2021

Cybersecurity INSIDERS

APPLICATION SECURITY REPORT

FORTINET®

INTRODUCTION

The 2021 Application Security Report is based on a comprehensive global survey of 344 cybersecurity professionals. This report reveals that the expanded use of applications for business-critical applications, combined with the increased pace of application changes that come with DevOps methodologies, has created security challenges for organizations.

The responses we received highlight the need to invest in application security tools and processes that can be easily deployed and managed.

Key findings include:

- Only 43% of organizations are very or extremely confident about their application security, with protecting data (46%) as a top concern.
- Forty-three percent of organizations confirmed they experienced application breaches or compromises in the past. More than a third of respondents (35%), however, acknowledged that they did not know when the last breach occurred.
- With an average of 25 software updates being published into production every month, consistent and frequent threat and vulnerability testing is critical. Only 21% of respondents confirmed that they test every time the code changes.
- Lack of skilled personnel tops the list of barriers that organizations are facing when securing their web applications (46%).

We would like to thank Fortinet for supporting this important industry research project.

We hope you find this report informative and helpful as you continue your efforts in securing your web applications.

Thank you,

Holger Schulze

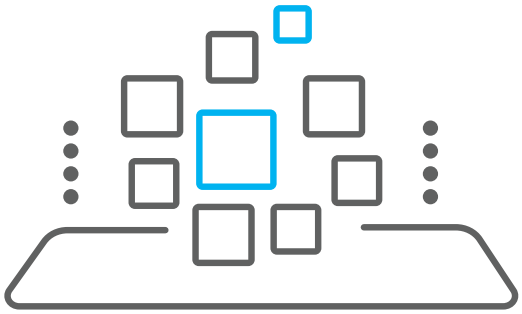
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

APPLICATION PROLIFERATION

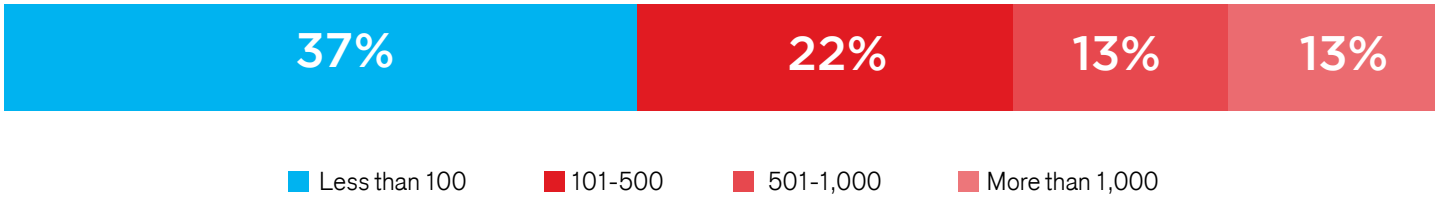
Applications are quickly multiplying in organizations, with half of those surveyed reporting they have more than 100 unique apps in their environment.

How many unique applications are in your environment?



48%

of the organizations have 100 or more unique applications in their environment*



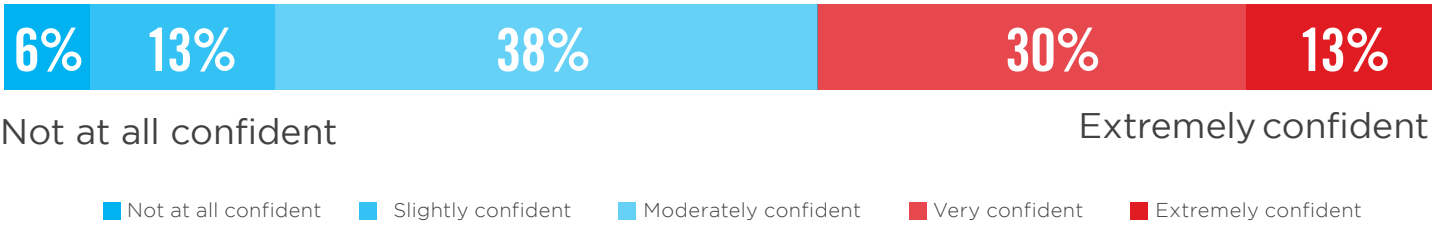
*Don't know/not sure 15%

APPLICATION SECURITY CONFIDENCE

Applications increasingly touch organizations' most sensitive data in order to support business-critical workflows. Only 43% of organizations are very or extremely confident about their application security, with protecting data (46%) as a top concern.

How confident are you in your organization's application security posture?

43% of organizations are moderately to extremely confident about security

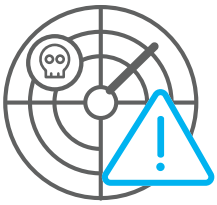


What are your biggest application security concerns?

46%
Protecting data

43%
Keeping up with the rising number of vulnerabilities

39%
Securing applications we develop



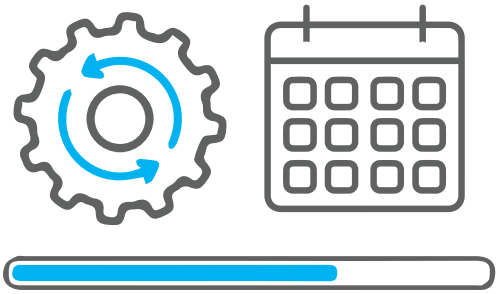
38%
Threat detection/ breach detection

Securing cloud apps 37% | Malware 28% | Effective threat modeling 28% | Securing mobile apps 26% | Meeting regulatory/ compliance requirements 26% | Effectively prioritizing and remediating vulnerabilities that pose the most risk 25% | Securing business apps (ERP, etc.) 23% | Meeting customers' security needs and requirements 21% | Securing open source software 21% | Securing commercial off-the-shelf software 17% | Securing embedded/IoT/hardware 17% | Securing blockchain 6% | Not sure/ other 6%

SOFTWARE UPDATES

We asked how many software updates organizations typically publish into production each month. On average, companies publish around 25 monthly software updates.

On average, how many software updates do you publish into production on a monthly basis?



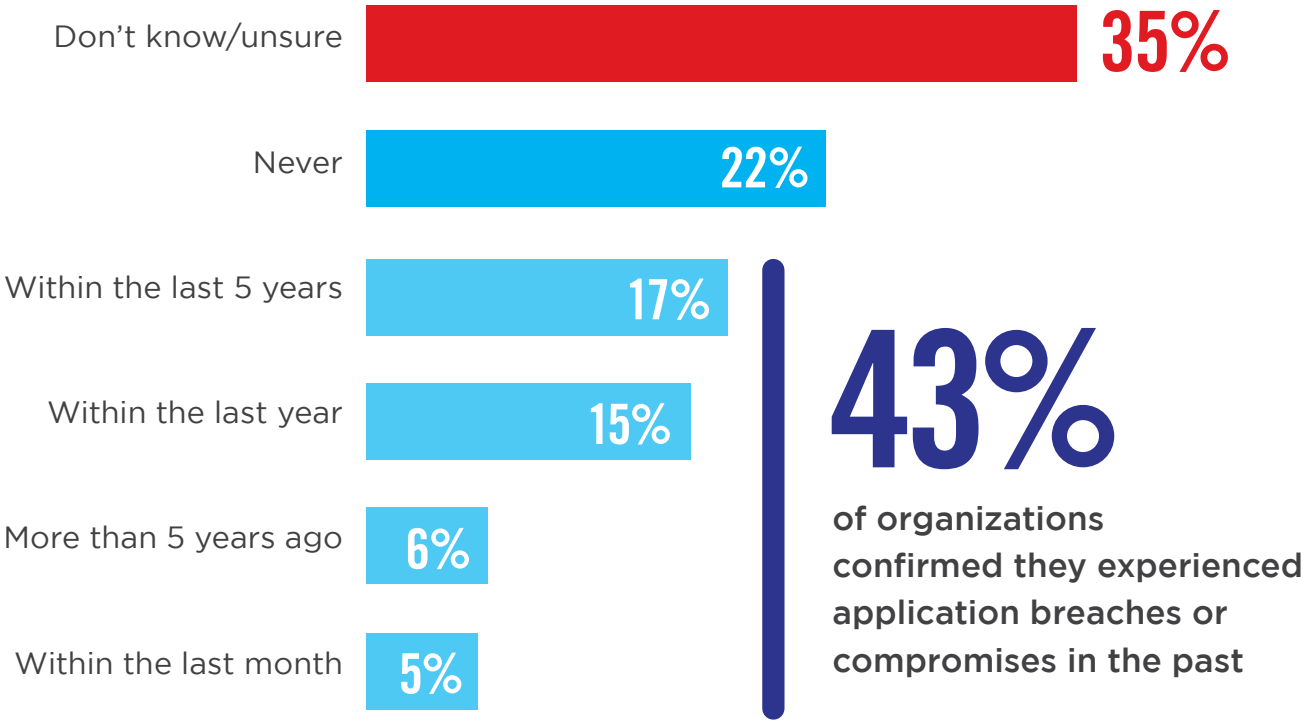
On average, companies publish

25 software updates into production on a monthly basis

COMPROMISED APPLICATIONS

Forty-three percent of organizations confirmed they experienced application breaches or compromises in the past. More than a third of respondents (35%), however, acknowledged that they did not know when the last breach occurred. This raises the question as to whether this is a tools and processes issue or just simply outside the respondent's remit.

When was the last time that one of your company's applications was breached/compromised?



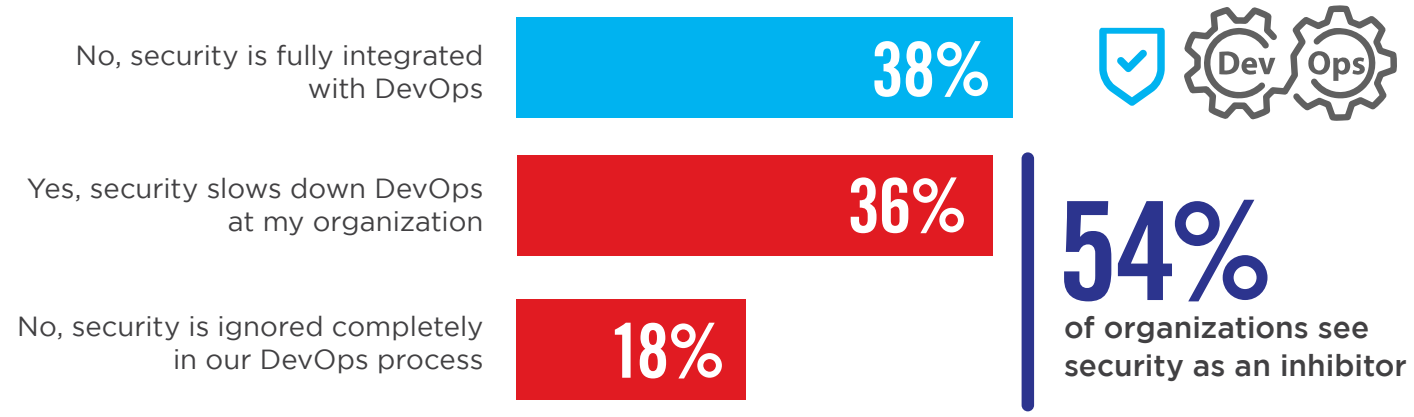
43%

of organizations confirmed they experienced application breaches or compromises in the past

SECURITY & DEVOPS

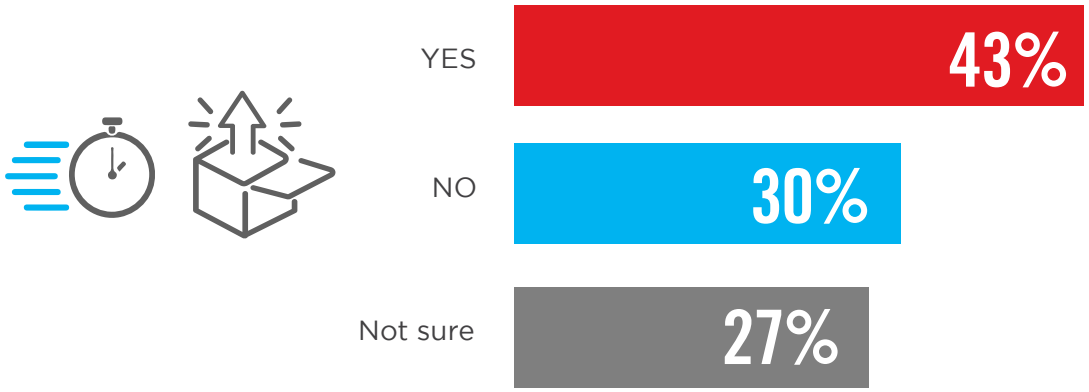
The survey results illustrate that it is still a challenge within organizations to get their security and development teams to work in lockstep. Security is still viewed as an inhibitor in 54% of organizations, and 43% admitted that they sometimes sacrificed security while prioritizing application delivery.

Does security slow down continuous development methods like DevOps at your organization?*



*Other 8%

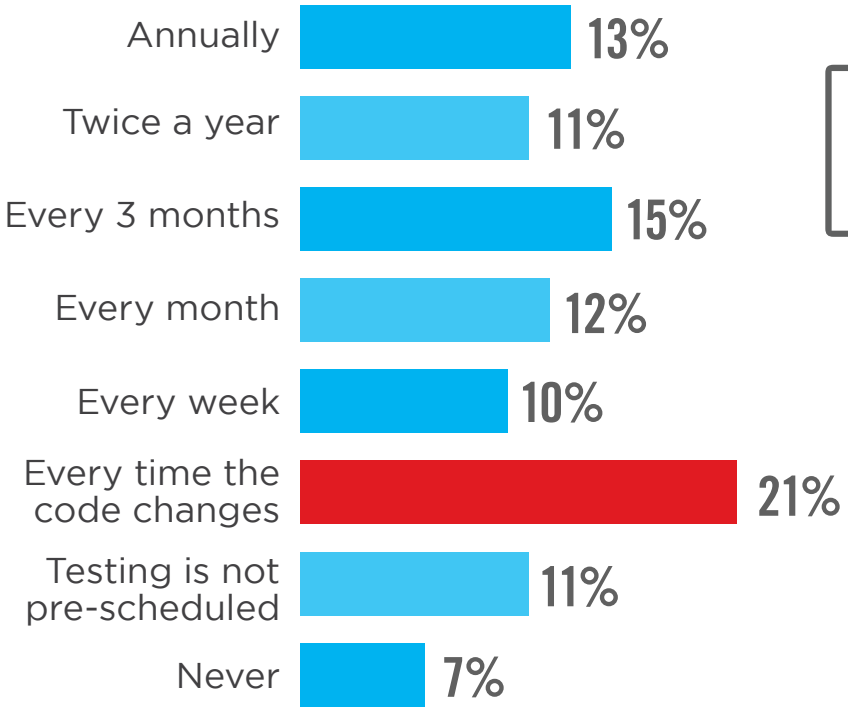
Does the "rush to release" cause application developers in your organization to neglect secure coding procedures and processes?

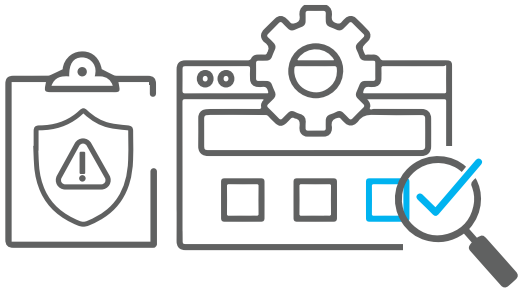


VULNERABILITY TESTING

With an average of 25 software updates being published into production every month, consistent and frequent threat and vulnerability testing is critical. Only 21% of respondents confirmed that they test every time the code changes, which means that many organizations are incurring risks that can be prevented by tools and processes fueled by automation.

How often does your organization test applications for threats and vulnerabilities?





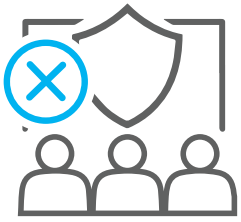
SECURITY BARRIERS

Lack of skilled personnel tops the list of barriers that organizations are facing when securing their applications (46%). This skills gap has been a known and ongoing issue that is unlikely to be resolved anytime soon. One way organizations can mitigate this issue is by investing in tools and processes that can automate previously-performed manual security tasks.

Which of the following barriers inhibit your organization from adequately defending against cyberthreats?

46%

Lack of skilled personnel

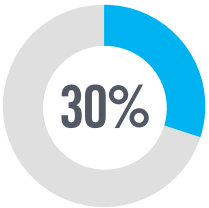


43%

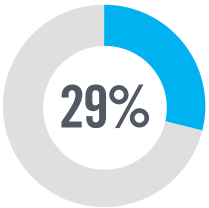
Low security awareness among employees

39%

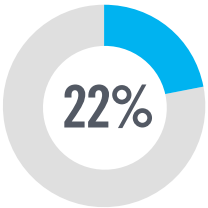
Lack of budget



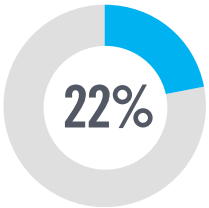
Lack of collaboration between separate departments



Lack of management support/ awareness



Too much data to analyze



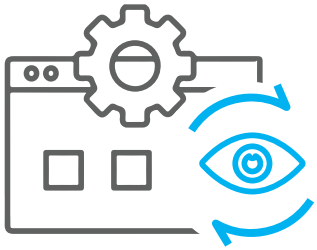
Poor integration/ interoperability between security solutions

Inability to prioritize vulnerabilities based on risk 21% | Lack of investment in effective solutions 20% | Lack of contextual information from security tools 14% | Inability to justify additional investment 13% | None 7% | Not sure/other 10%

APPLICATION MONITORING

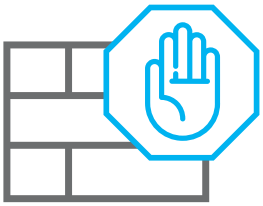
Half of organizations (50%) are actively monitoring applications in production to collect and respond to threat intelligence. They're using a variety of methods to monitor security issues, with Web Application Firewalls (WAF) being one of the primary solutions for web application security (43%).

How are you currently monitoring applications for security issues?



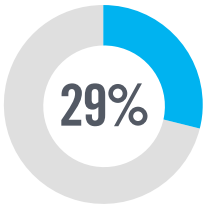
50%

We actively monitor applications running in production to collect and respond to threat intelligence

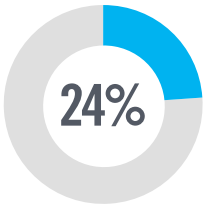


43%

We use a Web Application Firewall (WAF) to protect our application



We have a feedback loop to share incidents and/or possible vulnerable information with the development and design teams



We use code signing in deployment of our apps

Don't know/other 17% | None of the above 11%

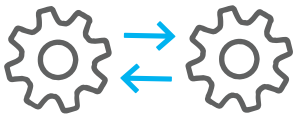
SELECTION CRITERIA

When asked about their most important buying criteria for application security solutions, respondents answered that pricing was the single biggest factor for most (54%). This is closely followed by ease of integration (53%). Combined with the noted skills shortage, this would suggest that teams will continue to be resource constrained, increasing the reliance on automation and platforms such as WAF, to strengthen their security posture and produce efficiencies.

What are your most important criteria when selecting an application security tool or service?

54%

Pricing/ licensing

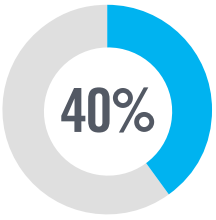


53%

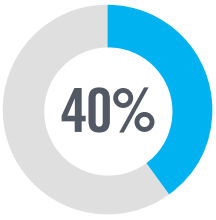
Ease of integration

42%

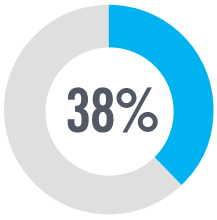
Scalability



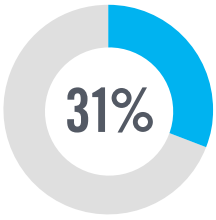
Ease of use



Accuracy



Comprehensiveness of capabilities



Enterprise-class support

Credibility (established vendor) 29% | Time required to get the tool up and running in my environment 18% | SaaS option 16% | Don't know/other 11%

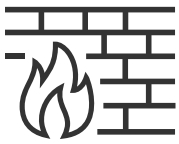
API WORKLOADS

Forty-six percent of organizations are using solutions such as cloud-based WAF for securing both on-premise and cloud. As their security solutions evolve, these organizations are now looking for more modern solutions that offer cloud-based options and API protection, as confirmed by 79% of cybersecurity professionals overall. These modern features can help mitigate resource constraints to provide more flexibility and comprehensive protections for apps.

Are you using a cloud-based WAF for securing both on-premise and cloud?

46% are using a cloud-based WAF for securing both on-premise and cloud

Is it important to you that a WAF understand API workloads and be able to protect them?



79% of organizations say it is important that a WAF understand API workloads and be able to protect them

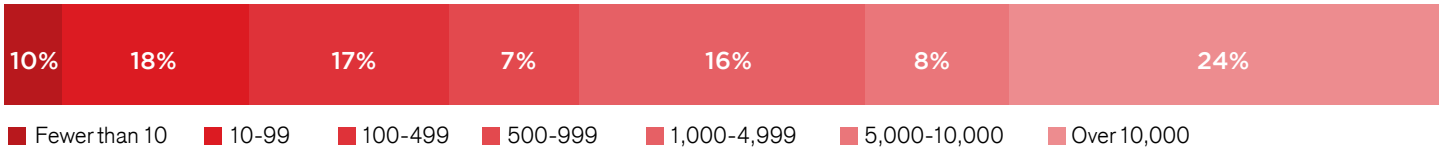
METHODOLOGY & DEMOGRAPHICS

The 2021 Application Security Report is based on the results of a comprehensive online global survey of 344 cybersecurity professionals, conducted in July 2021, to gain deep insight into the latest trends, key challenges, and solutions for application security. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

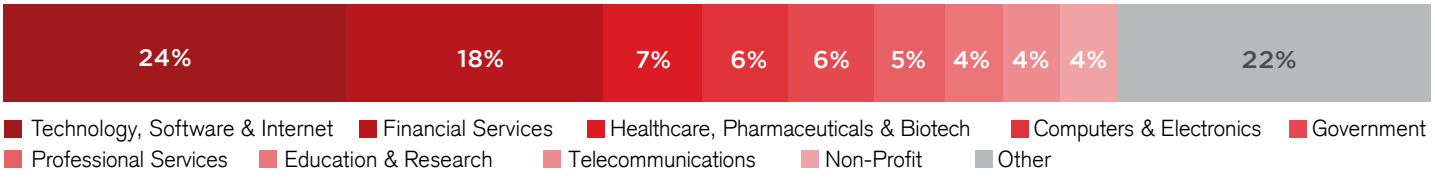
CAREER LEVEL

DEPARTMENT

COMPANY SIZE



INDUSTRY



Fortinet (NASDAQ: FTNT) secures the largest enterprises, services providers, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networks, application, multi-cloud, or edge environments. Fortinet ranks #1 as the company with the most security appliances shipped worldwide and more than 500,000 customers trust Fortinet to protect their businesses.

www.fortinet.com