BLIND SPOTS IN WEB APPLICATION SECURITY

Identify and combat the security gaps in your organization's defenses

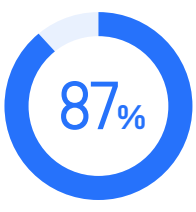


Unsecure File Uploads: A Key Area of Concern in Web Application Security

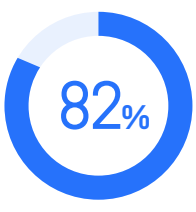
51% of surveyed organizations with a file upload portal process more than 5,000 file uploads per day.

99% of these companies are concerned about protecting against malware and cyberattacks from file uploads.

The Concerns Are Rising

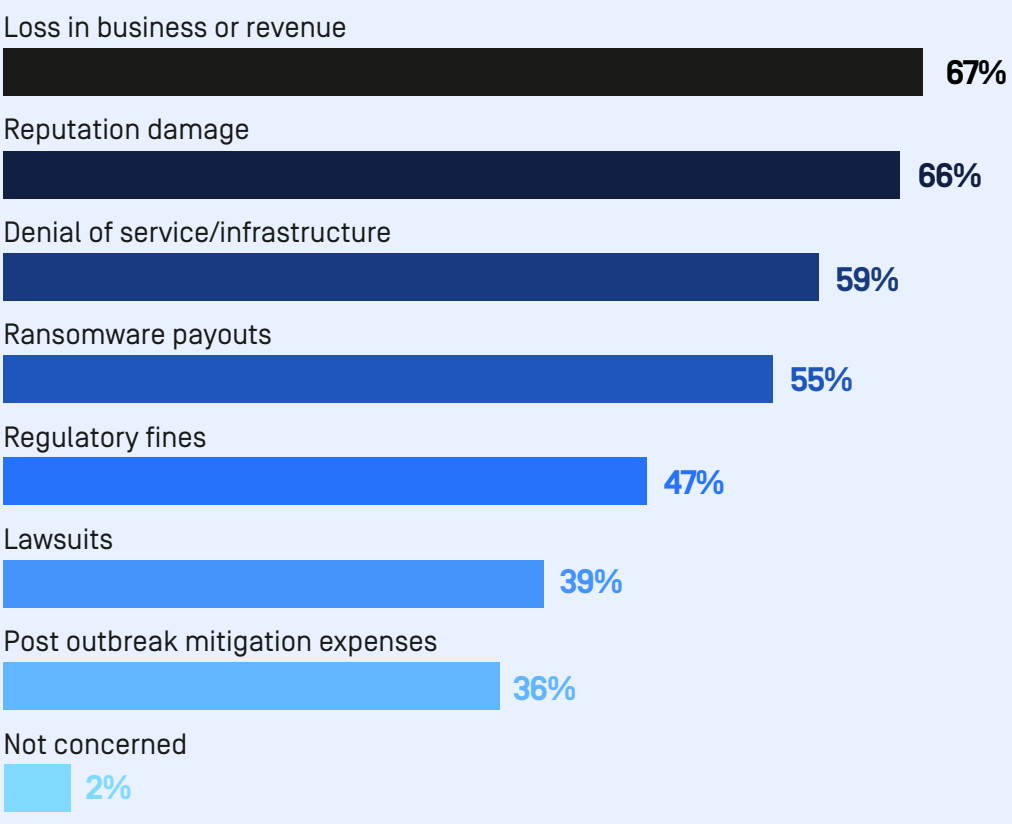


of organizations using a web application for file uploads are **extremely or very concerned** about secure file transfers.



of these organizations reported an **increase in concern** over the past year.

Organizations are concerned about these consequences



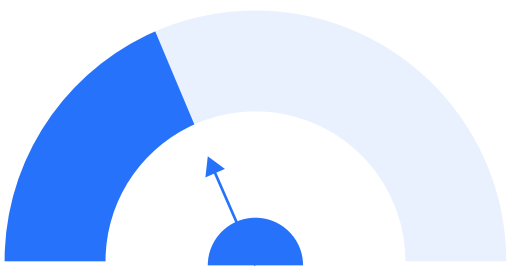
However,

Only 8% of surveyed organizations implement all 10 recommended best practices for file upload protection*

- Authenticate Users
- Set Maximum File Name Length and Size
- Scan All Files for Malware
- Use Simple Error Messages
- Store Uploaded Files Outside the Web Root Folder
- Verify Actual File Types
- Limit the Specific File Types
- Randomize File Names
- Check Files for Vulnerabilities
- Remove Embedded Threats with CDR

as identified by OPSWAT

Less than half of the organizations implemented more than five of the 10 best practices



Blind Spots in File Uploads that Create Severe Security Gaps

ANTI-VIRUS SCANNING

69%

Only two-thirds (69%) of organizations with web applications for file uploads are scanning all uploaded files with anti-virus and anti-malware engines.

DATA SANITIZATION

35%

Only one-third (35%) of organizations have deployed CDR (Content Disarm & Reconstruction) technology, which means many organizations are vulnerable to zero-day attacks.

OPSWAT Helps Organizations Achieve Comprehensive Web Application Security

THE BLIND SPOT	THE OPSWAT ADVANTAGE
Anti-Virus Scanning	**Malware Multiscanning** Achieve detection rates greater than 99% Simultaneously scan uploaded files with 30+ anti-virus and anti-malware engines
	The outcome: Organizations can detect threats sooner, respond to outbreaks faster, and minimize false positives.
Data Sanitization	**Deep CDR** An advanced threat protection technology that sanitizes file components and effectively 'disarms' all threats to create safe-to-consume files. Sanitize and reconstruct 100+ common file types and verify 4,500+ file types to prevent spoofing
	The outcome: Organizations can protect themselves against known and unknown threats, zero-day attacks, advanced persistent threats (APT), and sophisticated evasive malware.
Sensitive Data Loss	**Proactive DLP** Detect and automatically redact or block sensitive data from productivity documents, text files, and even non-searchable PDFs
	The outcome: Organizations can mask PII (Personally Identifiable Information) of customers and other confidential and proprietary data to prevent data loss and minimize the risk of regulatory compliance violations and expensive fines, penalties, and lawsuits.

Download the Web Application Security Report 2021 at info.opswat.com/web-application-security-report-2021

OPSWAT.
Trust no file. Trust no device.