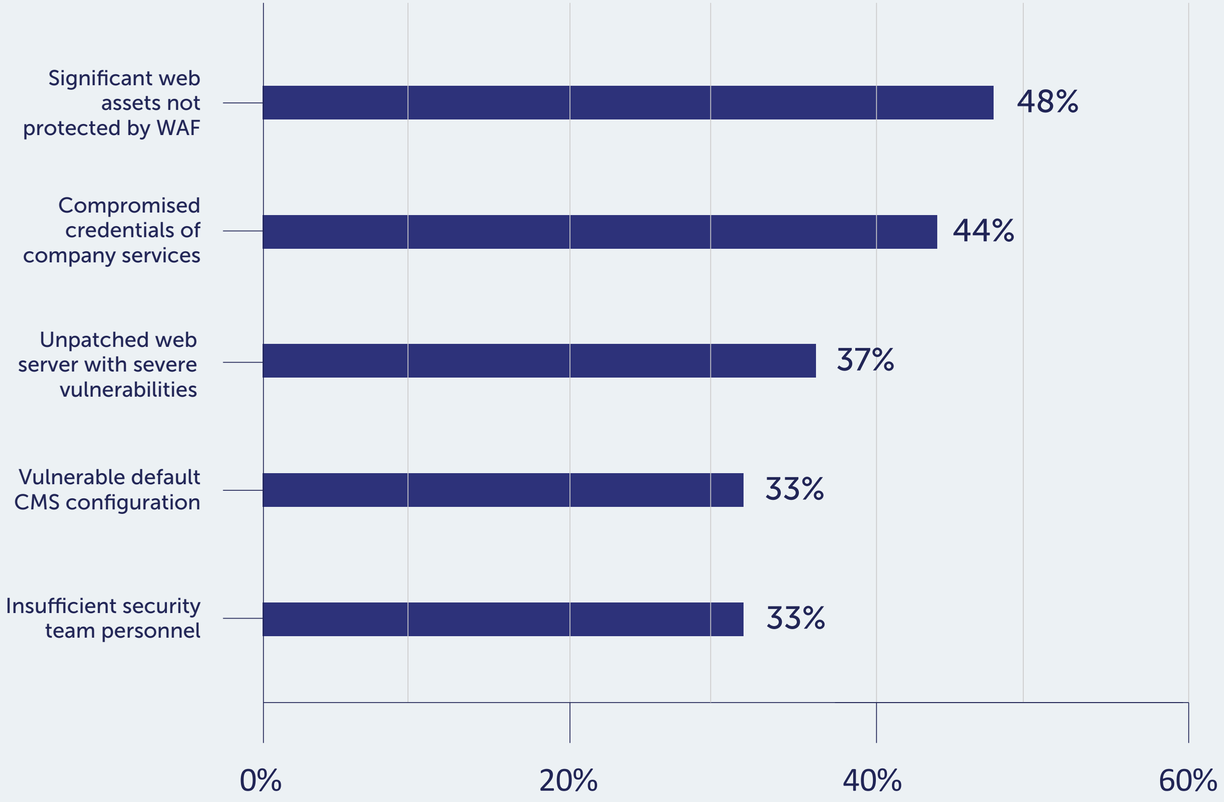
The Widespread Cyber Issues You Should Be Aware of for 2022

Panorays

How can you reduce supplier cyber risk?

To answer this question, Panorays used data from our cyber posture evaluations of tens of thousands of third parties from various industries over an extensive time period. We extracted findings that appeared in a large percentage of the companies while omitting obvious low-risk findings seen in all companies, such as missing recommended HTTP response headers. We focused on cyber gaps that may have a significant impact on the resilience of the vendors, and thus the organizations themselves.

Here are the most common cyber gaps that we found in 2021.



One of the cyber gaps, called “Compromised credentials of company services” is new to our top five this year. In addition, we can see that many of the most common cyber gaps remained about the same as 2020.

Here’s a closer look at the top gaps we found this year.

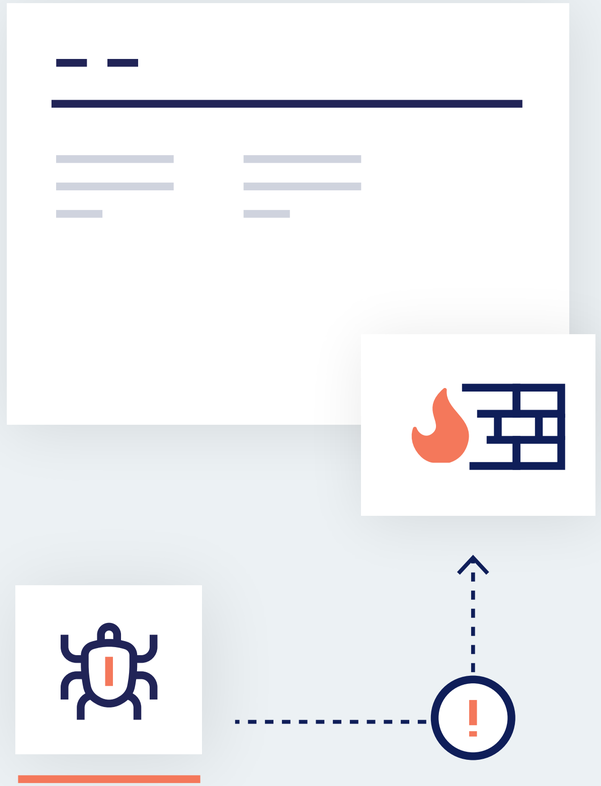
Significant web assets not protected by Web Application Firewall

Companies affected: 48%

Websites and apps are targeted by a wide range of attacks—from scraping and DDoS to injections and cross-site scripting. For this reason, Web Application Firewalls (WAF) have become a must-have for basic protection. However, WAF is expensive and notoriously difficult to configure and maintain, which explains why this cyber gap has consistently remained on our top five list every year.

Tip

With the recent Log4j attack, we saw that companies with successfully deployed WAFs were able to quickly mitigate the vulnerability, rather than patch numerous servers. Doing the latter can be extremely time consuming and can hinder business.



Compromised credentials of company services

Companies affected: 44%

Panorays recently added this test to its cyber posture evaluation, which explains why it is appearing on this list for the first time. This cyber gap indicates that malicious actors have breached an endpoint, such as a laptop, and are selling the stolen credentials on the dark web. Since it's fairly easy for attackers to opportunistically breach endpoints, we see this situation quite often. In fact, compromised credentials have been the entry point in many recent high-profile supply chain attacks.

Tip

Companies can effectively address this cyber gap simply by changing credentials. However, action is required immediately, since authenticated users can have access to internal systems that may be used to attack the company.

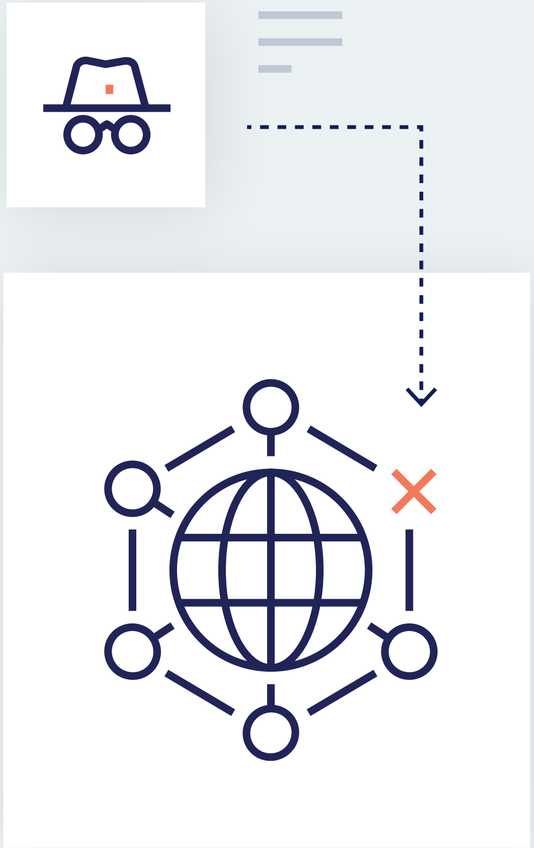
Unpatched web server with severe vulnerabilities

Companies affected: 37%

Patch management continues to be a very common and painful subject in the security world, because it involves a great deal of effort and can impact business continuity. In addition, employees who work remotely are often reluctant to patch because they are concerned about the possibility of being left without a work station. For these reasons, we see that many companies are still struggling to effectively patch against known critical vulnerabilities.

Tip

We've seen a slight improvement in the patching cadence of web servers compared to 2020, when this cyber gap affected 40% of companies. This could be because of the multiple critical vulnerabilities that were discovered in Apache in 2021; as a result, security teams might have done a better job patching their servers. It will be interesting to see if this trend continues in 2022.



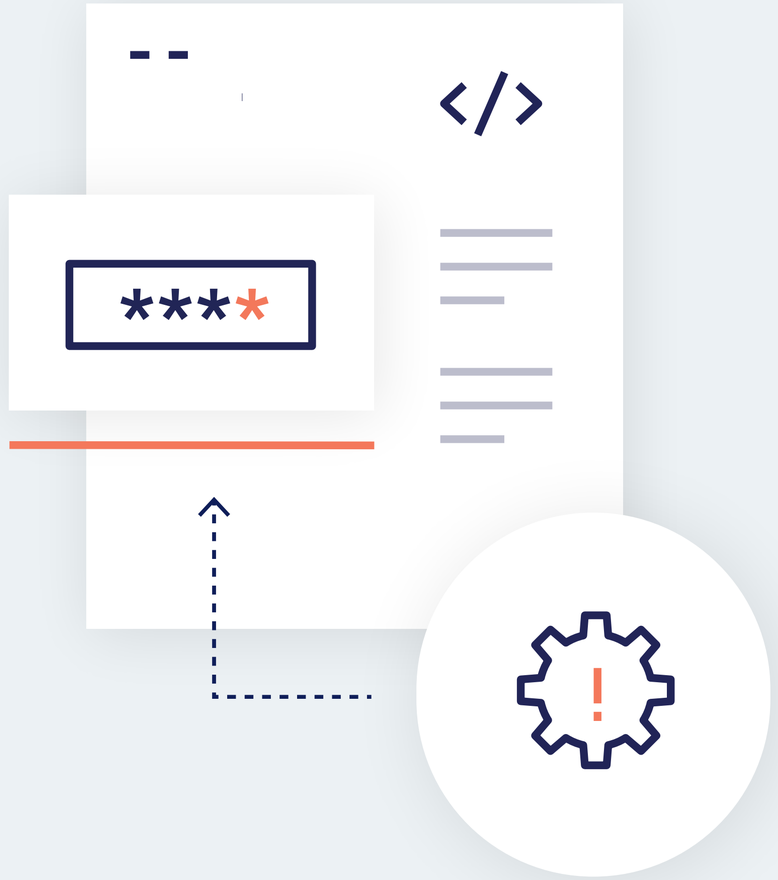
Vulnerable default CMS configuration

Companies affected: 33%

Content Management Systems such as WordPress are widespread, and so are their security vulnerabilities. Many users don't change default configurations such as passwords, user exposure and login pages, and that leaves them particularly vulnerable to cyberattacks.

Tip

To address this cyber gap, companies should begin by checking their CMS solution's security guide. By following best practices, companies can easily remediate this issue.



Insufficient security team personnel

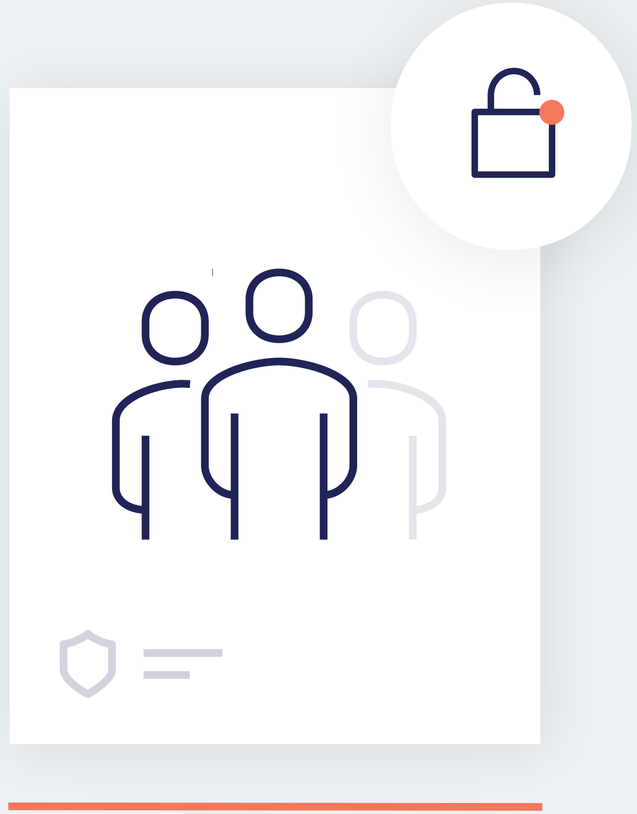
Companies affected: 33%

Dealing with the abundance of security responsibilities in today's organizations requires resources. Dedicated teams focusing on, for example, the CISO office and SOC, should be put in place and properly staffed to handle the increase in incidents and cyber-related tasks.

The percentage of companies with this cyber gap increased slightly over last year, indicating that this continues to be a problem.

Tip

Note that these are security personnel that can be detected externally; for example, by being mentioned on a company website or through a workplace social network like LinkedIn. It is important that your company has a visible security contact available to handle external requests such as bug disclosures.



Summing Up

While these are the most common cyber gaps we found, there are many more. Because technology keeps on evolving, new vulnerabilities are constantly being introduced, leading to new cyber gaps that can be exploited by criminals. For this reason, it's important for organizations to assess and continuously monitor their third parties to uncover all cyber gaps and close them.

How Panorays Helps

Panorays can help you create and improve your third-party security process. Using Panorays, you can:

Get a 360° view of your suppliers

Eliminate manual questionnaires

Comply with regulations

Benefit from contextual ratings

Engage effortlessly with suppliers

Remediate cyber gaps

Receive continuous visibility

Detect third and fourth parties

About Panorays

Panorays is a rapidly growing provider of third-party security risk management software, offered as a SaaS-based platform. The company serves enterprise and mid-market customers primarily in North America, the UK and the EU, and has been adopted by leading banking, insurance, financial services and healthcare organizations, among others. Headquartered in New York and Israel, with offices around the world, Panorays is funded by numerous international investors, including Aleph VC, Oak HC/FT, Greenfield Partners, BlueRed Partners (Singapore), StepStone Group, Moneta VC, Imperva Co-Founder Amichai Shulman and former CEO of Palo Alto Networks Lane Bess.

Visit us at **www.panorays.com**

Panorays

Want to learn more about uncovering and remediating your vendors' cyber gaps?
Contact Panorays today >