APPLICATION SECURITY

WHAT IS APPLICATION SECURITY?

Application security is a set of processes, technologies, and practices aimed at safeguarding applications against risks across their entire lifecycle.

WHY APPLICATION SECURITY?

According to various studies, bulk of the successful breaches targeted vulnerabilities in application layer, underscoring the necessity for enterprise IT departments to be extremely diligent about application security. Application security includes hardware, software, and methods for detecting and mitigating security issues.

*Source: atatus

WHAT ARE THE DIFFERENT TYPES OF APPLICATION SECURITY FEATURES?

Authentication

This feature ensures that the application is only accessible to authorized users.

Authorization

A user can be authorized to access and use an application once they have been authenticated.

Encryption

Encrypting the data prevents fraudsters from accessing important information.

Log record

Logging can assist with recognizing who had the option to access an application and how if a security break was to happen.

Application security testing

Testing the security of an application is an important step in ensuring that all security features are functioning properly.

EXAMPLES OF TOP APPLICATION SECURITY IN 2021:

Mobile application security- The use and need for mobile phones are increasing drastically over the years and these mobiles also transmit data within various networks. Any threat actor can exploit the vulnerabilities in the mobile app and the user will realize it only after the attack is executed.

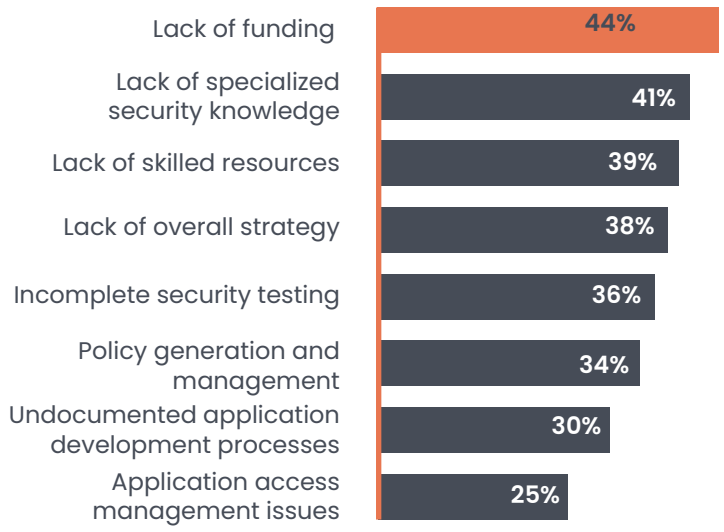
Enterprise application security- Intellectual property, sensitive data, and files protected by employee data privacy laws often pass-through enterprise apps, making security essential in 2021 for both, large- and small-scale industries.

Web application security- Several businesses use web apps during their daily workflows – for example, a no-installation browser-based video conferencing tool to quickly initiate a meeting.

Cloud application security- Most businesses are accelerating their cloud investments in 2021 for the following reasons:

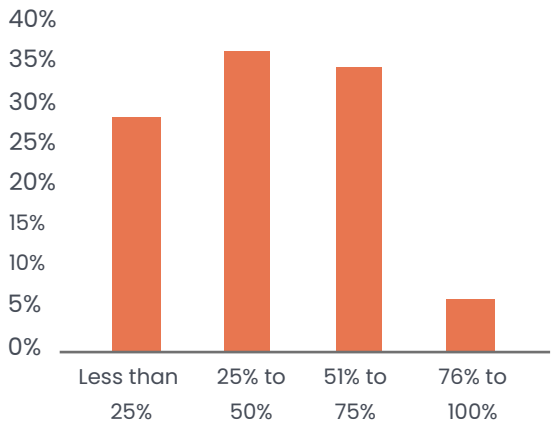
- Providing anytime, anywhere access to remote workers
- Reducing reliance on physical data centers

Challenges: According to Forrester's latest report, maximum attacks take place through vulnerabilities in software (42%) or by exploiting a web application (35%). Also, as a total, cybercrime has risen over 600 percent since the worldwide epidemic began. How we do business has been irrevocably altered by lockdowns. Just one single click may jeopardize a whole network.

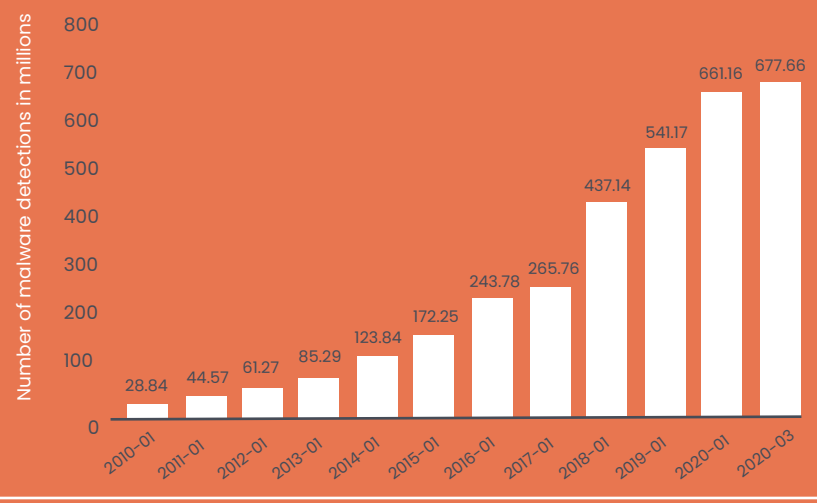


Challenges to ensuring protected applications

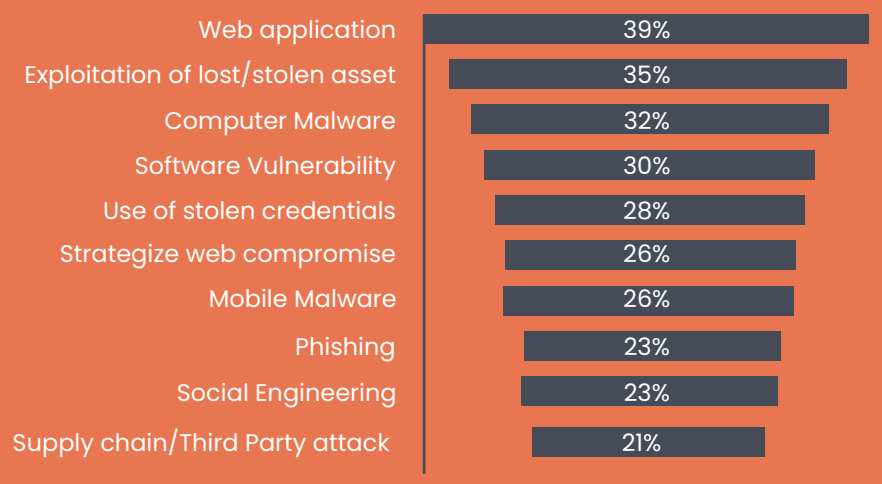
*Source: IDG Research services, April 2017



Percentage of apps organizations exposed to the internet or to third party services via APIs



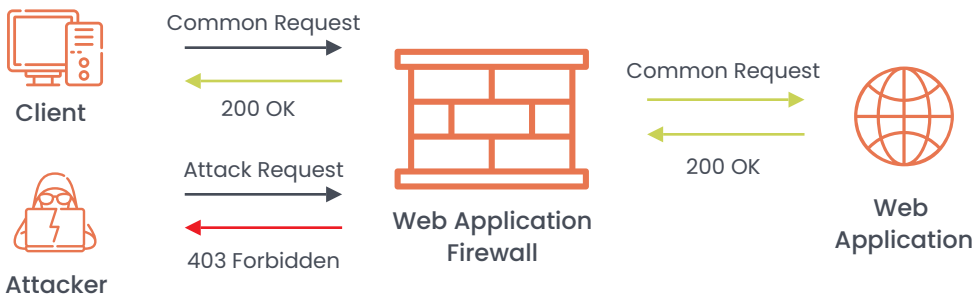
How was the external attack carried out?

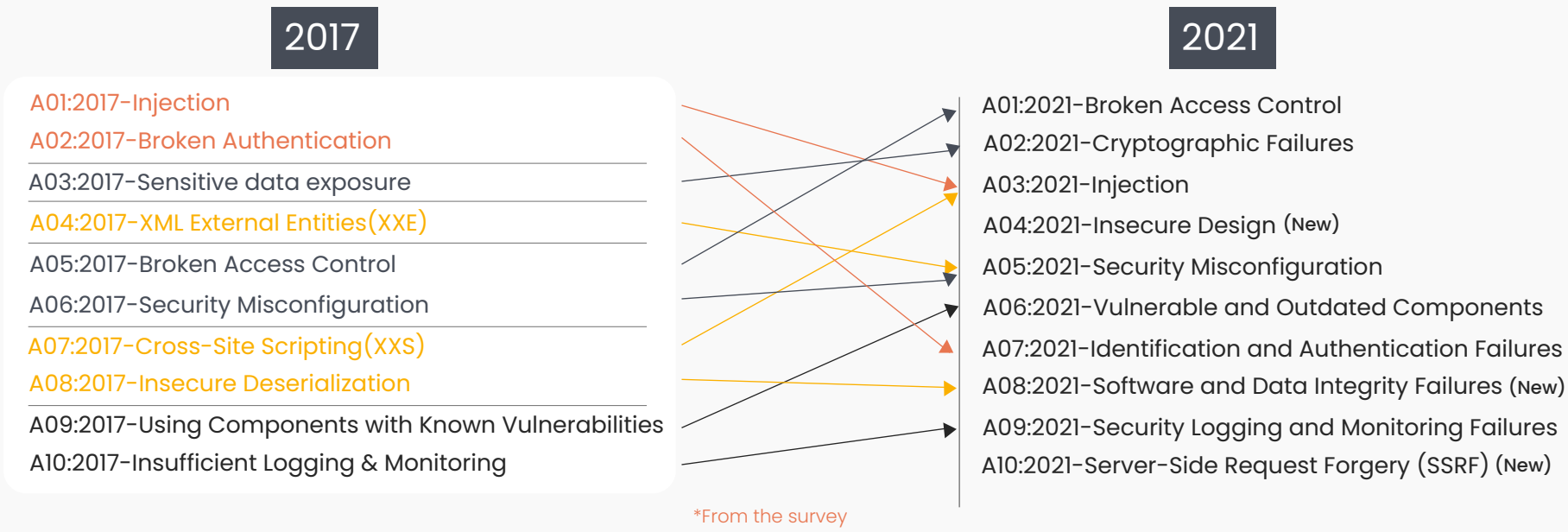


*Sources: Forrester Analytics Business Technographics® Security Survey, 2020 and "The State Of Web Application And API Protection," Radware.

OVERCOMING THE APPLICATION SECURITY CHALLENGES:

According to OWASP, businesses should adopt this paper and start the process of ensuring that their web applications are secure. The OWASP Top 10 is likely the most effective first step in transforming your company's software development culture to one that produces more secure code.





*From the survey

OWASP TOP 10' VULNERABILITIES OF 2021

A01:2021-Broken Access Control: Tops the list as 94% apps had instances of broken access than any other category with 34 CWEs mapped to it.

A02:2021-Cryptographic Failures: Previously known as Sensitive data exposure which was a symptom rather than the root cause. The focus here is on the cryptographic failures which frequently leads to data leakage or system penetration.

A03:2021-Injection: The 33 CWEs mapped into this category had the second most occurrences in applications, with 94 percent of the apps evaluated for some sort of injection. In this edition, cross-site scripting has been added to this category.

A04:2021-Insecure Design (*new): Focuses on risks related to flaws in design. More threat modelling, safe design patterns and principles, and reference architectures are required if we truly wish to "go left" as an industry.

A05:2021-Security Misconfiguration: It's hardly unexpected to see this category rise as more people turn to highly configurable software. This category now includes the old XML External Entities (XXE) category.

A06:2021-Vulnerable and Outdated Components: was previously titled Using Components with Known Vulnerabilities and came in second place in the industry survey, but it also had enough data to make the Top 10 via data analysis. This category has risen from #9 in 2017 and is a well-known problem that we find difficult to test and assess risk. It is the only category not to have any CVEs mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.

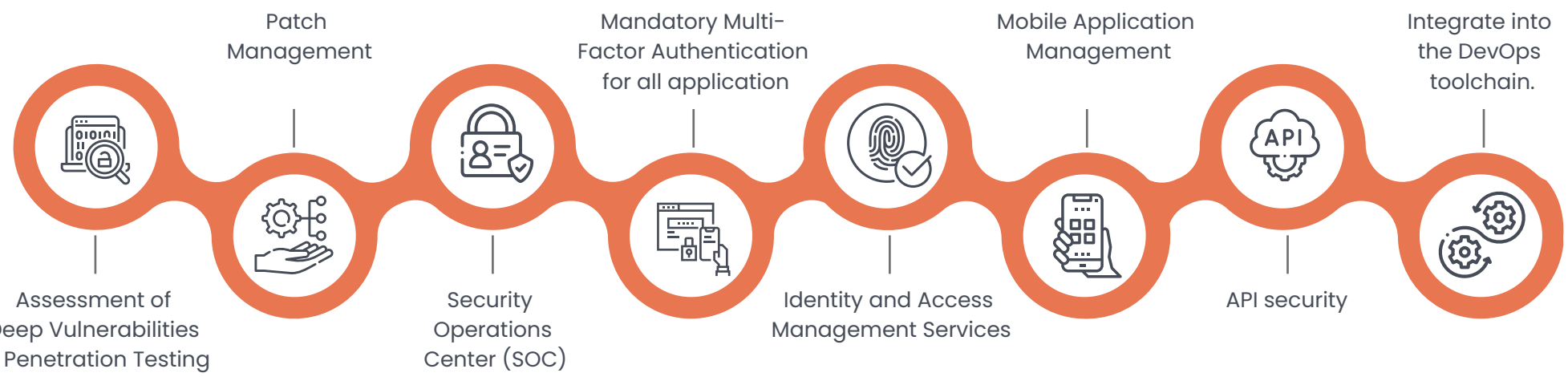
A07:2021-Identification and Authentication Failures: previously known as Broken Authentication, CWEs that are more related to identification failures are now included. Although this category remains in the Top 10, the increased availability of standardised frameworks appears to be helping.

A08:2021-Software and Data Integrity Failures (*new): Focuses on assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. Insecure Deserialization, which was introduced in 2017, has now been absorbed into this broader category.

A09:2021-Security Logging and Monitoring Failures: This category has been expanded to include a wider range of failures, is difficult to test for, and is underrepresented in the CVE/CVSS data. Failures in this area, on the other hand, can have a direct influence on visibility, incident alerting, and forensics.

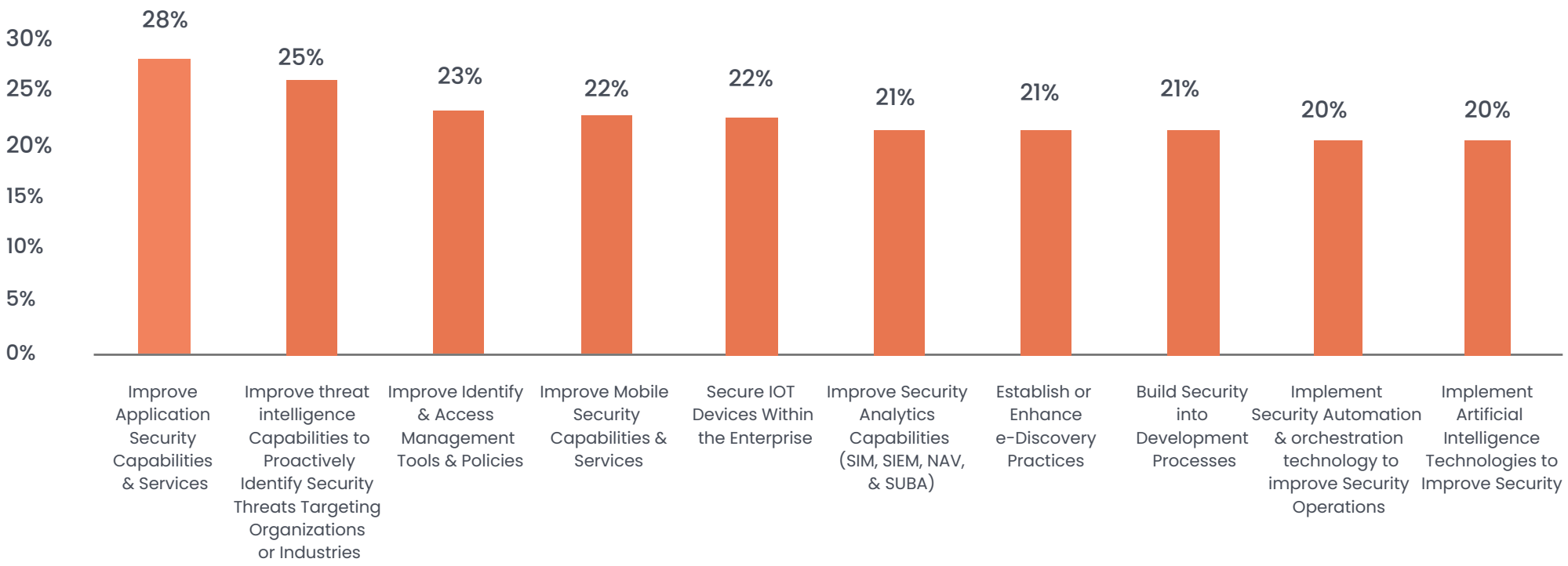
A10:2021-Server-Side Request Forgery (*new): This category depicts the situation in which industry professionals tell us that something is vital, even though it isn't reflected in the data at the moment.

FOLLOWING ARE SOME OF THE BEST PRACTICES EVERY ORGANIZATION MUST FOLLOW TO ENSURE APPLICATION SECURITY:



Firms Have Prioritized Application Security and the shift to the left continues, but firms are inconsistent in their adoption of new application security tools.

Which of the following initiatives are likely to be your organization's top tactical information/IT security priorities over the next 12 months?



*Source: Forrester Analytics Business Technographics® Security Survey, 2020

> If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people's accounts. If they know there's a key hidden somewhere, they won't stop until they find it.
>
> -Tim Cook (Chief Executive Officer of Apple)

SKILLMINE CYBER SECURITY TEAM

Skillmine
Technology • Consulting • Services
India | KSA | UK | USA

#46/4, Novel Tech park,
Kudlu Gate, Bangalore
Karnataka-560 068

+91 9920663515
www.Skill-mine.com
info@Skill-mine.com

Follow us on