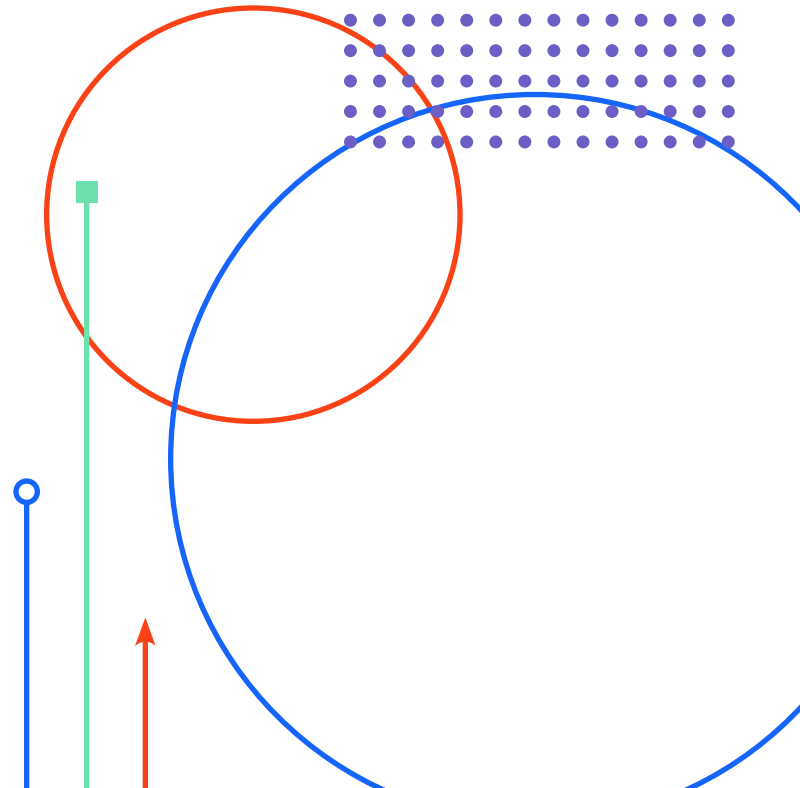




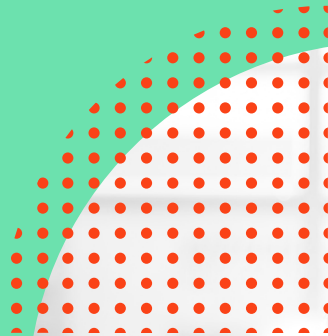
Threats are inevitable. Tradeoffs shouldn't be.

Welcome to modern
web application security.



Security professionals work hard every day to protect their companies, their customers, and society.

But the challenges they face are getting tougher and more numerous. And the stakes are higher than ever.





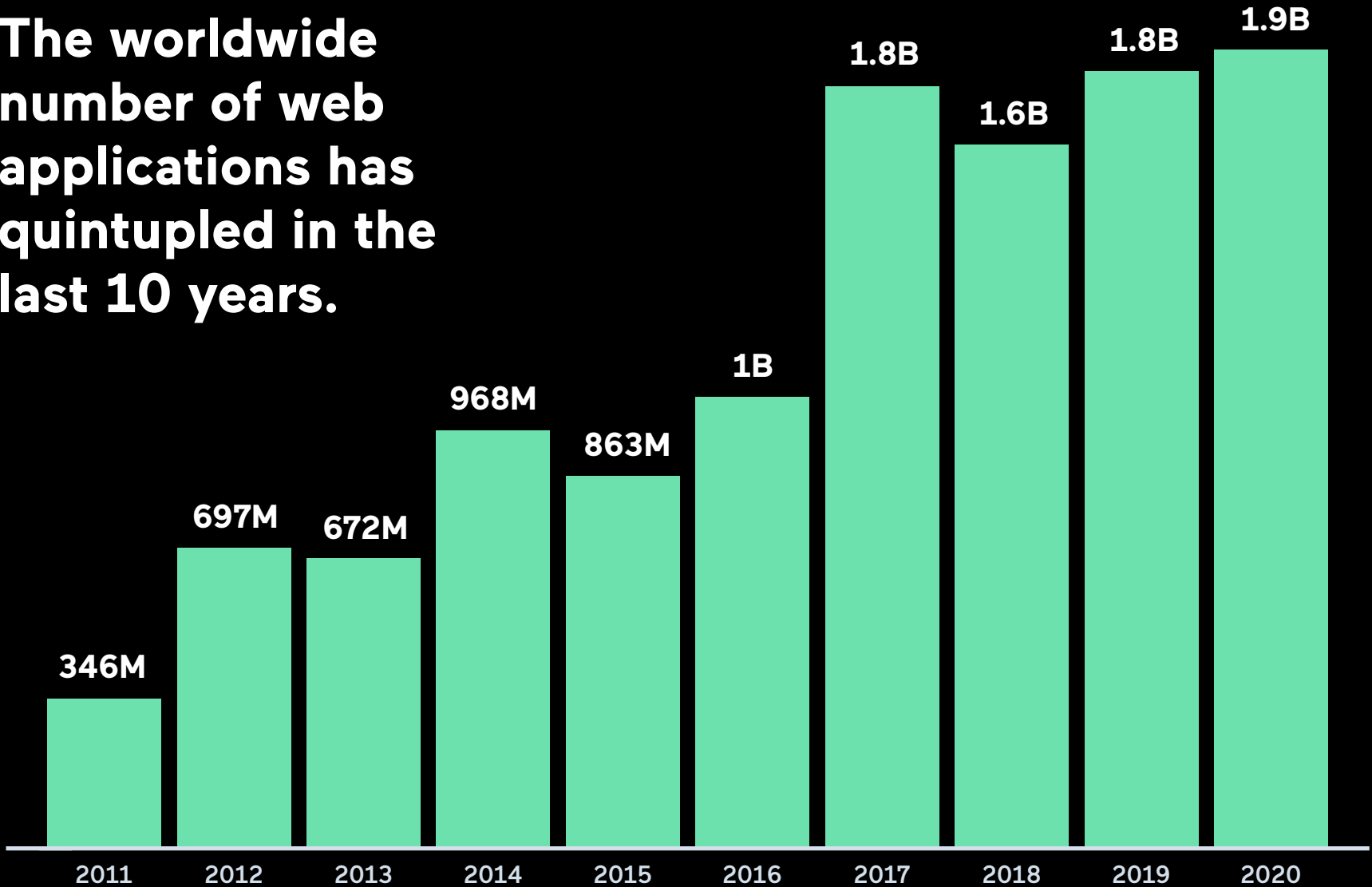
Web applications touch nearly every aspect of daily life.

From shopping to working remotely, to analyzing data, to powering critical infrastructure, web apps are everywhere.

And many of the 1.9B web applications in use today have serious vulnerabilities that put businesses, government agencies, and consumers at risk.



The worldwide number of web applications has quintupled in the last 10 years.



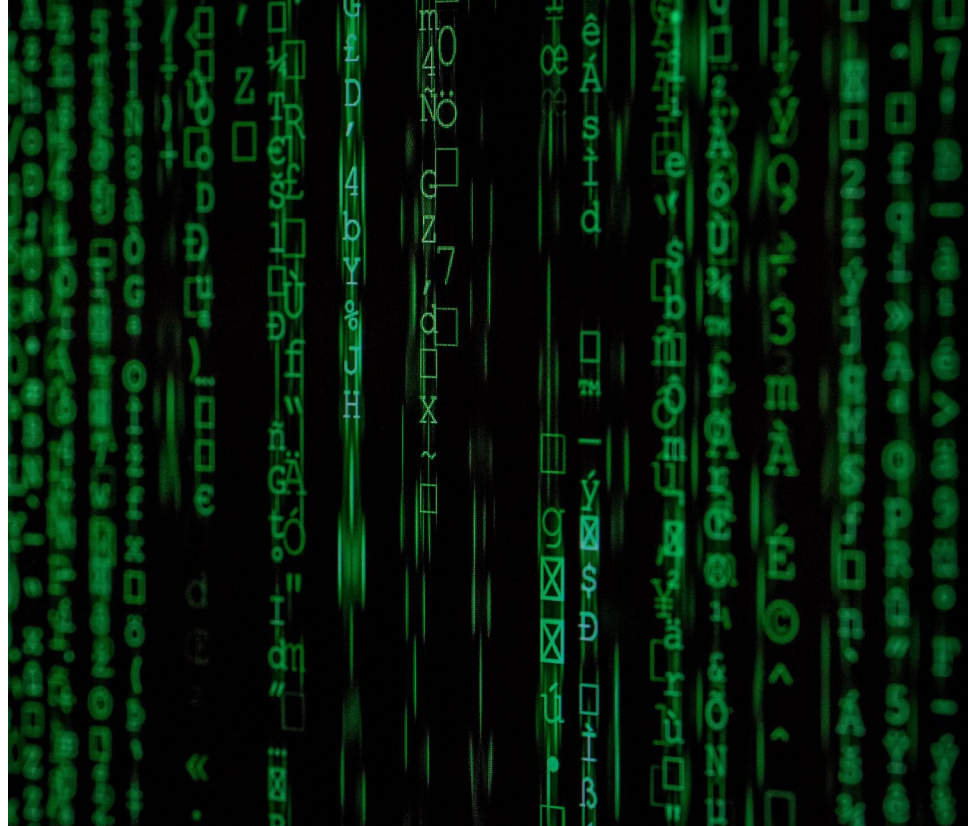
As web applications have grown, so have breaches – taking a technological, financial, and societal toll.

2020 marked a record year for data breaches, with the cost of an average enterprise breach clocking in at \$4.24 million – an all-time high.¹ One in five breaches costs \$20M.²

Recent breaches like SolarWinds, Microsoft Exchange, and Colonial Pipeline have commanded news attention because of their far-reaching impacts on both business and society. But there's much more to the story: cybersecurity is a problem everywhere, every day. The massive adoption of web applications in the past 10 years has increased risk for everyone.

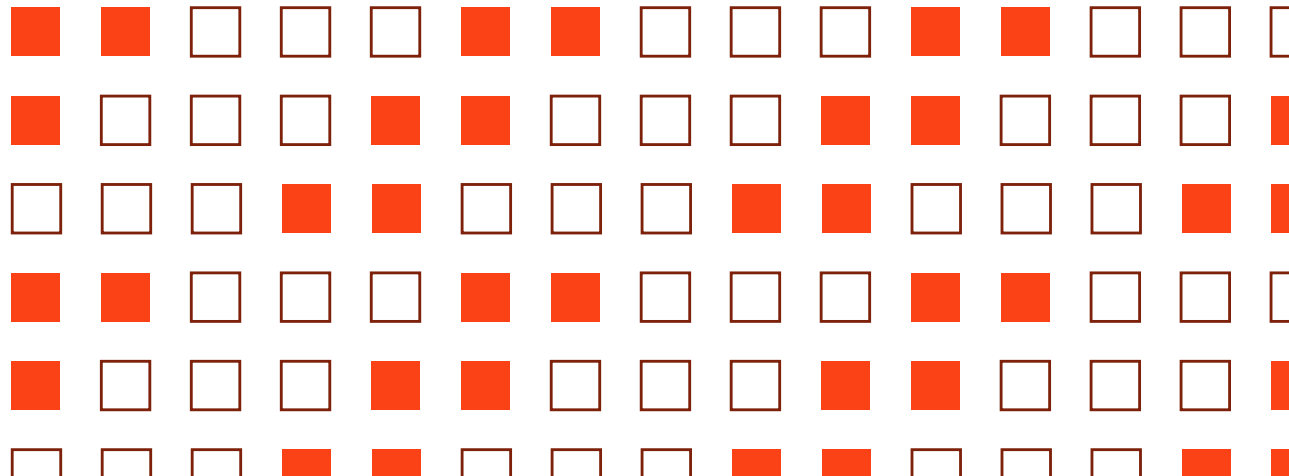
¹ IBM Cost of a Data Breach
² <https://www.cyentia.com/iris/>

- **Significant breaches have occurred on every type of website:** social media sites, shopping and entertainment, government, healthcare, developer code repositories, and even cryptocurrency-related sites.

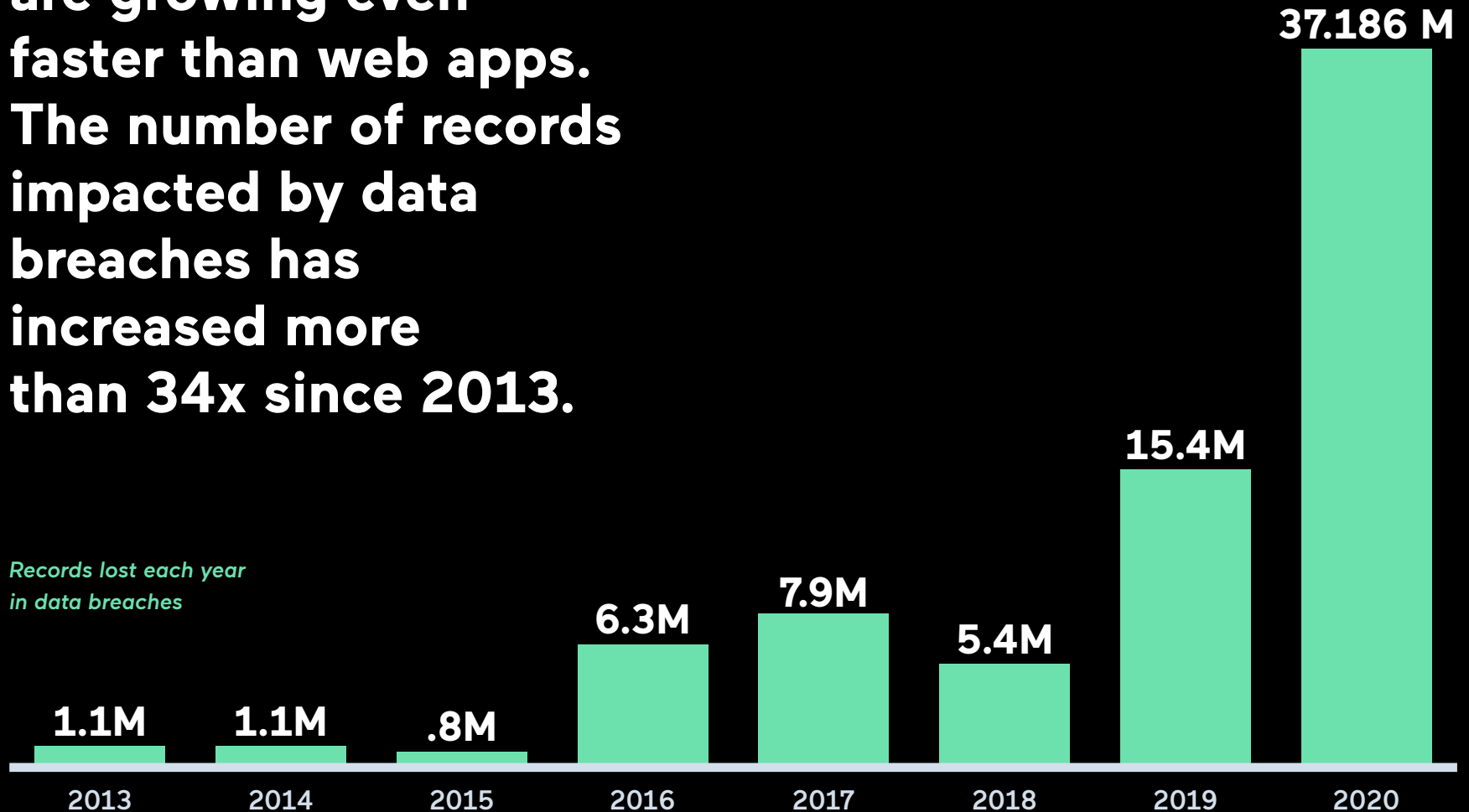


2 out of every 5

breaches originate
in a **web application**.³



**Data breaches
are growing even
faster than web apps.
The number of records
impacted by data
breaches has
increased more
than 34x since 2013.**



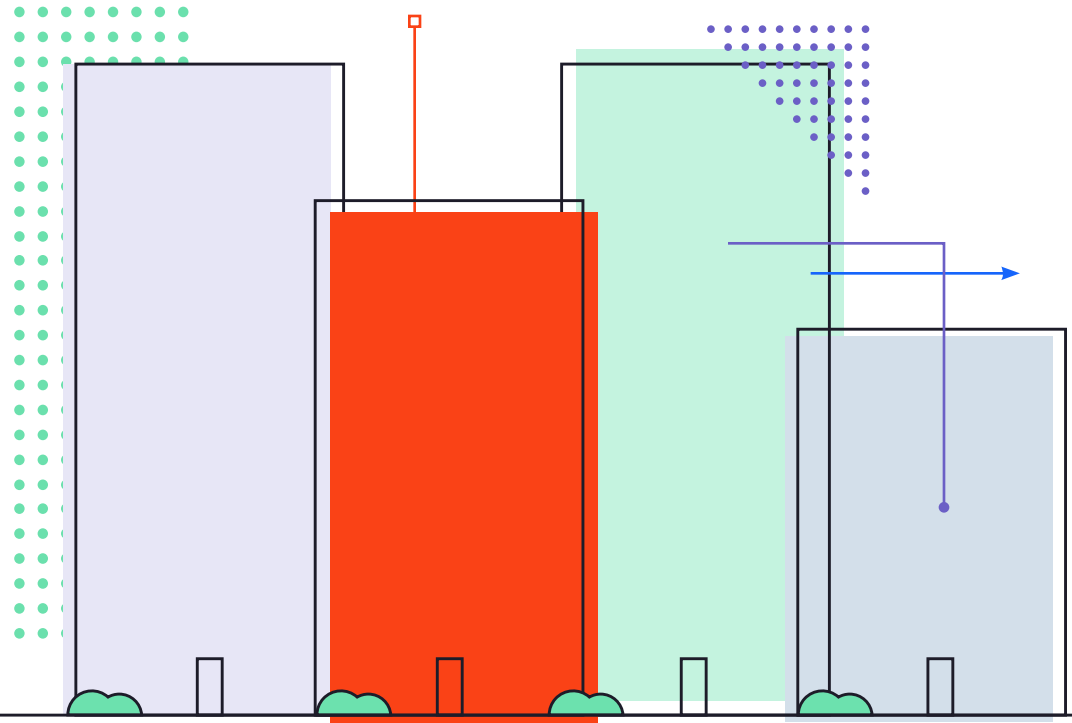
Every company is now a software company.

The average large enterprise is managing 946 custom apps and developing 193 more. Even small organizations can have dozens of custom web applications.

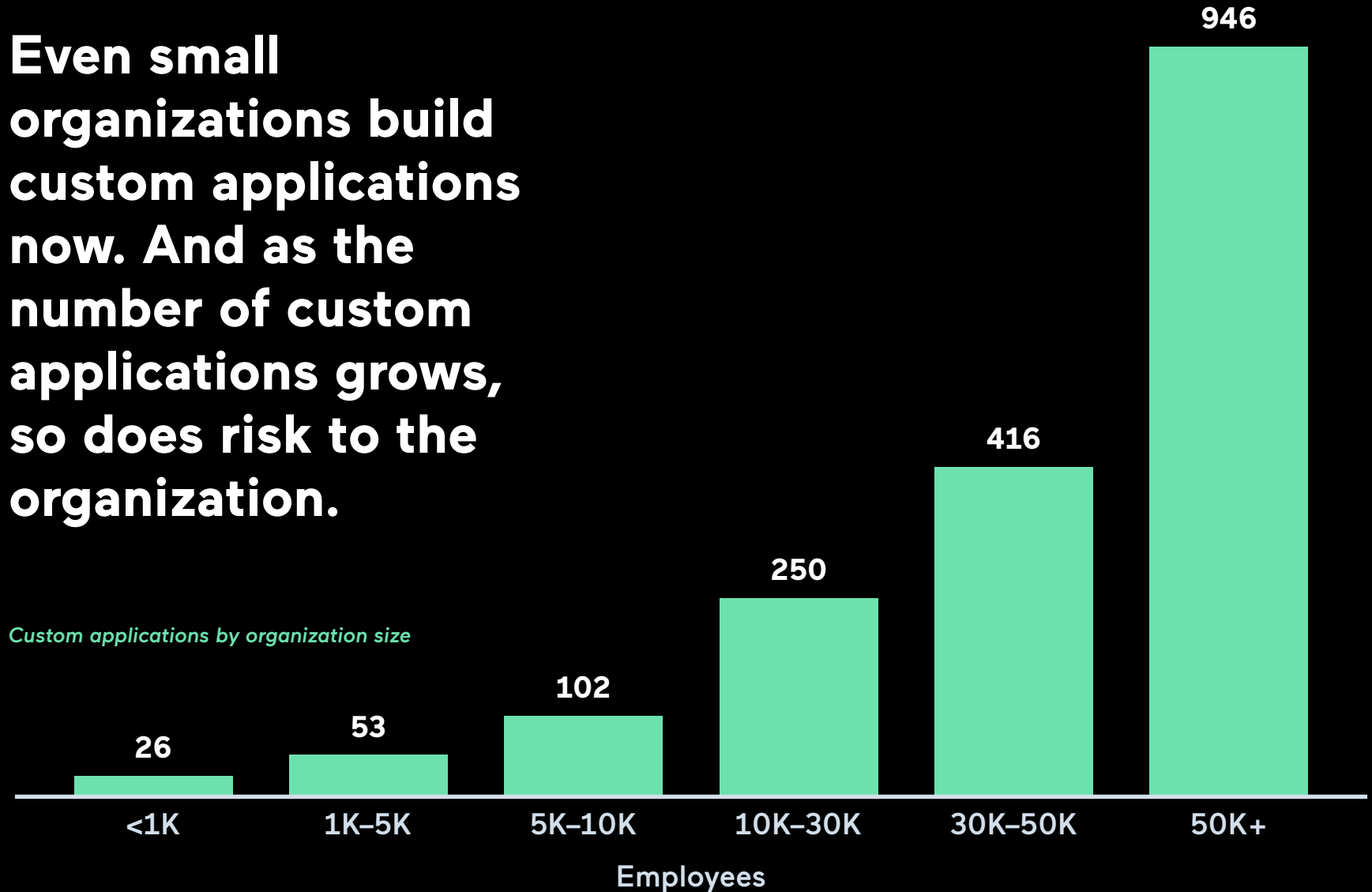
These applications are built using more advanced and complex technologies than ever before. In some organizations, the development is partially or entirely outsourced. And many of them process sensitive data and share resources with other systems and applications.

Every organization is at risk – and so are their customers.

1 in 4 Fortune 1000 companies will experience **a breach this year**



Even small organizations build custom applications now. And as the number of custom applications grows, so does risk to the organization.



Things aren't getting better.

Of course, companies and organizations know that web app security is important. They are **spending more than ever** to ensure they protect themselves and their customers.

But it's not always enough.

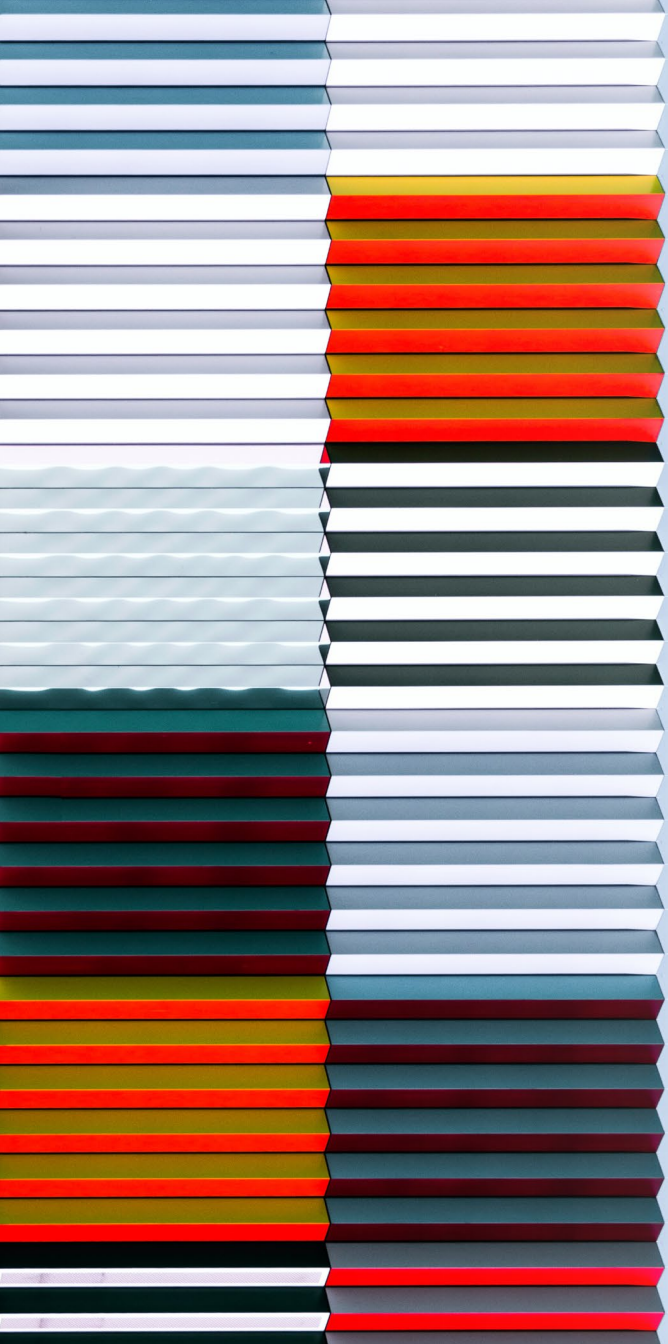
Simply put, AppSec isn't improving.

Data breaches are increasing faster than organizations can scale security, and the costs are real.

Enterprises will spend
\$3.7B
on application security this year alone.⁴

⁴ <https://www.securityweek.com/gartner-global-security-spending-will-reach-150-billion-2021>





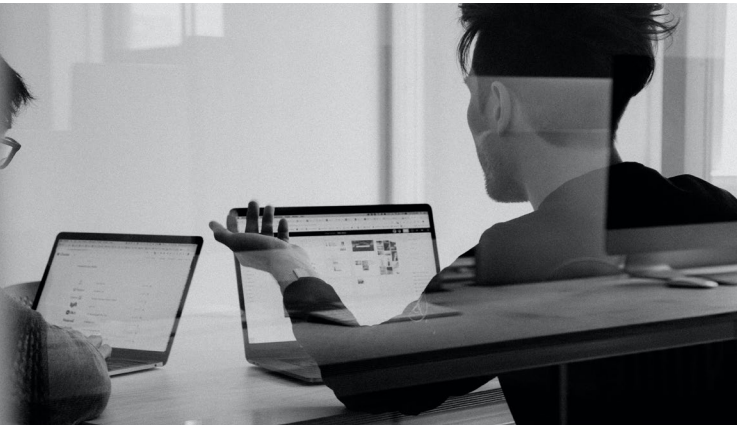
So what's going wrong?

Developers ship insecure code because of innovation pressures. Security teams are constrained – and the talent gap is growing, not getting smaller. Organizations are forced to prioritize security efforts. This leads to risky tradeoffs, like only focusing on part of the attack surface. And a lot of organizations have adopted security models such as shifting left, at the risk of having an incomplete strategy.

Efforts to staff up, prioritize resources, and situate security in the SDLC are all needed – but insufficient.

Security teams can't meet the demands of their charter.

Even when security teams have adequate resourcing for personnel, hiring is really tough. The security skills gap and talent crunch are massive.



57%

of IT and security leaders say that they are impacted by the cybersecurity skills shortage and more

than three quarters say it is

extremely

or somewhat difficult to recruit and hire security professionals.⁵

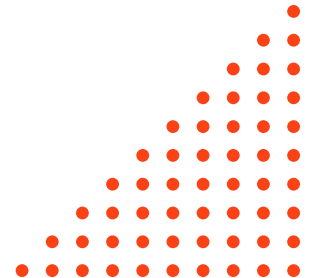
76%



Securing only flagship apps leaves the rest exposed.

Security teams are strapped, so they just focus on what they think are the most critical applications, ignoring the vast majority of the web application attack surface.

Even worse, in most organizations, there are a lot of web assets that have been lost or forgotten but are still potential attack vectors.



**Blind spots
in the attack
surface
increase an
organization's
risk every day.**

Highest-profile applications
that get the lion's share
of security resources

Lower-profile applications
that are still regularly
getting code updates

Lost or forgotten
web applications

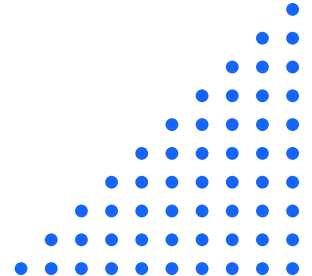
Shifting left is popular, but it falls short.

In an effort to reduce the amount of vulnerable code being shipped to production, 71% of organizations are bringing security tooling and processes earlier in the SDLC,⁶ testing the code during QA, and encouraging developers to incorporate security practices.

That's a good thing. But it's not enough.

Production applications are the bulk of the attack surface in any organization and they take on new risks with every update. Even worse, most organizations aren't aware of every live asset they still have.

⁶ Cowen Equity Research



Resource constraints make it challenging for organizations to shift left.

Percentage of respondents who do not have sufficient resources for key strategies

Support shift left

39%

Work with the dev team

45%

Address prioritized vulnerabilities

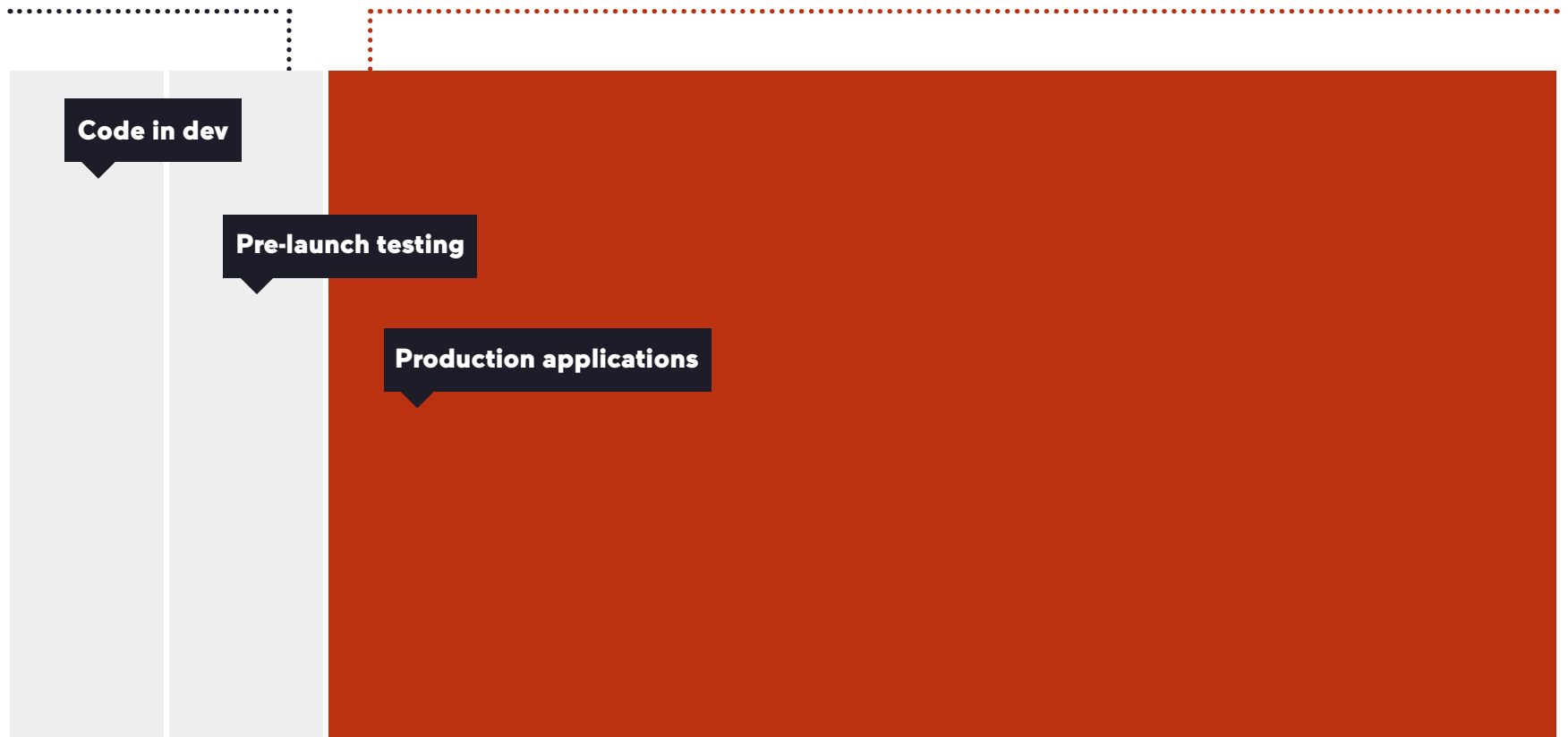
52%

And shifting left is only one part of risk reduction.

Shift left

focuses security
efforts here...

...and leaves most applications unprotected

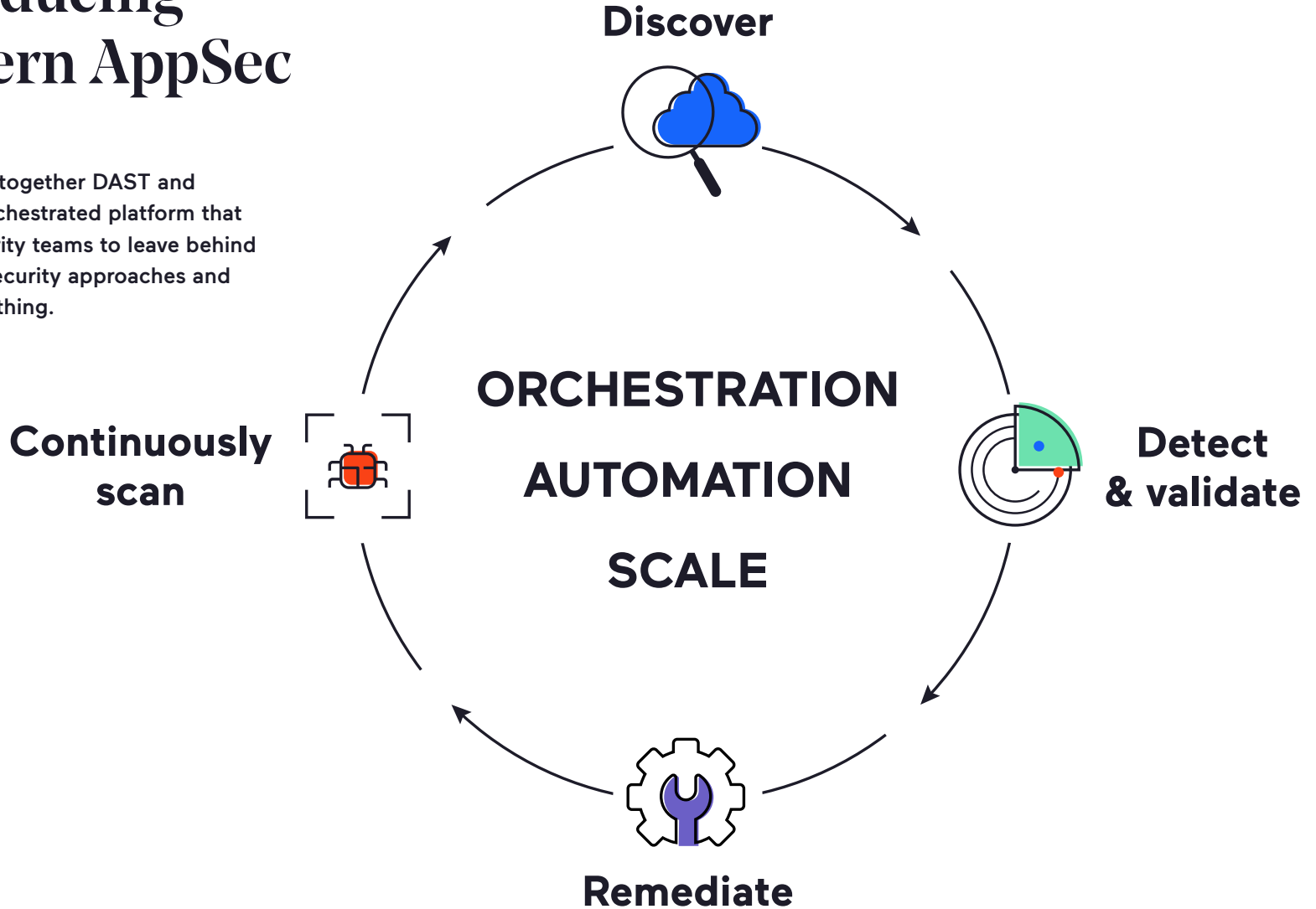


But all is not lost.

**Modern AppSec
can help.**

Introducing modern AppSec

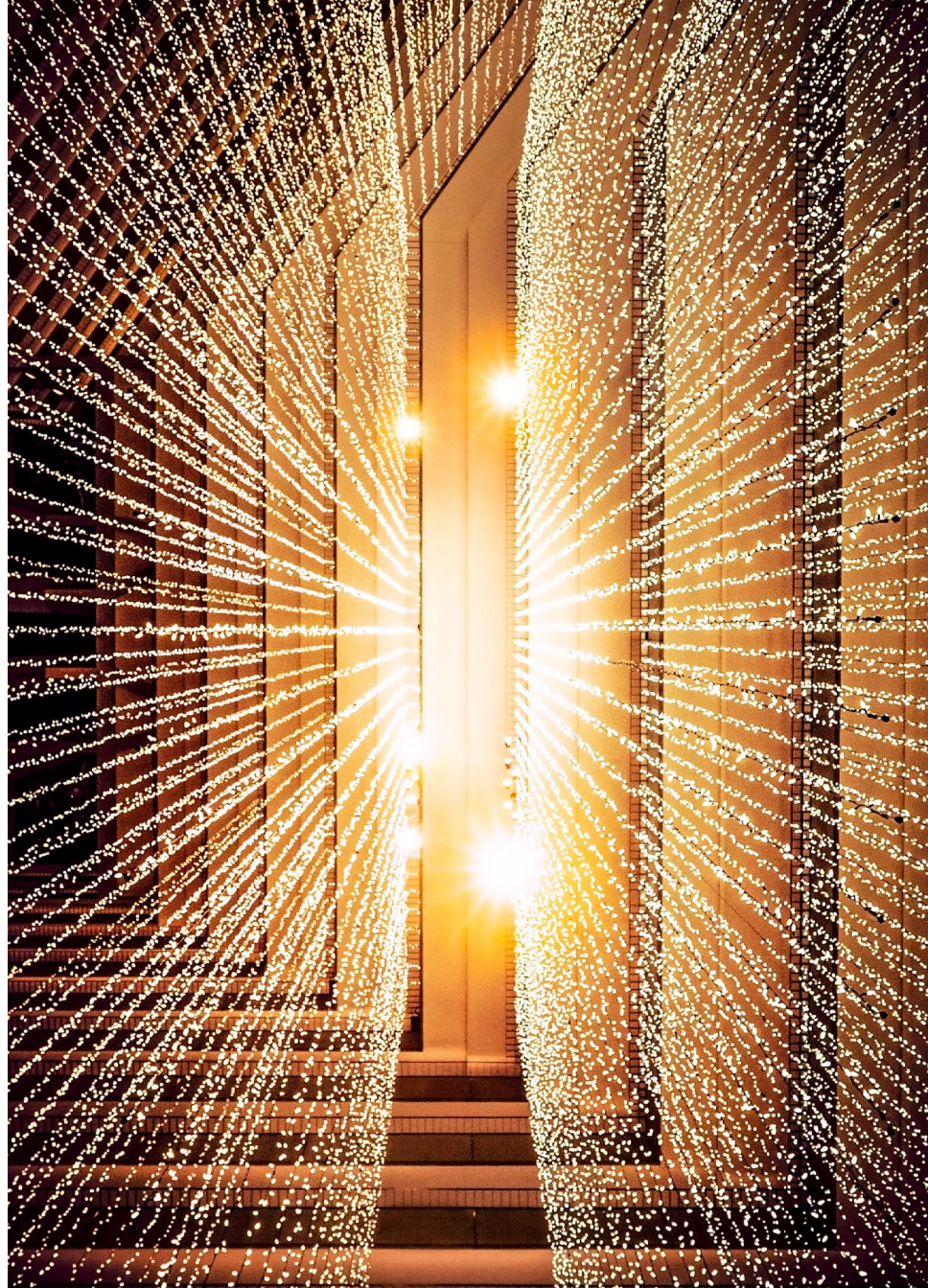
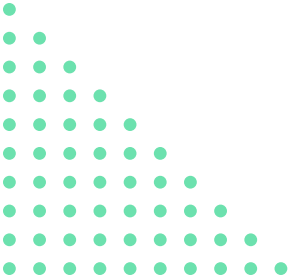
Invicti brings together DAST and IAST in an orchestrated platform that enables security teams to leave behind incomplete security approaches and protect everything.

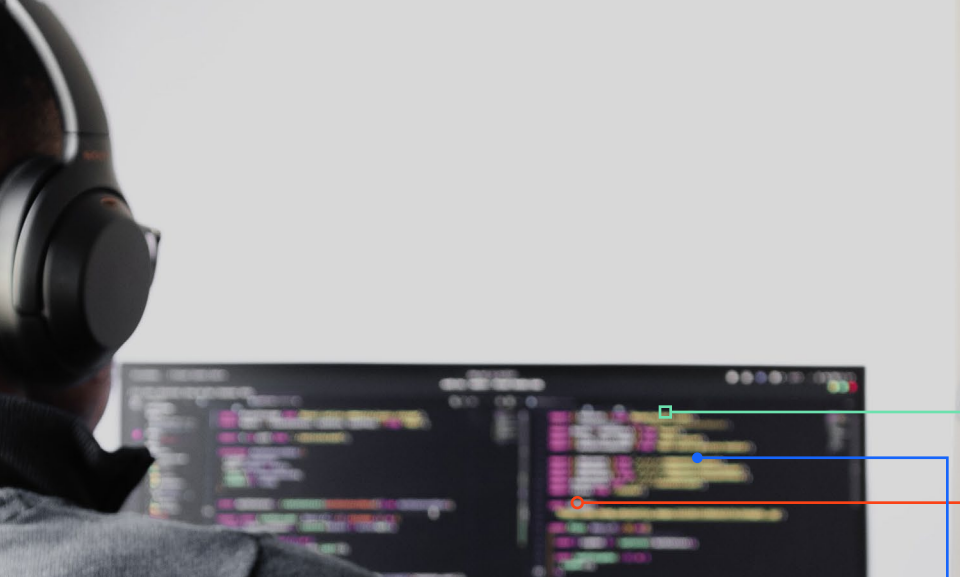


**Modern AppSec
means zero
compromises.**

Scan everything, not just the flagship assets

With Invicti's zero-compromise approach, even small security teams can inventory every web application in their portfolio. Their entire attack surface is always mapped, even as new apps are released and code is updated.





And yes, shift security left... but keep scanning on the right.

Innovation demands are outweighing security practices. Developers are under a ton of pressure to release code as quickly and frequently as possible, and sometimes cut corners.

Organizations can't count on code to be free of vulnerabilities even on the day it's released.

The best approach is to scan in development and extend to production, and to keep up with code releases in real time. Integrating security into CI/CD workflows makes it possible.



81%

of developers knowingly release insecure code at least some of the time.⁷

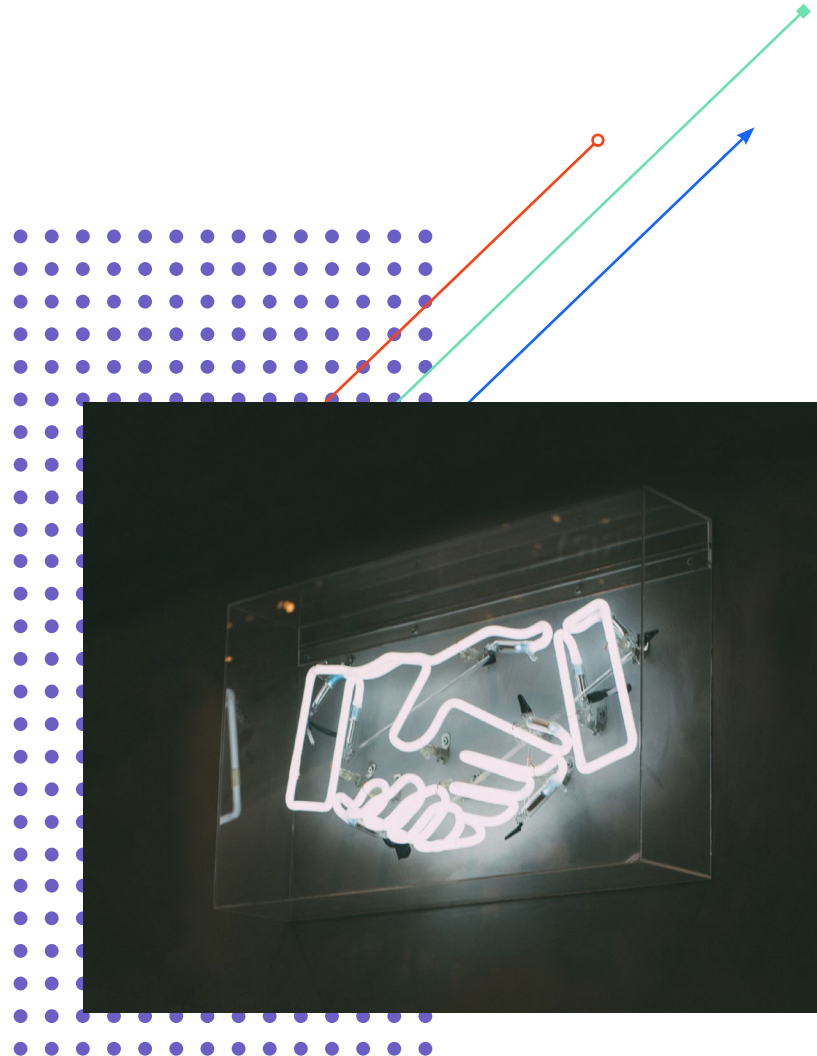
⁷ Osterman, 2021

Invicti makes true collaboration among Dev, Sec, and Ops a reality.

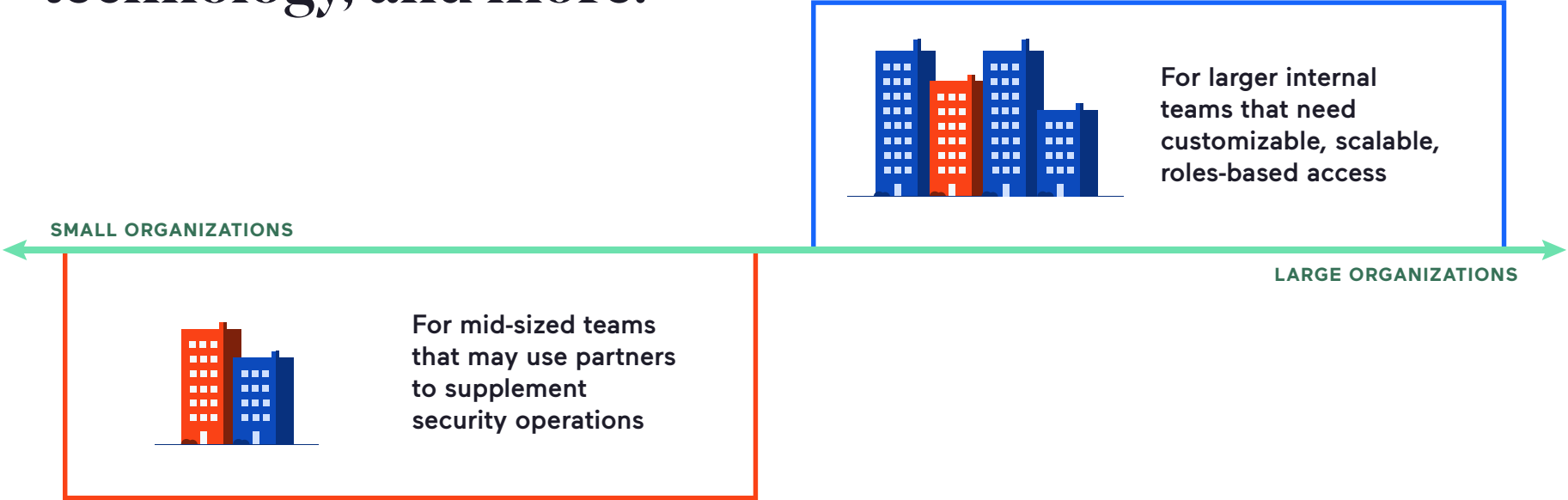
Invicti's zero-compromise platform maximizes your coverage to reduce the risk of breaches. Because it includes both DAST and IAST, you get an outside-in and inside-out view of the entire application – including line-of-code level details to help pinpoint the problem. And this isn't the typical DAST/IAST tool you might have heard of in the past – with automations and our prioritization engine, you can truly cover everything.

Our proof-based approach doesn't just flag vulnerabilities – it demonstrates with 99.98% accuracy which ones are exploitable.

And remediation is easier and less disruptive with developer workflow integrations and automatic rescans to confirm that fixes are effective.



Invicti's solutions support organizations across government, financial services, healthcare, manufacturing, technology, and more.





Don't just take it from us: Security pros love Invicti and Acunetix.

Compared to the solution we had before, we **lowered our false positives** by a high margin and improved the detection of security issues.

– Julien L.

Invicti **helped us understand the risks**, how to mitigate them before they are deployed and provides ongoing incremental scans to ensure compliance.

– Tim W.

Invicti integrates with so many technologies in such an efficient manner it makes **complete CI/CD coverage possible** from a DAST perspective.

– Damien S.

Detailed reports can be presented to software architects and developers on the team and summary reports can be presented to management.

– Chris A.

You can run the test and you will have a report within a few hours, so you can **iterate quickly and recheck security again** after developers fix the issues.

– Lubos B.

Stop

Get your security team the modern tools that will enable them to keep up with today's security landscape.

compromising.

Invicti: Zero-compromise web application security

Find out more:

Book a demo today.



Invicti Security is transforming the way web applications are secured. An AppSec leader for more than 15 years, Invicti enables organizations in every industry to continuously scan and secure all of their web applications and APIs at the speed of innovation. Through industry-leading Asset Discovery, Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), and Software Composition Analysis (SCA), Invicti provides a comprehensive view of an organization's entire web application portfolio and scales to cover thousands, or tens of thousands of applications. Invicti's proprietary Proof-Based Scanning technology is the first to deliver automatic verification of vulnerabilities and proof of exploit with 99.98% accuracy, returning time to development teams for critical projects and innovation. Invicti is headquartered in Austin, Texas, and serves more than 3,500 organizations all over the world.

Invicti 

www.invicti.com