CROWDSTRIKE

2024 State of Application Security Report

Table of Contents

Executive Summary

Application security is the practice of protecting and securing applications throughout the software development life cycle. As organizations shift their focus to driving revenue through software, application security (AppSec) is becoming one of the most essential forms of security for modern enterprises to invest in.

Beyond generating revenue, software is also the backbone of the customer experience and is vital to creating a respected brand. In short, applications run the world.

At the same time, the attack surface is shifting to application and APIs from classic infrastructure configuration and permissions. **Eight out of the top 10 data breaches of 2023 were related to application attack surfaces.**[1]

These eight breaches alone are estimated to have exposed around 1.7 billion records. **The staggering number of records exposed proves that the status quo in application security isn't enough.** But before we can develop the next generation of preventive and remediative AppSec solutions, we need to understand the predominant challenges facing those on the front lines. Much like developing a vaccine or an antiviral, we need some data to figure out if we're addressing the most critical issues. Which problems are we trying to solve? What's really going on in application security teams? What are their greatest challenges? How are they doing their jobs today?

This report synthesizes data collected from a survey of application security professionals to reflect the current state of application security. **Here are the key findings:**

1. **More frequent deployments mean more languages to manage.**
   Organizations that deploy 1x/day or more use 5+ programming languages.
2. **Teams use manual processes to inventory and catalog apps and APIs.**
   74% rely on documentation, and 68% rely on spreadsheets.
3. **Only 54% of major code changes go through full security reviews.**
   22% review a quarter or less.
4. **Traditional security reviews are time-consuming and expensive.**
   81% report that security reviews take longer than one business day, and 35% say that security reviews take longer than three business days.
5. **Security teams are using multiple tools.**
   90% use 3+ tools to detect and prioritize application vulnerabilities and threat.
6. **Prioritizing what to fix first is a top challenge.**
   61% of AppSec professionals cite it as their top challenge working with developers.
7. **Remediation is slow.**
   70% of critical issues take 12 hours or more to resolve.
8. **Different-sized organizations have differing views on application security responsibility & accountability.**
   Smaller orgs (100-999 employees) see the CTO (22%) as most responsible; larger orgs (1,000 employees or more) view AppSec teams (23%) and DevSecOps (22%) as most responsible.

---

[1] Source: According to industry data, List of Data Breaches and Cyber Attacks in 2023 by IT Governance looking at data breaches by the total number of records impacted.

Key Finding #1:

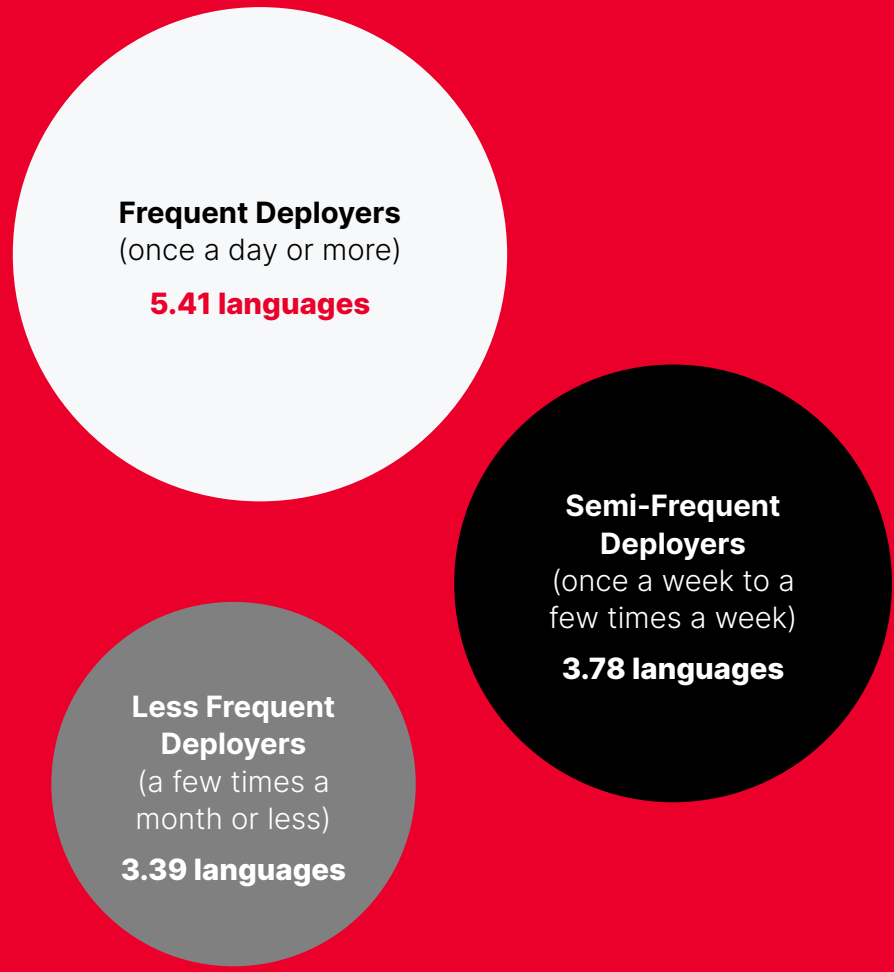
Frequent Deployments Mean More Programming Languages to Manage

Continuous integration and continuous delivery (CI/CD) became mainstream in 2011 alongside the release of Jenkins. With each passing year, software teams are empowered to push code into the world faster than before.

Companies eager to quickly produce software features allow development teams to choose the programming language for each project. **As the number of software projects, the number of development teams and the frequency of deployment increase, so does the number of programming languages used within an organization.**

Programming language sprawl complicates the job of application security professionals, as security teams must learn secure coding paradigms in multiple programming languages. Furthermore, they must find tools that support each coding language used internally.

Number of Programming Languages by Deployment Cadence



Key Finding #2:

Teams Rely Heavily on Manual Processes to Inventory/Catalog Application Microservices and APIs

Despite frequent deployment — 71% of organizations report releasing application updates at least once a week — **teams are primarily using documentation (74%) and spreadsheets (68%) to catalog and inventory their applications and APIs.**

These methods rely heavily on humans, making them prone to error. Furthermore, a faster deployment velocity makes it difficult for teams to have up-to-date, accurate information.

Prevalence of Manual Processes to Catalog Applications and APIs

Method	Percentage of Respondents
Documentation	74%
Spreadsheets	68%
Custom in-house service catalog	61%
CMDB	54%

Key Finding #3:

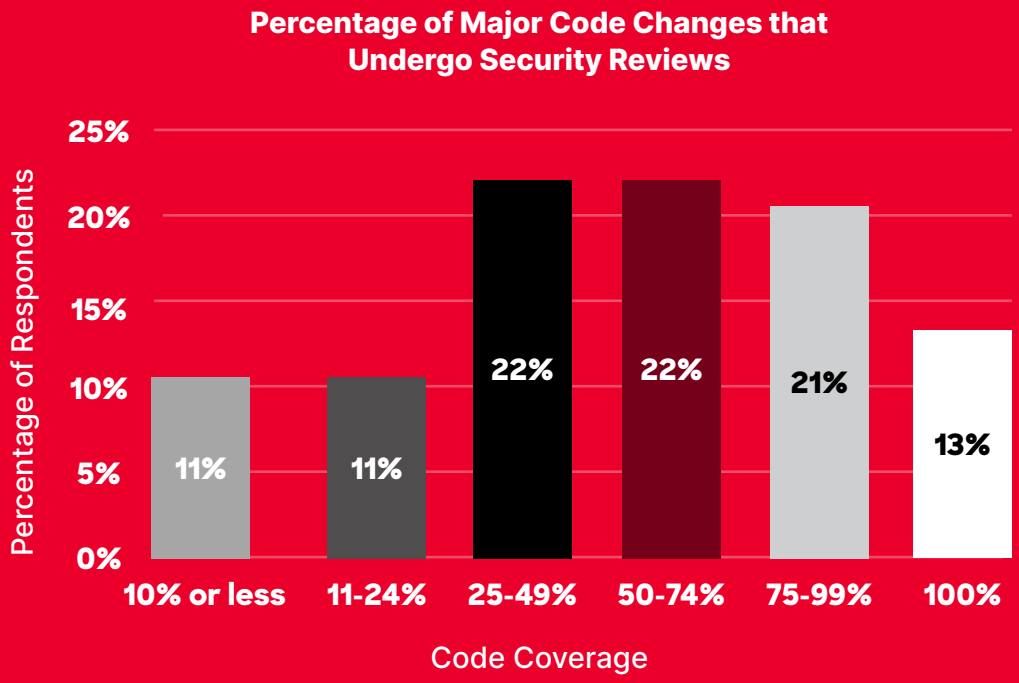
Only About Half of All Major Code Changes Go Through Full Security Reviews

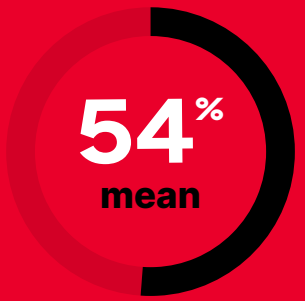
If the crew on your next flight decided to skip the standard preflight checks because they had already covered their quota for the day, would you feel safe? Probably not. The same goes for code.

Survey respondents estimated that, on average, **54% of major code changes undergo a full security review before deploying to production.**

When looking at the breakdown of responses, 22% report reviewing 50-74% of code changes, 22% review 25-49% of code changes and 22% review 24% or fewer code changes.

So why aren't teams reviewing more of their code changes? The next key takeaway provides some insight.



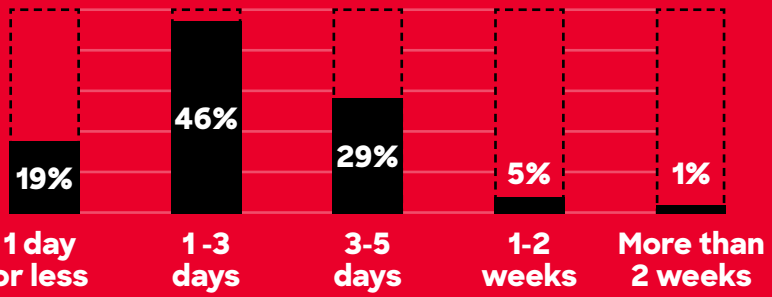


Key Finding #4:

Traditional Security Reviews Are Time-Consuming and Expensive

Interestingly, **81% of the respondents indicate that a security review takes more than one business day, with 35% saying it takes more than three business days.** Here's a full breakdown of how long security reviews take across the survey sample.

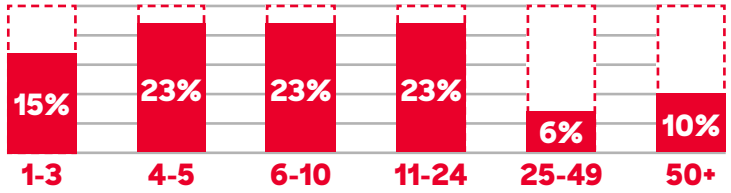
Duration of Security Reviews



Traditional security reviews are even more resource-depleting due to the number of people participating in them. Survey data shows that 10 is the median number of individuals involved in a security review.

10 median | **16.5** mean

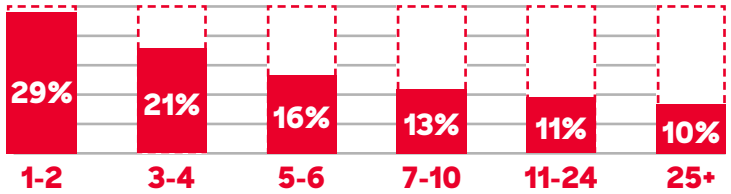
Number of Individuals Involved in Security Reviews



Despite taking significant time to complete and involving several individuals, organizations reported conducting a median of four security reviews per week, with 21% doing 11 or more each week.

4 median | **10** mean

Number of Security Reviews per Week



For organizations deploying frequently, security cannot be a bottleneck. In fact, DORA metrics identify elite DevOps performers as organizations with change lead times of one hour or less.[2] As an industry, if we are measuring security reviews in days – not hours – then there is opportunity for improvement.

[2] https://cloud.google.com/blog/products/devops-sre/using-the-four-keys-to-measure-your-devops-performance

Cost Breakdown of Security Reviews

A quick exercise to quantify the cost of security reviews for an average organization helps to more realistically understand the impact of this data.

Using conservative estimates from the survey data, let's say that security reviews take place during one-hour sessions. Using the median value of two days, respondents are estimated to dedicate roughly two hours (or one quarter of a standard eight-hour business day) to a single security review. The median values indicate there are four reviews per week, so it can be assumed each participant spends a full business day on security reviews each week.

If each individual contributing to the security review has a yearly salary of $100,000 USD, the cost of one day of work — for an individual with this salary is roughly $385 USD (based on 260 days per year and disregarding taxes, deductions, benefits, etc.).

Multiplying $385/week by the median number of employees involved (10) yields a total weekly cost of $3,850 USD.

If the team works 49 weeks out of the year, the annual cost of security reviews — without inclusion of tool costs — is $188,650 USD.

Doing the same calculation using mean values, which is more representative of large enterprises, yields a substantially higher annual cost. If each individual now participates in three separate one-hour sessions per review, and there are 10 reviews per week, then each participant is now spending 30 hours (or 3.75 business days) on security reviews each week. Multiplying by the mean number of security review participants, 16.5, shows the company is paying for 61.875 business-days-worth of security reviews each week. It is likely that, in the real world, there are more than 16.5 individuals involved across the organization, each of whom does less than 30 hours of work each week; however, that does not change the calculation. Using the same number of working weeks and salary cost as before, the estimated annual cost of security reviews becomes just over $1,167,000 USD.

Estimated Cost of Security Reviews

62

Business days' worth of security reviews each week

$1,167,000

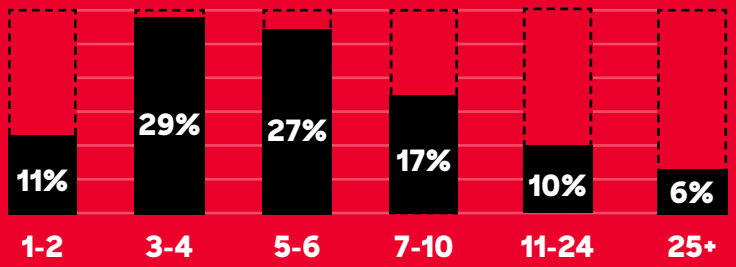
Estimated annual cost of security reviews

Key Finding #5:

Security Teams Are Using Multiple Tools

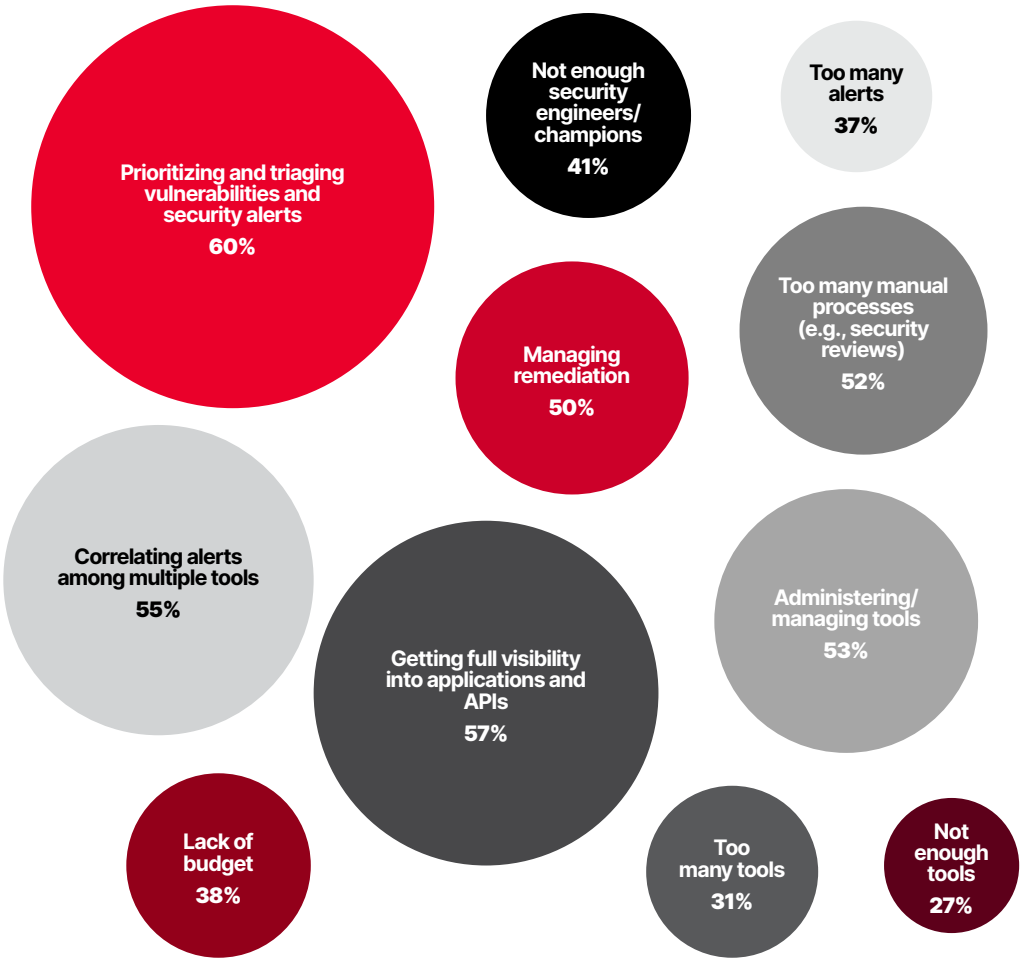
Almost 90% of security professionals report using three or more tools to detect and prioritize vulnerabilities and threats. Having multiple tools results in more complexity, more alerts to correlate and more spend.

Number of Tools Used to Find and Prioritize Vulnerabilities



These vulnerability management tools are not necessarily solving these teams' challenges. When asked to name their top application security challenges today, respondents pointed to prioritizing and triaging vulnerabilities and security alerts and getting full visibility into applications and APIs. Correlating alerts among multiple tools and managing those tools were also cited as issues.

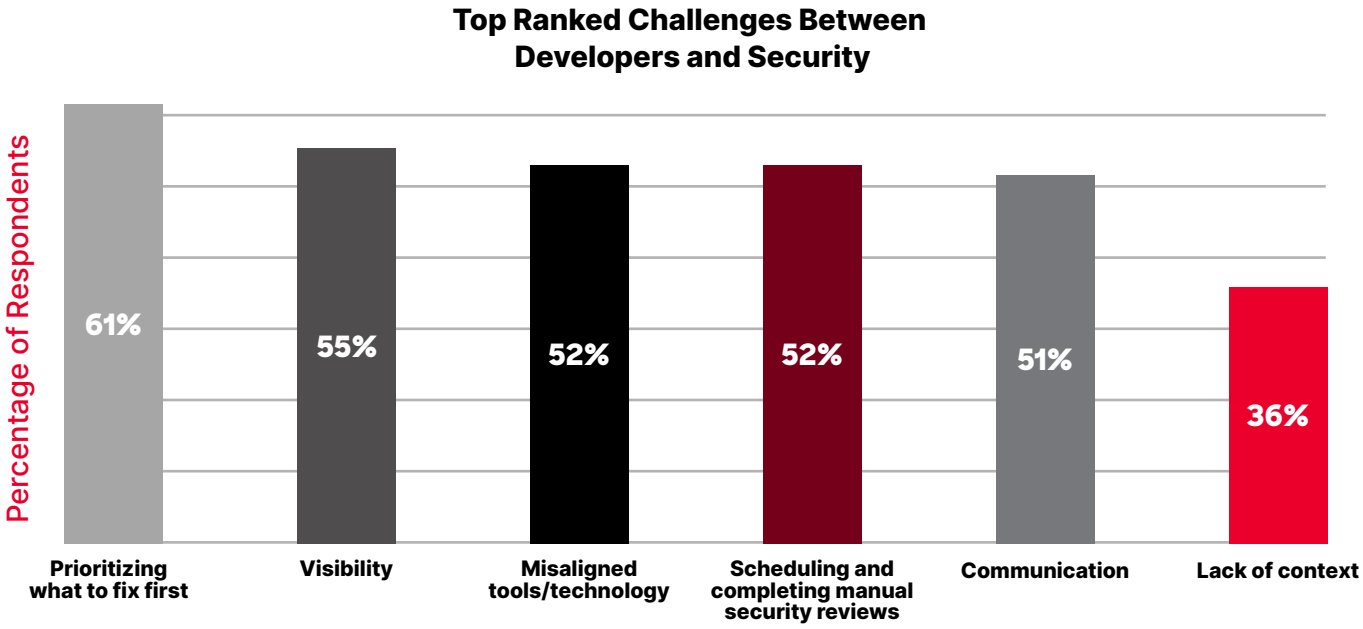
Application Security Challenges Ranking in Survey Respondents' "Top 5"



Key Finding #6:
Prioritization Is a Top Challenge

When asked to rank their top challenges when interacting with engineering teams/developers, **22% of respondents ranked prioritizing what to fix first as their top obstacle, with 61% ranking prioritization among their top three challenges.**

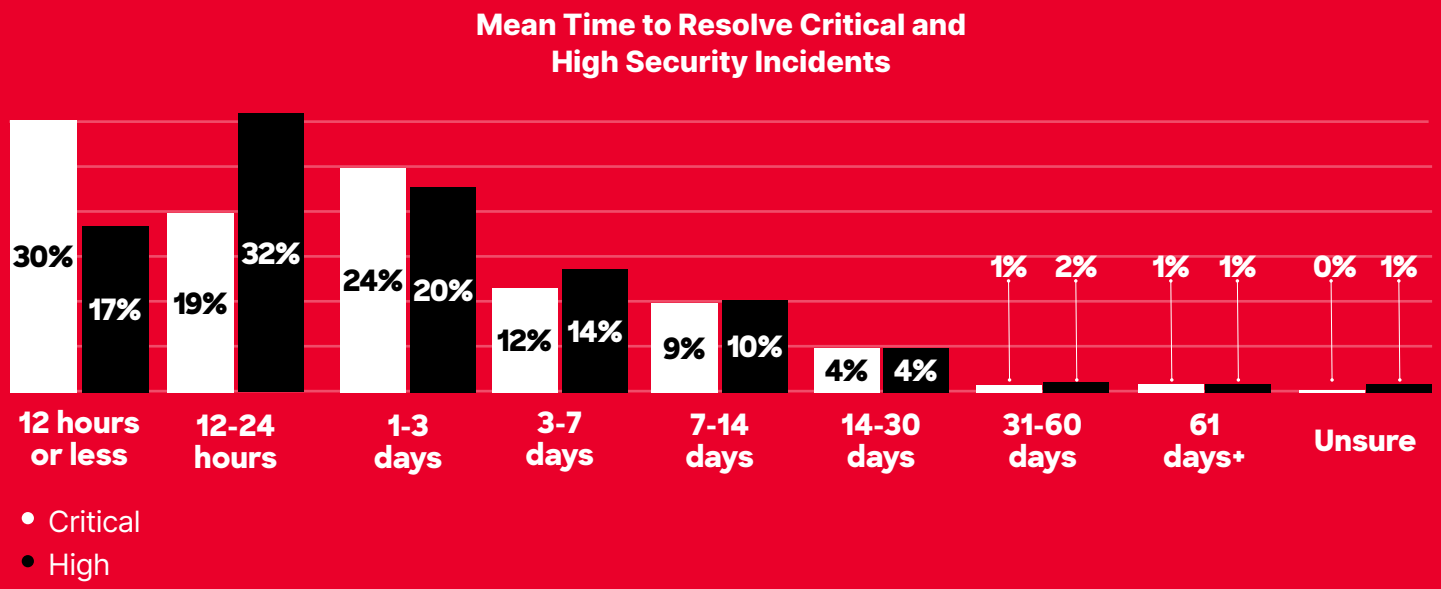
The second most prevalent challenge in the sample is visibility, with 21% of respondents ranking it as their top choice and 55% ranking it in their top three.



Key Finding #7:
Remediation is Slow

Only 30% of the respondents are able to resolve critical security incidents in 12 hours or less, meaning **70% of critical incidents take longer than 12 hours to resolve**

Organizations are releasing updates at a rapid pace, but they are not keeping up with the vulnerabilities and security incidents that follow.



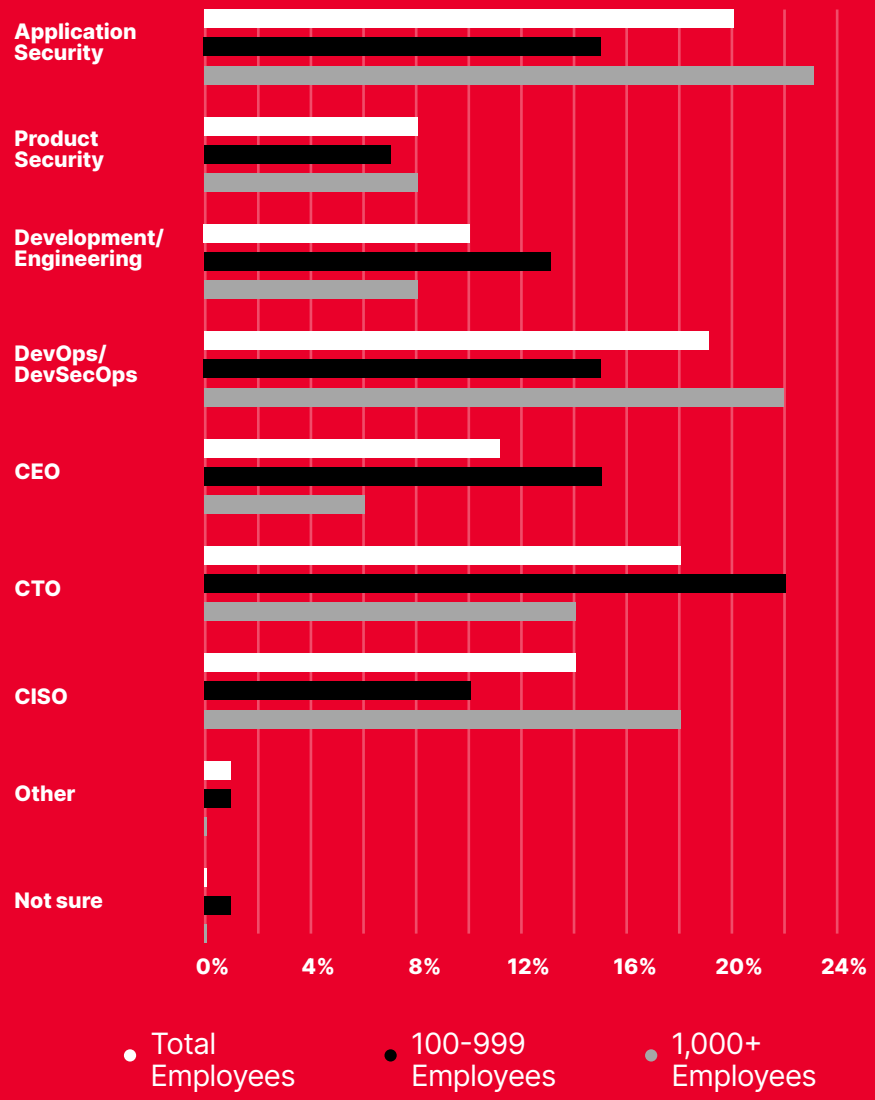
Key Finding #8:

Views on Application Security Responsibility and Accountability Change with Organization Size

Survey findings indicate that the individual or team most responsible and accountable for the security of applications varies across organizations of different sizes. Among respondents from smaller organizations of less than 1,000 people, 22% named the CTO as the most responsible and accountable. In larger organizations of over 1,000 people, 23% of respondents named the application security team as the most responsible and accountable, and 22% stated the DevOps/DevSecOps team was the most responsible.

In general, organizations with less than 1,000 employees are more likely to hold the CEO, CTO and software development teams accountable. As organizations grow past 1,000 employees, they are more likely to consider the CISO, DevOps team and application security team accountable.

Views on Application Security Responsibility and Accountability by Organization Size



Conclusion

This research provides insight into the greatest challenges organizations face in securing their applications and how current application security practices affect their business operations.

The data is clear: **Applications and APIs are not secure enough.** Organizations must rethink their approach to application security. Relying on manual processes slows down security and drives up cost. Traditional security reviews are time-consuming and costly. Security teams juggle multiple individual security tools — and even with those tools, many share the common challenge of prioritizing which issues to fix first.

As adversaries evolve their techniques and operate with greater speed, **it is imperative that organizations strengthen their application security posture.** Fortunately, new technologies have emerged to address these common challenges. **Application security posture management (ASPM)** provides full visibility into deployed applications, continuously updates the application bill of materials, automates many aspects of traditional security reviews, and triages and prioritizes application vulnerabilities based on risk and exploitability. **ASPM tools help organizations scale their application security so they can build strong, secure applications and prevent breaches.**

Appendix

Methodology

CrowdStrike's Application Security Research Team developed a set of 31 questions to better understand the current state of application security and the specific pains that companies are experiencing when securing their applications.

This report features insights from 400 U.S.-based security professionals across a variety of industries and company sizes.

The survey was conducted in July 2023. The sample was provided by Sago, a research panel company. Panel respondents were invited to take the survey via email invitation and were incentivized to participate via the panel's established points program.

Survey Demographics

This section describes the survey population, including company size, industry and application code change velocity.

Company Size

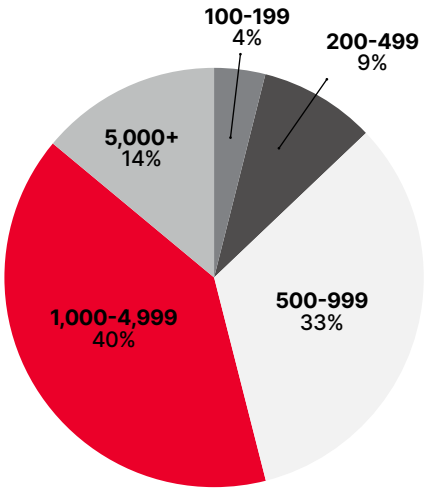
CrowdStrike sought out application security professionals from organizations with at least 100 employees. Across the sample, 40% of these professionals work for enterprise-sized organizations (1,000-4,999 employees), and 14% of them are with large enterprises (5,000+ employees). A third of the sample works for medium to large organizations that have between 500 and 999 employees. The remaining 9% and 4% are with medium/small organizations (200-499 employees) and small organizations (100-199 employees), respectively.

Industry

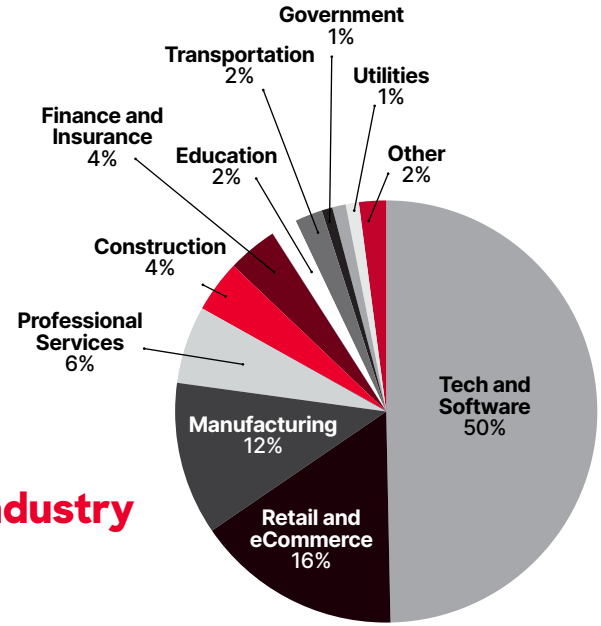
About half of the survey population works for technology or software companies. The other half is scattered across retail/eCommerce, manufacturing, professional services and a handful of other industries.

Deployment Velocity

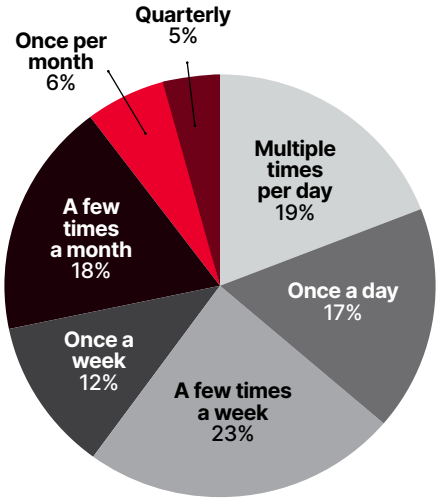
When asked how frequently their organizations release application updates, 23% of the respondents indicated they push updates multiple times per week, and 19% said they push updates multiple times per day.



Company Size by Number of Employees



Industry



Deployment Velocity

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We Stop Breaches.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/