OPSWAT.

Web Application Security Report 2021

Secure File Uploads in Web Applications:

Attitudes, Statistics, Trends, and Best Practices to Secure Critical Infrastructure from Security Breaches and Compliance Violations

an OPSWAT Research Report

KEY FINDINGS

State of Cybersecurity

Readiness (or lack thereof)

87% of organizations using a web application for file uploads are very concerned about secure file transfers; **82% report an increase in concern over the past year.**

40% of critical infrastructure industries **significantly increased their concern in the past year, versus 25%** of other industries.

66% Two-thirds of organizations with a web application for file uploads are concerned about **a loss in business or revenue or reputational damage** related to unsecure file uploads.

The Blind Spots

Huge gaps that need to be addressed

32% One-third of organizations with a web application for file uploads **do not scan all file uploads** to detect malicious files.

18% One in five of these organizations **scan with just one** anti-virus engine.

65% Two-thirds of organizations with a file upload web portal **do not sanitize file uploads** with Content Disarm and Reconstruct (CDR) to prevent unknown malware and Zero-day attacks.

TABLE OF CONTENTS

INTRODUCTION

The emergence of the hybrid workspace is driving a new decade of digital transformation and cloud migration initiatives.

The rise of cloud services, mobile devices and remote workers has driven organizations to develop and deploy web applications that enhance the experience for their customers, clients, partners, and employees.

However, the widespread adoption of web applications has introduced new and expanded existing attack surfaces that many organizations are not effectively protecting. Organizations have also become more concerned with mitigating third-party risk in the wake of the SolarWinds compromise.

Many organizations leverage web applications for file uploads to streamline their business by making it faster, easier, and less expensive to submit and share documents. However, this productivity and enhanced user experience also opens additional attack vectors into your environment, including the potential for hackers to upload malicious files. Many common file types, such as word processing documents, spreadsheets and PDFs include enhanced productivity functionality which also makes it easier for malicious actors to hide ransomware, zero-day attacks, and other advanced or targeted malware, e.g., Advanced Persistent Threats (APTs).

OWASP has identified "Unrestricted File Uploads" as a vulnerability with significant risk because file uploads provide malicious actors with direct access to the systems they are trying to attack.

What is OWASP?

The Open Web Application Security Project (OWASP) is a nonprofit organization that tracks the most common risks for web application security and provides best practices for their mitigation.

According to OWASP, "The consequences of unrestricted file upload can vary, including complete system takeover, an overloaded file system or database, forwarding attacks to back-end systems, client-side attacks, or simple defacement."

Very few organizations follow all the recommended security practices and principles. This, combined with increasingly sophisticated tactics and more dangerous variants used by cybercriminals, resulted in adjusted ransomware losses of over $29M in 2020, up over 200% from the previous year[1]. Data breaches were up 38 percent in Q2, 2021[2]. This is a worsening trend that comes on top of the worst year that saw record-breaking activity from hackers during the pandemic.

OPSWAT conducted this web application security research with a focus on file uploads to identify trends and gaps in current cybersecurity measures, so that security professionals may better understand and address the risks to their organizations.

Critical Infrastructure Under Siege

During 2020 and 2021, ransomware attacks have surged within the critical infrastructure sector.

During 2020, in the midst of a pandemic, at least 59 hospitals and healthcare systems were targeted by ransomware attacks, including all 250 U.S. facilities of Universal Health Services. In 2021, the DarkSide ransomware group shut down Colonial Pipeline, causing a week-long gas crisis and costing Colonial Pipeline $5 million. Next, the REvil ransomware gang targeted JBS meatpacking with an $11 million attack, and is suspected of breaching Sol Oriens, a U.S. nuclear weapons contractor.

As these attacks increase, copycat ransomware groups have begun targeting critical infrastructure sectors with increasing frequency.

CYBERSECURITY READINESS: MEASURES TO PREVENT SECURITY BREACHES AND PROTECT DATA AT RISK

Organizations have some options to help mitigate threats posed by an evolving cybercriminal industry, but none of them solve the problem effectively on their own.

Denying and/or allowing only certain file types may not be a solution for many organizations, as malicious actors may still be able to bypass this weak protection. Likewise, detecting file types and checking image sizes are both considered weak protections that malicious actors may bypass.

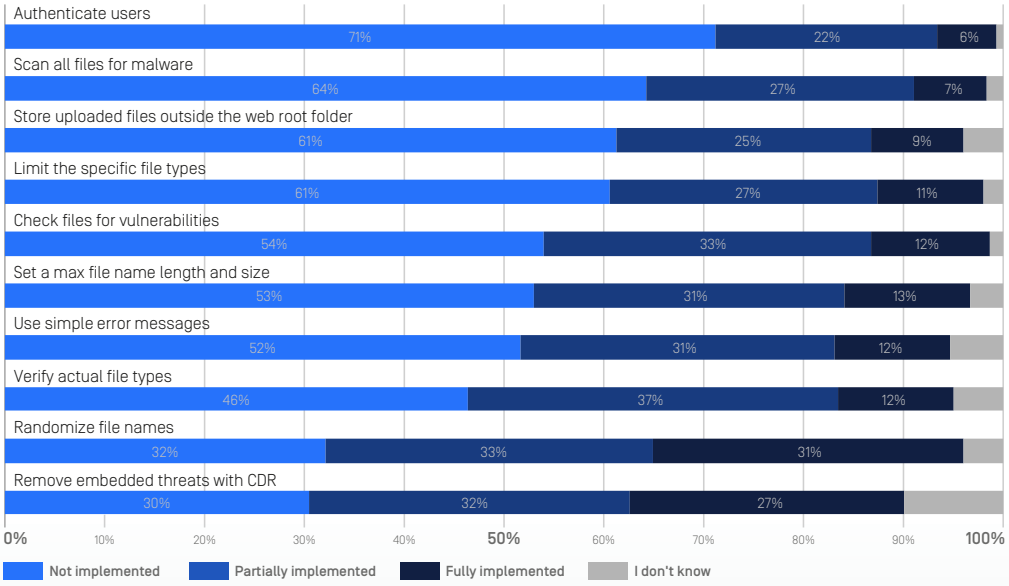
OPSWAT has identified 10 best practices for file upload security, but only 8 percent of organizations with web applications for file uploads have fully implemented all ten. More than half the organizations (56%) that accept file uploads have only implemented five or fewer of these best practices. Overall, adoption rates for these best practices are poor.

Among these best practices, authentication, anti-virus, and storing files outside the web root were the most adopted, while verifying the file type, randomizing uploaded file names, and removing embedded threats with Content Disarm and Reconstruction (CDR) (data sanitization) were among the least adopted.

Less than two-thirds (64%) of organizations that accept file uploads scan all files for malware. Only half (54%) check files for vulnerabilities. Less than one-third (30%) remove embedded threats with Content Disarm and Reconstruction (CDR) technology.

FILE SECURITY **BEST PRACTICES NOT BROADLY IMPLEMENTED**

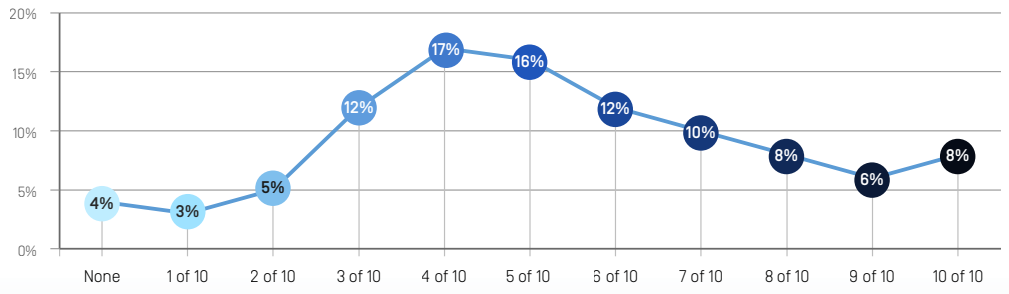
Survey Response: Please rate your organization's level of implementation for each of the following file upload security best practices.



More than half the organizations surveyed implement five or fewer of the recommended 10 best practices. It should come as no surprise that they are worried about the security of files uploaded to their web applications.

FILE SECURITY **BEST PRACTICES NOT BROADLY IMPLEMENTED**

Number of fully implemented file upload security best practices



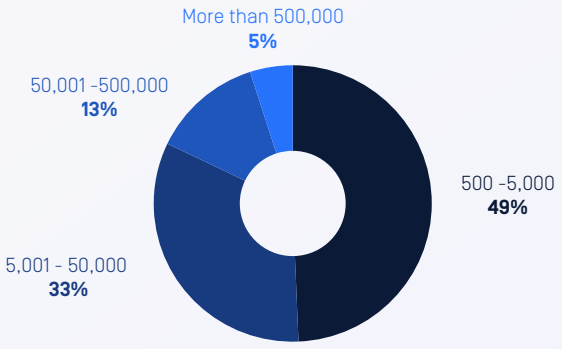
UNSECURED FILE UPLOADS: KEY AREA OF CONCERN IN WEB APPLICATION SECURITY

Organizations deploy web applications for file uploads for a variety of reasons, such as submitting forms and applications or sharing and collaborating on content. Among organizations with file upload portals, most of them had multiple portals and process tens of thousands of file uploads per day.

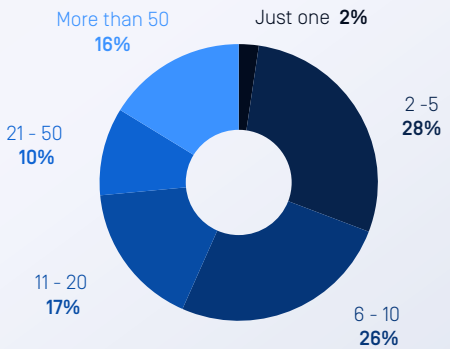
Only 2 percent of survey respondents had just one file upload portal, while 16% had more than 50. **More than half (51%) of organizations with a file upload portal process more than 5,000 file uploads per day.** Security professionals need to remain diligent because attackers will try all these numerous entry points to slip through undetected amidst such a high volume of file uploads.

PARTICIPANT PROFILE

Number of daily file uploads



Number of portals accepting external file uploads

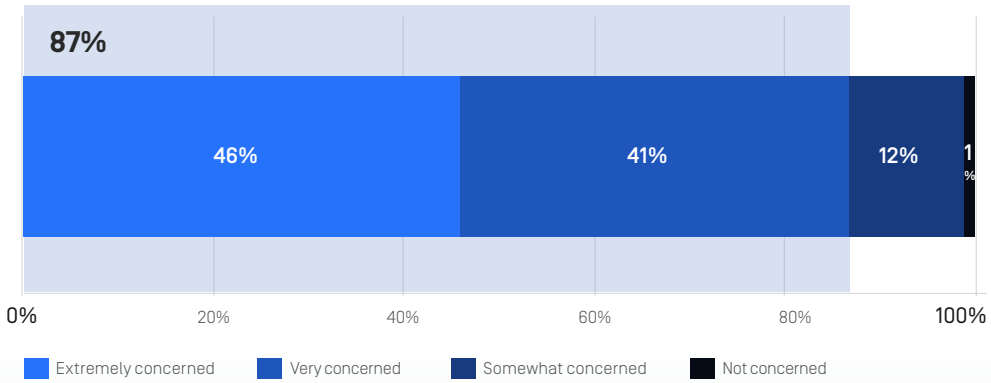


49% of critical infrastructure industries are **"extremely"** concerned about protecting file uploads from malware vs 36% of other industries. 40% of critical infrastructure industries have significantly increased this concern in the past year vs 25% of other industries.

The overwhelming majority of respondents were concerned about file uploads as an attack vector for malware and cyberattacks.

87% ARE "EXTREMELY" OR "VERY" CONCERNED ABOUT FILE UPLOAD SECURITY

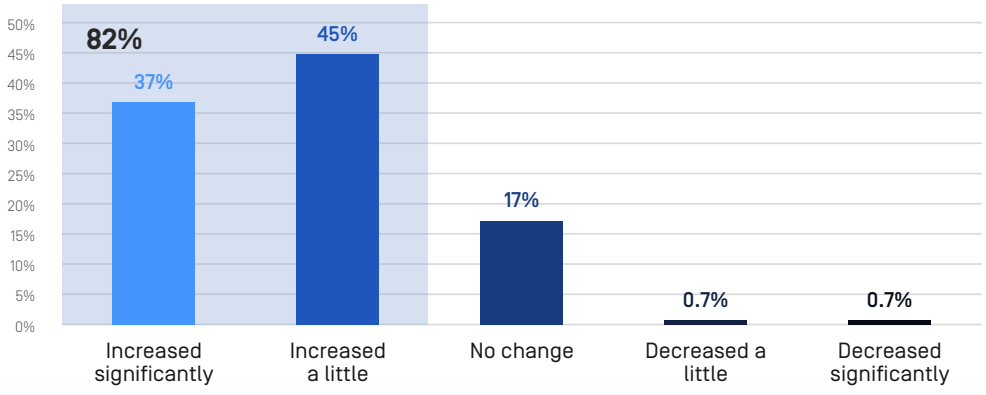
How concerned is your company about protecting against malware and cyberattacks from file uploads?



And the concern is increasing: 82% of organizations with file upload portals have increased concern about malware attacks from file uploads since last year.

82% REPORT AN INCREASE IN CONCERN ABOUT FILE UPLOAD ATTACKS IN PAST YEAR

In your experience, how has the concern about malware attacks from file uploads changed over the past year?



THE OPSWAT ADVANTAGE

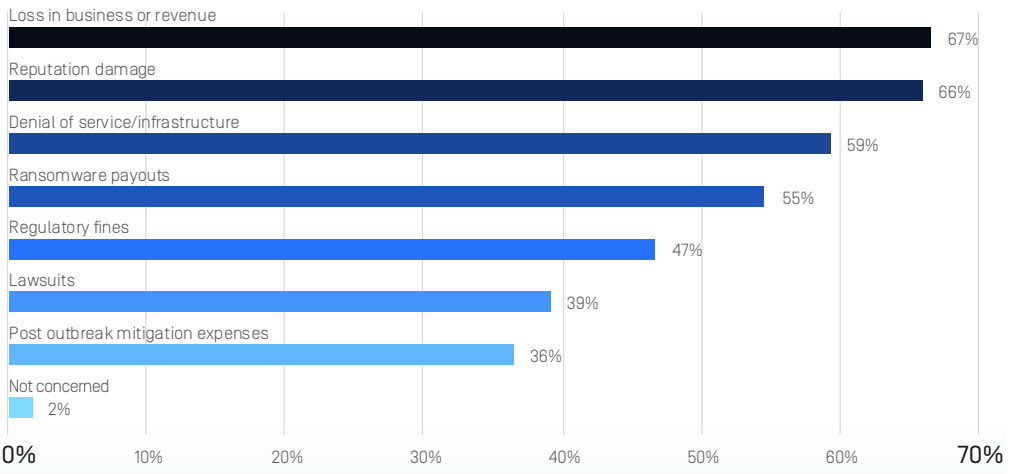
Proactive DLP

OPSWAT Proactive Data Loss Prevention (DLP) enables organizations to move beyond check the box compliance and mitigate third-party risk. OPSWAT Proactive DLP can detect and block sensitive data in more than 30 common file types, automatically redact sensitive information, remove metadata containing confidential information and watermark files for better security, accountability, and traceability.

Two-thirds of respondents (67%) were concerned about a loss in business or revenue and two-thirds (66%) were concerned about reputational damage. More than half (59%) were concerned about denial of service on their infrastructure, and more than half (55%) were concerned about ransomware payouts.

98% CITE CONCERNS ABOUT CONSEQUENCES RELATED TO UNSECURE FILE UPLOADS

Which of the following consequences of unsecure file uploads are you concerned about?

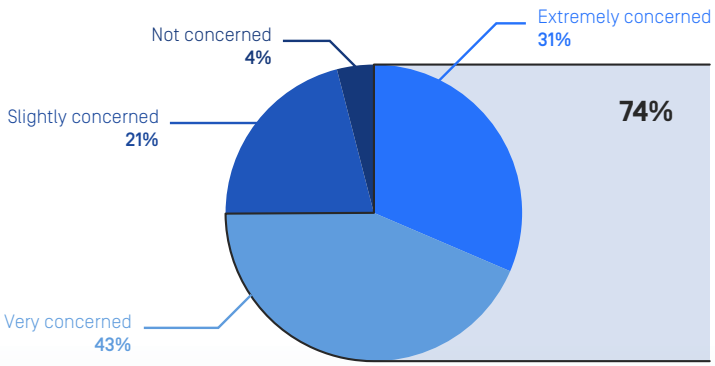


74% were very concerned about preventing compliance issues related to file uploads. Organizations in general seem to be more worried about reputational damage (66%) than the resulting regulatory fines (47%) or lawsuits (39%). In the case of concern about lawsuits there was a wide gap between the US (45%) and other countries (28%).

49% of critical infrastructure industries were concerned about regulatory fines, vs. 38% of other industries. 60% of financial services were concerned about regulatory fines.

74% ARE "VERY" OR "EXTREMELY" CONCERNED ABOUT FILE UPLOAD COMPLIANCE

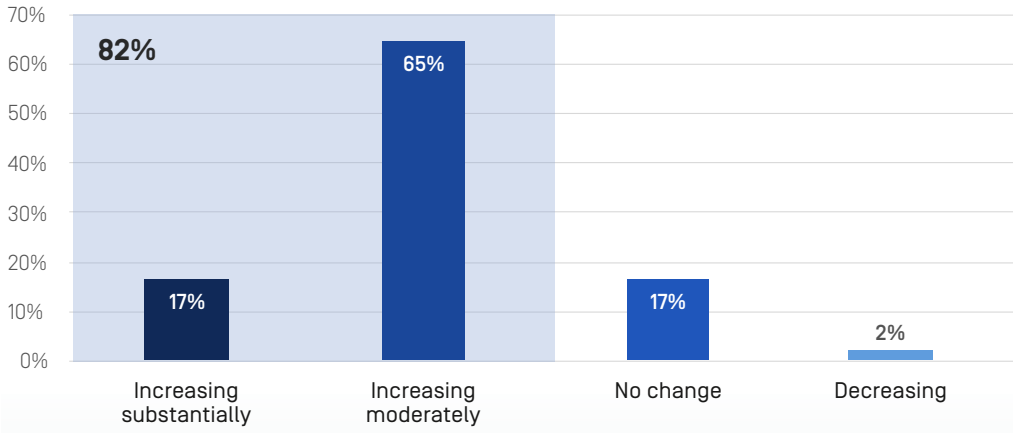
Which of the following consequences of unsecure file uploads are you concerned about?



82% of respondents said their company was increasing its security budget in 2021. These attitudes and trends could be explained by the fact that many organizations still have some major file upload security blind spots, as we will explain in the next section.

82% REPORT THEIR SECURITY BUDGETS ARE INCREASING FOR 2021

How would you characterize the changes to your company's security budget for 2021?



BLIND SPOTS THAT CREATE SEVERE SECURITY GAPS

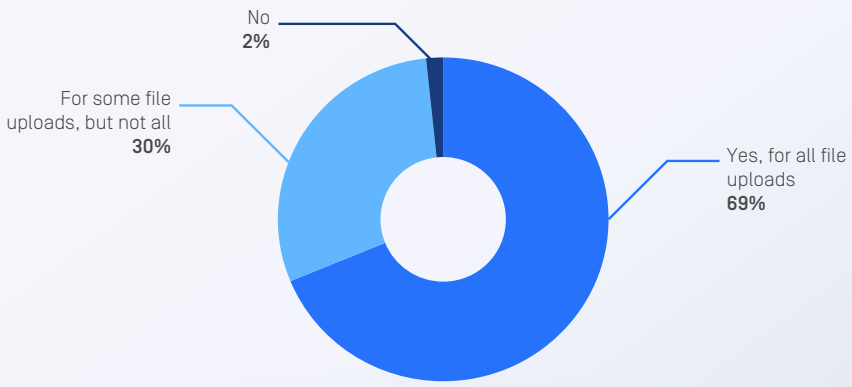
BLIND SPOTS: ANTI-VIRUS SCANNING

Anti-virus scanning is table stakes for any organization concerned with detecting malicious file uploads, but only two-thirds (69%) of organizations with web applications for file uploads are scanning all uploaded files with anti-virus and anti-malware engines.

Another major security hole is that two-thirds of organizations are scanning with five or less anti-virus engines, while one-in-five are scanning with just one anti-virus engine.

WIDE USE OF ANTI-VIRUS OR ANTI-MALWARE FOR FILE UPLOAD SECURITY

Does your company use anti-virus or anti-malware scanning to detect malicious file uploads?



THE OPSWAT ADVANTAGE

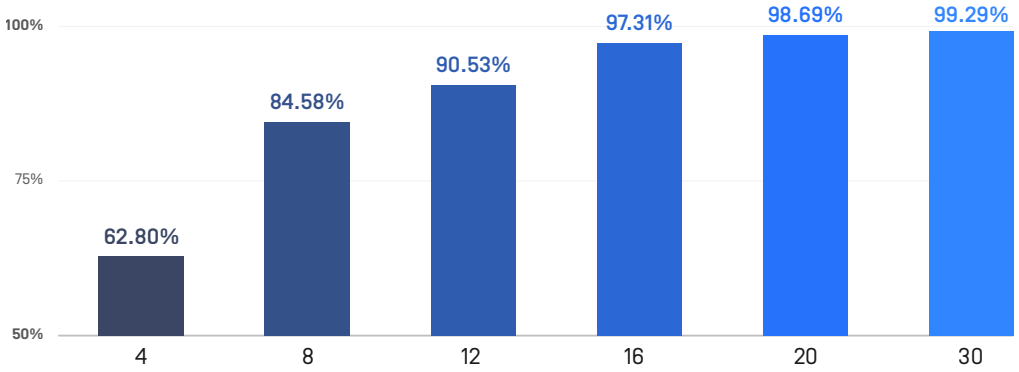
Malware Multiscanning

OPSWAT Multiscanning enables organizations to achieve detection rates greater than 99 percent by simultaneously scanning with more than 30 anti-virus and anti-malware engines, so that organizations can detect threats sooner, respond to outbreaks faster, and minimize false positives.

The efficacy of anti-virus scanning is directly correlated to the number of engines in use because each additional engine increases the chances of detecting a threat. Previous OPSWAT research reveals that scanning with just four (4) anti-virus engines only results in a 62.80% detection rate of the top 10,000 threats. Even scanning with eight (8) anti-virus engines only results in an 84.58% detection rate.

DETECTION EFFICACY OVERVIEW

Detection rates of the top 10,000 threats per MetaDefender search volume

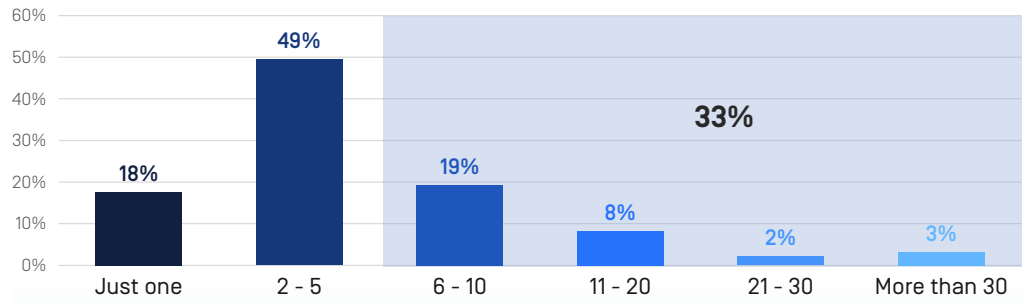


87% of critical infrastructure industries are using more than one anti-virus engine vs 68% of other industries; however, 84% of critical infrastructure industries are still using 10 or fewer anti-virus engines.

It is not until scanning with at least 12 anti-virus engines that detection rates surpass 90% – yet only 13% of organizations with file upload portals are scanning with more than 10 anti-virus engines. Organizations need more than 30 anti-virus engines to reach a 99% detection rate, but only 3% of respondents have deployed more than 30 anti-virus engines.

ONLY ONE-THIRD OF ANTI-MALWARE USERS HAVE DEPLOYED MULTIPLE ENGINES

Approximately how many anti-virus or anti-malware engines does your company deploy to detect malicious file uploads?



THE OPSWAT ADVANTAGE

Deep CDR

OPSWAT Deep CDR is an advanced threat protection technology that can sanitize and reconstruct more than 100 common file types, and verify more than 4,500 file types to prevent spoofing. OPSWAT Deep CDR integrates with OPSWAT anti-malware Multiscanning and other technologies to provide comprehensive protection for web applications.

38% of critical infrastructure industries are using Content Disarm & Reconstruction (CDR) technology vs 26% of other industries.

BLIND SPOTS: DATA SANITIZATION

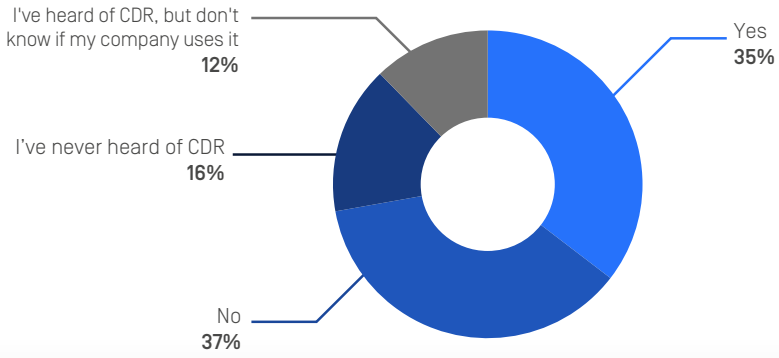
As cybercriminals continue to play a cat and mouse game with anti-virus and anti-malware engines, organizations need to consider a zero-trust approach to web application file upload security.

Content Disarm and Reconstruction (CDR) is a data sanitization technology based on prevention rather than detection. Instead of detecting malicious files, CDR presumes that all files are potentially malicious. It deconstructs files into discrete components, removes anything potentially malicious from them i.e. sanitizes the individual components, and reconstructs them back into a safe to consume file without impacting file integrity or functionality.

CDR is effective at preventing zero-day attacks that evade detection because CDR does not rely on detection. However, only one-third (35%) of organizations with a web application accepting file uploads have deployed CDR technology, which means many organizations are vulnerable to zero-day attacks.

ONLY A THIRD (35%) REPORT USE OF CDR

Does your company use CDR (Content Disarm and Reconstruction) for data sanitization to disarm embedded threats (e.g., macros in word documents or scripts in PDFs)?



CONCLUSION

The critical infrastructure industries have a heightened sense of security—they are more confident about their budgets and technology, but they are also more concerned about malware.

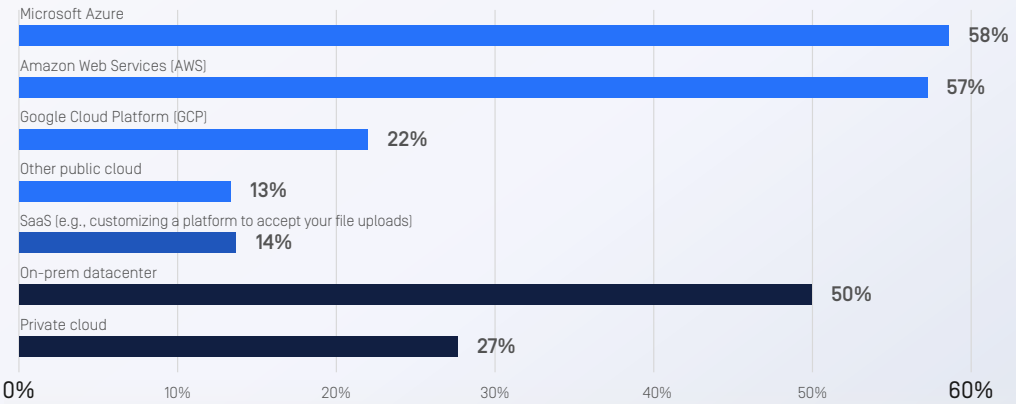
Ultimately, the critical infrastructure industries share many of the same security blind spots as other industries.

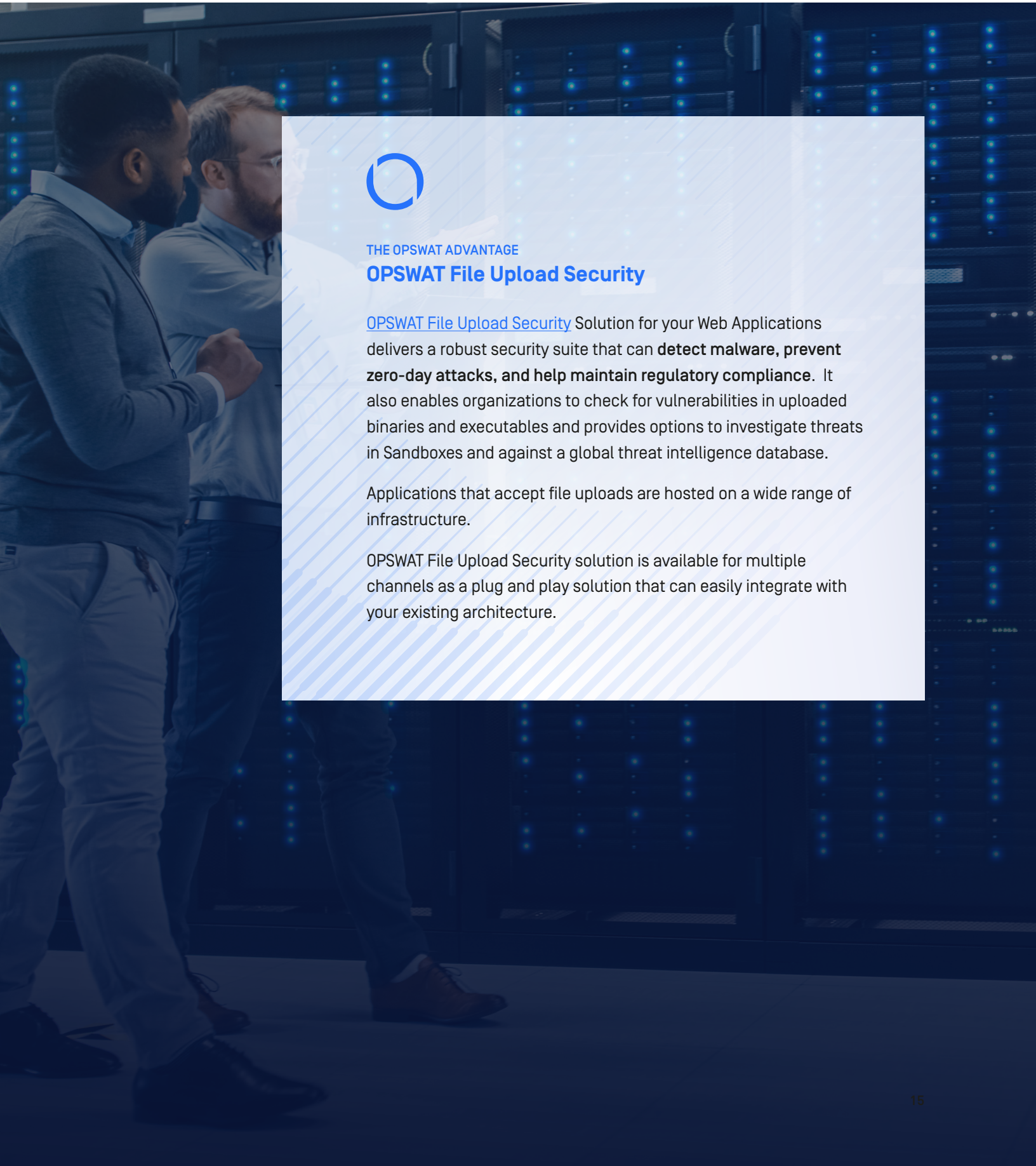
While there is an increasing awareness of the need to secure file uploads as an integral part of web application security and an increase in budgets to solve this problem, there are still some major blind spots when it comes to file upload security: organizations aren't following best practices, they aren't using comprehensive anti-virus technology effectively, and most are not using CDR technology to prevent known and unknown attacks

Pragmatically, organizations are concerned with file upload security, and it makes sense why: organizations are processing tens of thousands of file uploads per day that are vulnerable to being exploited to launch a cyberattack. But realistically, if organizations want to close their web application security gap, then they need a solution that offers comprehensive protection with a few integrated advanced technologies like anti-virus multiscanning and CDR.

APPLICATIONS THAT ACCEPT FILE UPLOADS ARE **HOSTED ON A WIDE RANGE OF INFRASTRUCTURE**

Where are your company's web applications that accept file uploads currently hosted?





THE OPSWAT ADVANTAGE

OPSWAT File Upload Security

OPSWAT File Upload Security Solution for your Web Applications delivers a robust security suite that can **detect malware, prevent zero-day attacks, and help maintain regulatory compliance**. It also enables organizations to check for vulnerabilities in uploaded binaries and executables and provides options to investigate threats in Sandboxes and against a global threat intelligence database.

Applications that accept file uploads are hosted on a wide range of infrastructure.

OPSWAT File Upload Security solution is available for multiple channels as a plug and play solution that can easily integrate with your existing architecture.

About OPSWAT

OPSWAT is a global leader in critical infrastructure cybersecurity that helps protect the world's mission-critical organizations from malware and zero-day attacks. To minimize the risk of compromise, OPSWAT Critical Infrastructure Protection solutions enable both public and private organizations to implement processes that ensure the secure transfer of files and devices to and from critical networks.

More than 1,500 organizations worldwide spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems trust OPSWAT to secure their files and devices; ensure compliance with industry and government-driven policies and regulations, and protect their reputation, finances, employees and relationships from cyber-driven disruption.

Methodology

Dimensional Research, an independent research firm specializing in enterprise technology, invited independent sources of IT security professionals to participate in an online survey. A variety of questions were asked on topics including overall IT security, current file upload environments, and security of external file uploads.

A total of 302 qualified participants completed the survey. All had direct responsibility for the security of web applications or portals that accept at least 500 file uploads per day (with more than half dealing with at least 5,000 daily uploads and 18% with more than 50,000/day) from customers or partners. This global survey included individuals from around the world who worked at companies with at least 250 employees (with more than 75% with at least 1,000 employees).

Footnotes

1 FBI Internet Crime Complaint Center (IC3) 2020 Internet Crime Report

2 Identity Theft Resource Center® (ITRC)

OPSWAT.

OPSWAT Research Report
August 2021