

The State of Security 2026:

Forget AI. Fear Imbalance.





Table of Contents

4 INTRODUCTION: REFRAMING THE SCAPEGOAT

6 PART ONE: ENTERPRISE CHECK-IN

Overall Level of Security
Frequency of Security Incidents
Most Secure Business Areas
Key takeaways

8 PART TWO: CHALLENGES, RISKS, AND ROADBLOCKS

Biggest Overall Security Concerns for 2026
Biggest Barriers to Improving Security
Growth Strategies Most Affected by Security
Key takeaways

11 PART THREE: SECURITY IN THE AGE OF AI

Biggest AI Security Concerns
AI's Expected Impact on Security Practices
Key takeaways

13 CONTENT SECURITY STARTS WITH STORYBLOK

14 PART FOUR: DEFENSE PRIORITIES

What security certification do you prioritize most?
How prepared is your company to respond to a website security incident?
Key takeaways

16 PART FIVE: FUTURE PRIORITIES

What are you prioritizing for future website security investment?
What will have the biggest impact on enterprise security in the next 3-5 years
Key takeaways

18 CONCLUSION: SEE THE FOREST, NOT THE TREES

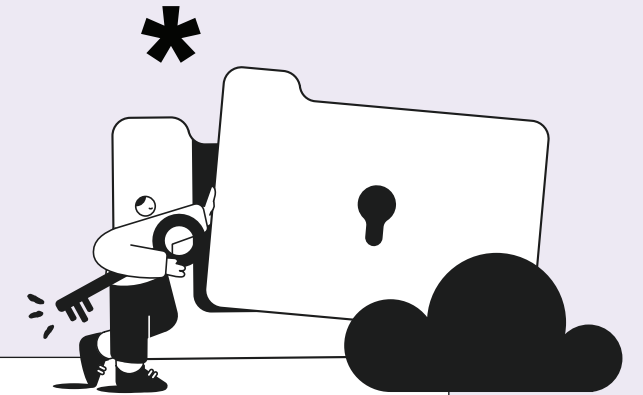
About Storyblok

INTRODUCTION

Reframing The Scapegoat

AI has become inescapable. No matter what industry you work in, it seems like it's all anyone wants to talk about. The world of cybersecurity is no different. While some conversations cover the benefits, more are worried about the risks. Will people use it to launch unstoppable attacks? Engineer hyper-effective phishing scams? Fake authentic content?

With so much uncertainty, AI has become the most popular scapegoat for security woes. But while it's undeniably a big part of our lives these days, the obsession has begun to eclipse every other aspect of security strategy. That's why we talked to 300 security teams across the US, the UK, and Germany. We wanted to get an expert-level view of what we should actually be worrying about when it comes to security in 2026.



UNFORTUNATELY, RESEARCH SUGGESTS THAT THE AI OBSESSION HAS INDEED ECLIPSED OTHER VERY REAL RISKS. EXPERTS REVEAL THEIR CONCERN LIES NOT SOLELY WITH LLMS, BUT A WIDE RANGE OF MORE SUBTLE SECURITY THREATS – JUST AS DEADLY, YET OFTEN IGNORED IN FAVOR OF THE MORE BUZZ-WORTHY SCAPEGOAT.

So, let's take AI off the pedestal. Let's evaluate it realistically in the context of everything else that goes on behind the scenes to keep websites safe.

Let's find out where your security concerns – and your investments – should really lie in 2026.

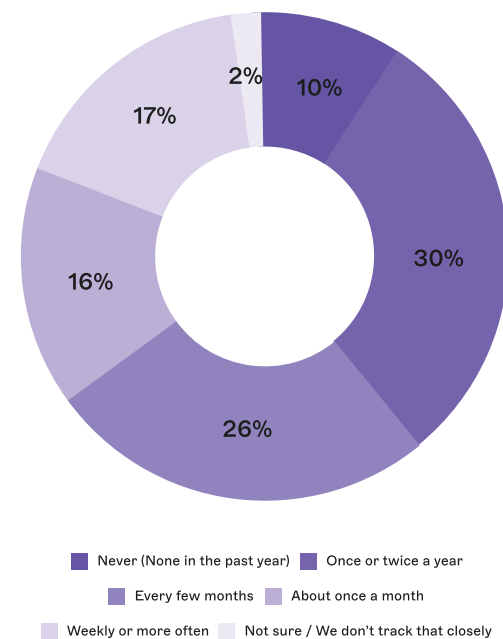
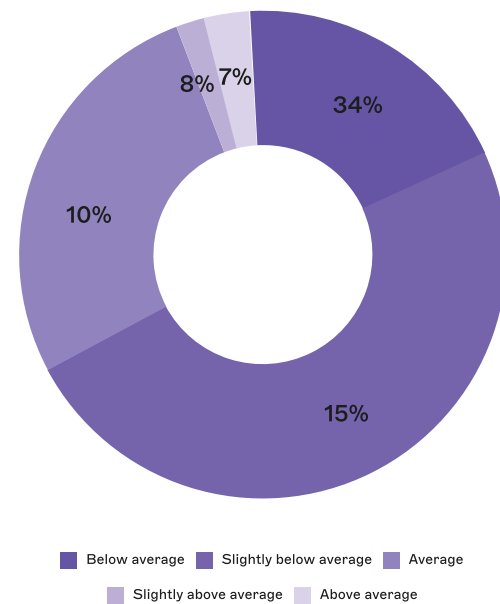
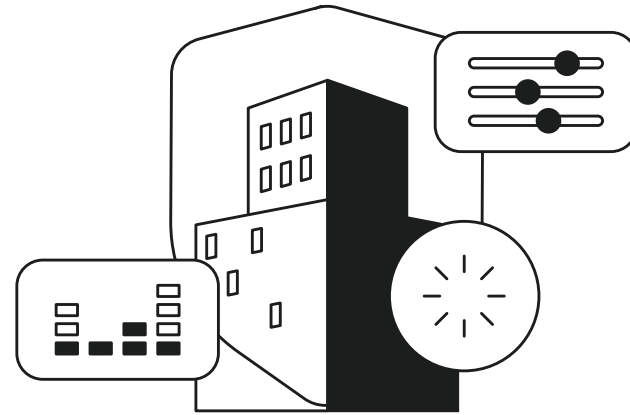
PART ONE

Enterprise Check-In

Let's kick things off with a birds-eye view. How do enterprises judge their own security, and how are their current strategies playing out?

Overall Level of Security

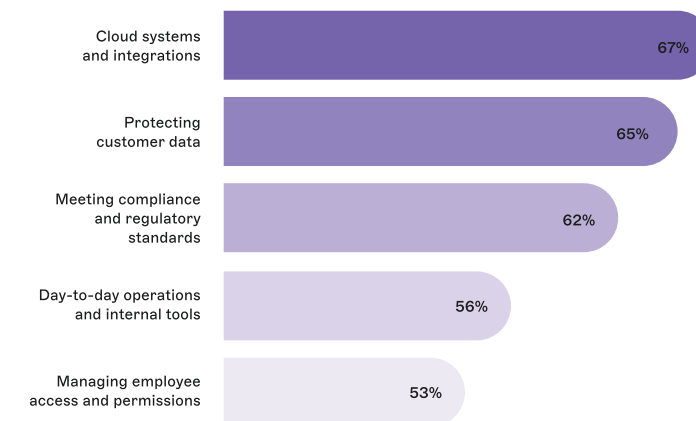
In a world where threats evolve every day, it's easy to feel increasingly vulnerable. **But security decision-makers aren't so easily spooked.** The vast majority rate their overall security as better than average, with only 5% falling below the threshold. Even with the rapid pace of technological advancement today, most experts haven't lost confidence in their strategies and remain optimistic.



Frequency of Security Incidents

56% of the sample only deal with security incidents every few months or less – a solid sign that their earlier optimism isn't misplaced. Still, that leaves **44% who are still fighting off risks at least 12 times a year.** As new tech facilitates new attacks, staying up-to-date with the best way to fend off hackers will be crucial to ensuring your company lands on the lower end of this scale – and with any luck, joining the coveted 10% who haven't had an incident in the past year.

Most Secure Business Areas



As for where exactly that confidence comes from, experts feel the most confident in the security of their Cloud systems, customer data protection, and regulatory standards.

Where they feel least secure tells an equally compelling story: The human element. Experts reported the least confidence in managing employee access and permissions (53%). In any well-oiled content machine,

humans will always be the wild card that can change everything – for better or worse. Humans are central to creating high-quality, enterprise-critical content, but they're also less predictable than regulations and data safety. It's another reminder that even less-advertised safety features, like custom user roles and permissions, are no less critical to overall security.



LEARN MORE

Prioritizing data management and compliance will be a big trend for 2026. It's not just security teams keeping an eye on it, either: IT leaders feel the same, particularly when it comes to AI. Learn more in our free infographic, ["IT Leaders Weigh In: Data, Risk, and Optimism In The Age Of AI"](#).

KEY TAKEAWAYS

- **76% of users rated their security slightly above average or better.** Enterprises are clearly investing in their security infrastructure and are reasonably confident about their setups.
- But even that doesn't guarantee safety. Slightly under half of the sample are still dealing with a dozen or more incidents a year, **with a shocking 17% doing digital battle every week.**
- **The human factor remains the most unpredictable element in a security environment,** presenting a harder security challenge than integrating external tools or protecting customer data.

PART TWO

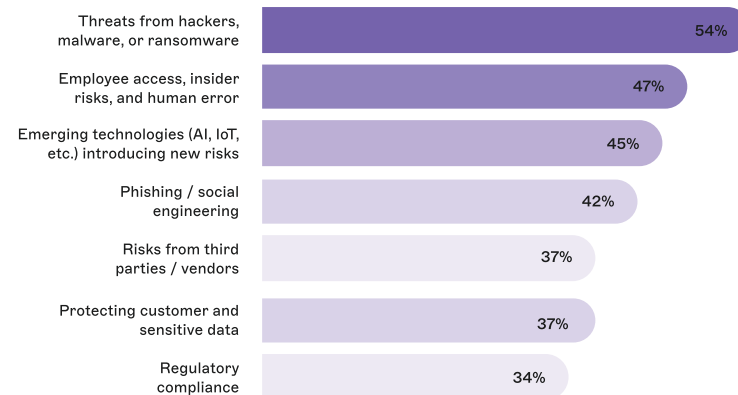
Challenges, Risks, and Roadblocks



Enterprises have reason to be optimistic. But in a field as complex as security, there are bound to be vulnerabilities. As threats become more sophisticated, shoring up your defenses now can be the difference between a minor hiccup and a total catastrophe.

Let's see what the experts are keeping tabs on as we head into 2026.

Biggest Overall Security Concerns for 2026



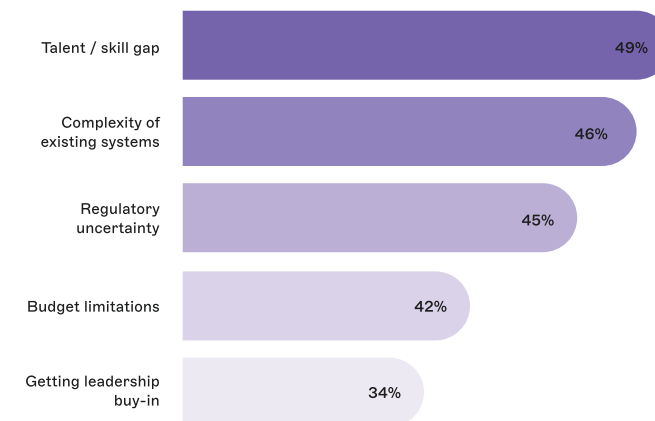
In a world where new AIs pop up every day and technological standards don't stop rising, you'd think that all eyes would be on the more technical side of security. But what we see here – and what the previous section started to uncover – is that technology isn't what's scaring security leaders the most in the new year.

They're still most scared of the human element, whether it comes from the outside (hackers, malicious actors) or the inside

(internal attacks and human error). Now, that's not to say that human risk is the whole picture. Companies are still keeping an eye on new tech like AI. But they're not putting all their eggs in one basket, either. Worries about vendors, data, and regulations are still prevalent.

The message is clear: security is a team sport, and experts can't afford a weak link anywhere in the ecosystem.

Biggest Barriers to Improving Security



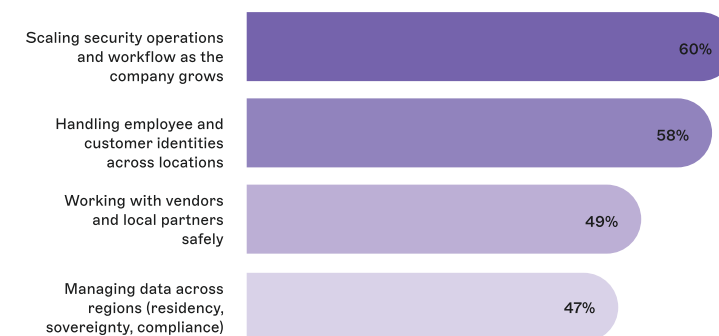
When it comes to what gets in the way of the perfect strategy, it's a people-problem once again: 49% reported they didn't have the right talent or skills within the team to make improvements.

However, like we saw earlier, there's enough concern to go around. Close behind was the difficulty of adding security measures to existing systems. This is a frequent complaint of legacy CMS users in particular

– not a great sign for that tech's longevity, especially given the fact that legacy systems are already less secure than headless by default.

On a broader scale, most of these barriers come within 10% of each other. **It's a testament from experts that the best security strategy doesn't focus too heavily on one aspect, but on the overall health of the larger ecosystem.**

Growth Strategies Most Affected by Security



Growth strategies often come with their own security concerns. Mapping these out before serious expansion helps you to avoid losing your footing at a crucial business moment. **Scaling security operations and workflows**

is the greatest growth barrier in 2026. Unfortunately, security measures and workflows that are perfect for a startup won't always translate to the big leagues. Picking technology that's designed to scale from the

start makes it easier to evolve your safety work-
flows without worrying about weak spots. We're seeing troubles across the board in 2026,
though: **99% of respondents reported at least one security issue hampering their growth**, highlighting how universal the issue is.



LEARN MORE

As competitors struggle to grow in the new tech landscape, now is the perfect time to get ahead of the game. With [Storyblok's FlowMotion](#), you can scale content without scaling complexity. Reduce manual work, personalize to a global audience, and use AI-enhanced workflow automations to leverage content to its maximum potential.

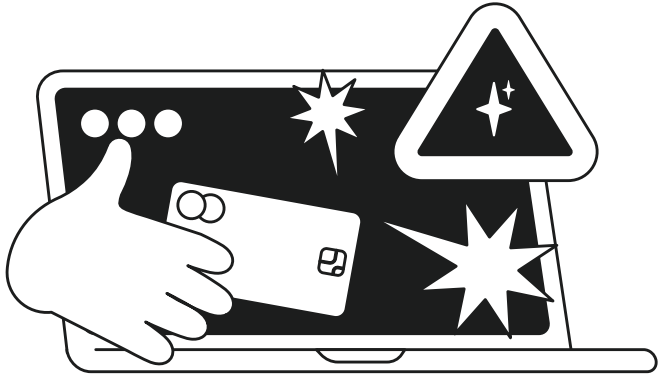
[Learn more and request early FlowMotion access for 2026 today!](#)

KEY TAKEAWAYS

- The **two biggest overall security concerns for 2026 involve a human element**: hackers launching external attacks, and insiders causing damage on accident or with malice.
- The biggest barrier to improving security is also human-driven: **almost half of the respondents struggle with filling a talent gap**. Having the best tech is essential, but it won't do you any good if you don't have the team to properly leverage it.
- Users report that their growth strategy is most held back by an inability to scale existing security workflows. **Use of scalable tech will become the differentiator for both expanding and securing your content strategy.**

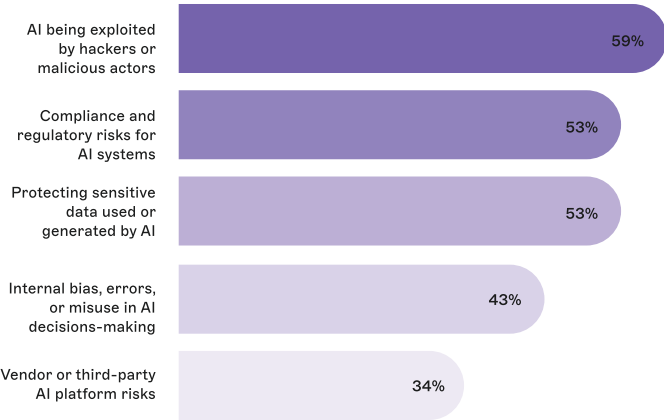
PART THREE

Security in the Age of AI



AI as a scapegoat might be overhyped, but that doesn't mean it doesn't still present some very real risks. Let's get to the heart of it and see what security teams are really worried about with this new tech.

Biggest AI Security Concerns

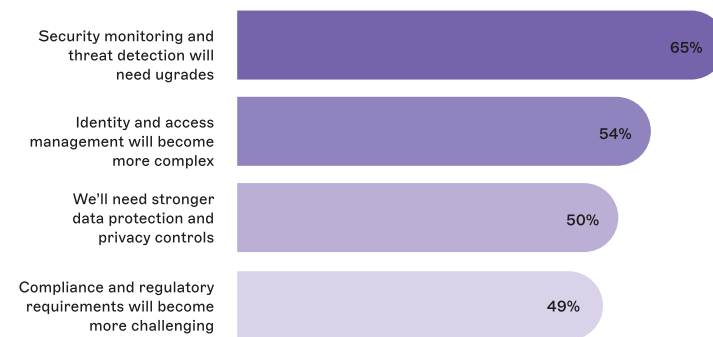


The biggest issue is still those pesky humans. **When it comes to AI, people are most worried about it in the context of how human bad actors can leverage it.** It seems even with all the technical power of artificial intelligence, the scariest thing about it is how dangerous it could make a human malicious actor. This is especially clear given that concerns about AI decision-making – the AI acting without supervision, without the human element – were less frequently reported.

Beyond the human threat, experts acknowledge there is still a lot to grapple with. **They still worry about AI's compliance capability as well as how it might put sensitive data at risk.**

Both can open your business up to possible legal consequences, angry customers, and financial disaster. Take it from the experts: **keeping an eye on how a still-developing technology navigates those choppy waters is a wise move.**

AI's Expected Impact on Security Practices



AI might present novel threats, but experts see solutions in the systems they've already built. The main adaptation strategy is predicted to be security and threat detection upgrades – notably, **something that will also protect against non-AI threats for holistic security improvements**. The human users of AI are also represented as threats here, as user role access improvements beat out

both data protection and compliance issues.

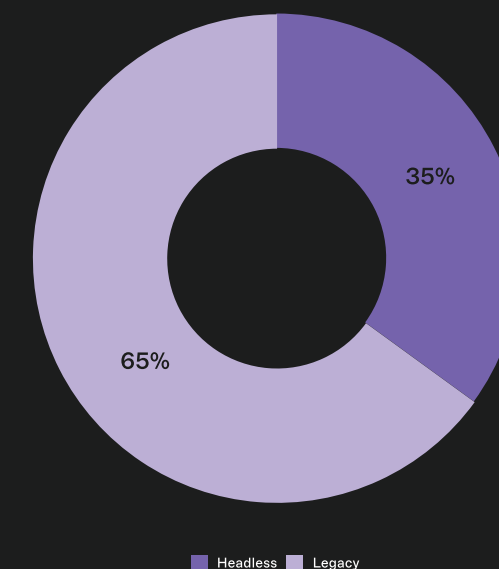
It's interesting to note that while security teams may have differing ideas on the best way to prepare for the age of AI, 99% of our respondents agree on at least one thing: **AI is guaranteed to change how they approach security**, even if that just means beefing up the measures they already have in place.

KEY TAKEAWAYS

- When it comes to AI, businesses are definitely concerned, but not about the tech itself. **It's the potential that human bad actors have to leverage it that worries them.**
- **99% of people agree that AI will have an impact on their security practices**, with the data showing intent of a well-rounded approach to prepare.

Content Security Starts With Storyblok

39% of our respondents indicated that they had experienced a security issue impacting their content strategy in the last year. When you break that group down to **Legacy** or **Headless** systems, a pattern becomes clear:



THE MAJORITY OF PEOPLE WHO HAD SECURITY ISSUES INTERFERE WITH CONTENT STRATEGY WERE USING LEGACY SYSTEMS.

A security strategy that treats each defense as an isolated factor will not last. It doesn't matter if it's because of technical limitations or strategy decisions. If you're not treating your security as an entire ecosystem, your defense has holes.

That's where Storyblok comes in.

With centralized permissions, API-first architecture, and built-in regulatory compliance, Storyblok's cohesive enterprise security standards have earned certificates including ISO27001 and SOC2.

Learn more about Storyblok's enterprise-grade security features by visiting our [Trust Center](#).

PART FOUR

Defense Priorities

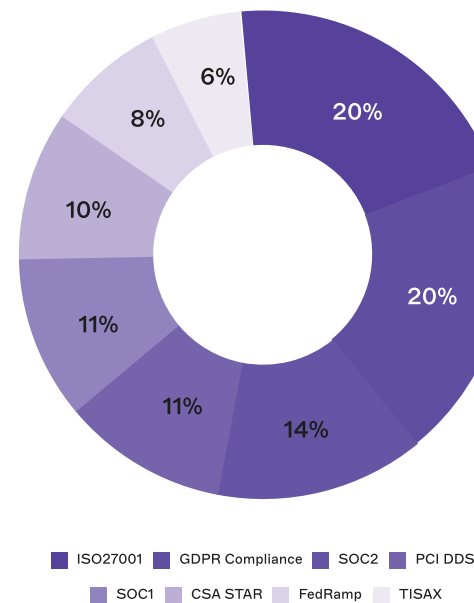
Now that we're more familiar with the security challenges users are facing in 2026, let's take a look at how they're responding and where their priorities lie.

What security certification do you prioritize most?

The two most prioritized security certifications for 2026 are ISO27001 and GDPR Compliance.

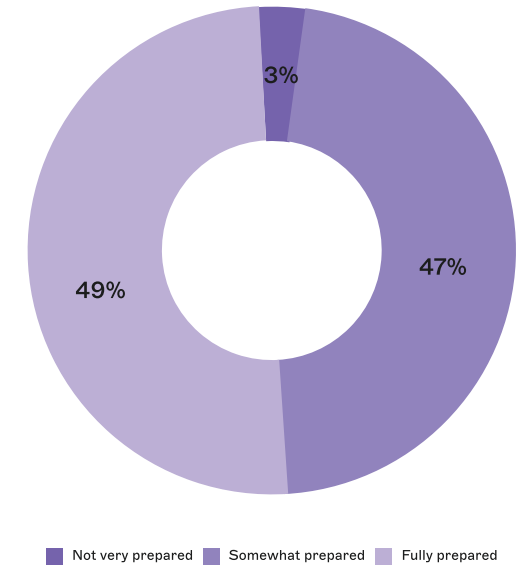
ISO27001 ties for the most prioritized certification. Given that it's the world's best-known standard for information security management systems, it's no surprise that many see it as the gold standard. Any company that can earn that certification is demonstrating the highest levels of cybersafety.

It shares the podium with GDPR compliance. While companies don't need any GDPR certification to demonstrate compliance with the mandatory law, doing so can add an extra layer of assurance for users. It's important enough to rank highly on their cert list despite not explicitly needing it.



How prepared is your company to respond to a website security incident?

Just under half (49%) of respondents showed a very encouraging response: they feel fully prepared to tackle any website security incident that comes their way. Most of the rest (47%) are more modest, but still somewhat prepared. **With only 3% rating themselves on the lower end of the scale – and a comforting 0% indicating total unpreparedness – users are demonstrating confident optimism while allowing room to improve.**



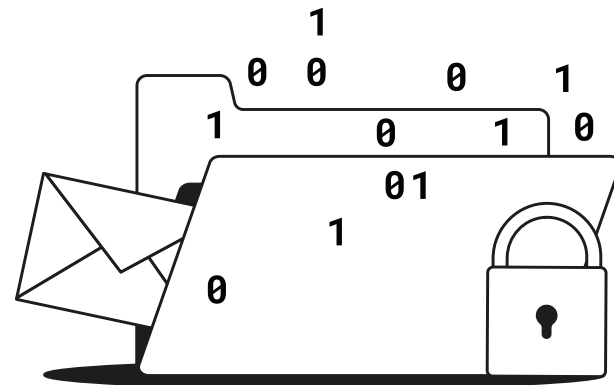
KEY TAKEAWAYS

- **ISO27001 and GDPR are the most sought-after certifications**, though SOC2 remains popular as well.
- **Enterprises are optimistic about their security capabilities, but they're also realistic.** In a world of constantly mutating threats, it's a very encouraging combination.

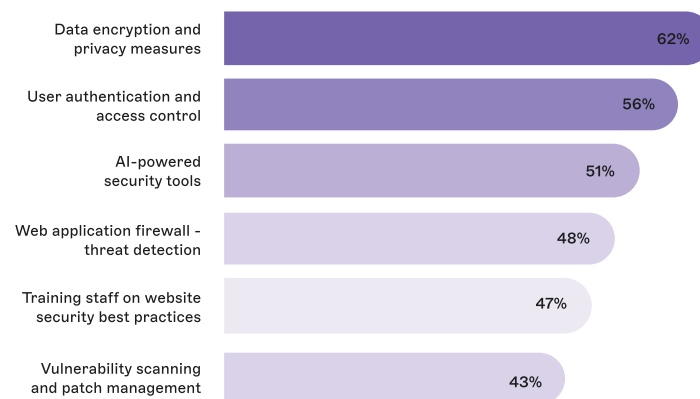
PART FIVE

Future Priorities

Nobody can predict the future. But with a little insight from security teams, we might be able to get a sneak peek.



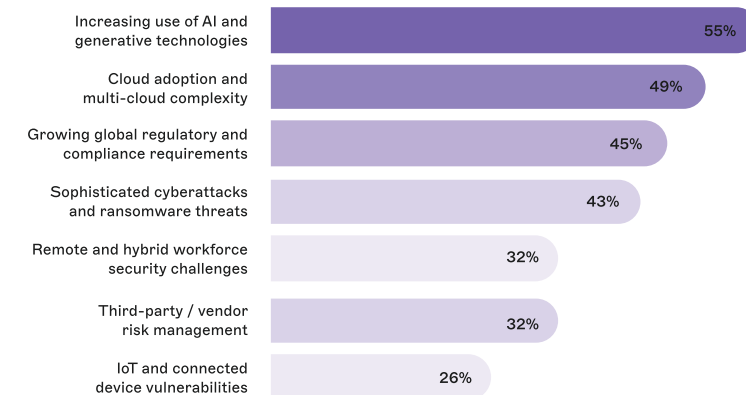
What are you prioritizing for future website security investments?



Businesses are mainly looking to shore up their data encryption and privacy measures. Not exactly surprising in an era where major breaches are a routine part of daily news. But teams are also looking inward for investments: **the fear of human error and influence haunts website security as**

well, with user authentication and access control a top priority. And, while users remain wary about AI's risks, just over half plan to balance them with the benefits of AI-powered security tools. If you can't beat 'em...

What will have the biggest impact on enterprise security in the next 3-5 years?



While it's clear that AI remains front of mind for security teams, it's far from the only consideration as they look towards the future. Cloud tech, increasing regulations, and advanced cyberattacks also remain squarely on their radar.

Fleeting fad or lasting industry change, the best security teams don't isolate any risks for special treatment. They operate within the context of the entire security landscape, maintaining a well-rounded, healthy ecosystem that's easily calibrated and well-balanced.

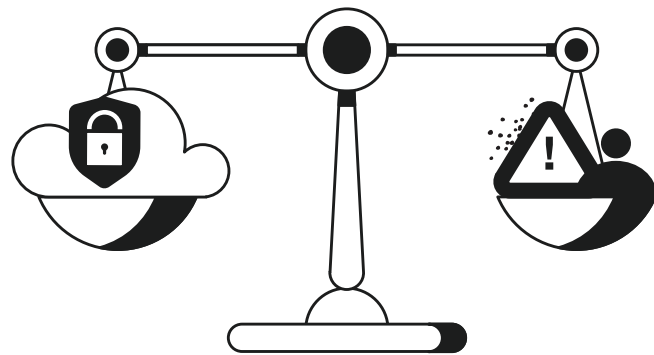
KEY TAKEAWAYS

- **Data encryption reigns as the biggest investment priority for 2026** – but finding a way to control the human element with user authentication and access controls isn't far behind.
- Enterprises are expecting AI to have the biggest impact on their security practices in the coming years, **but answers reflect that most are favoring a well-rounded approach over an AI obsession.**

CONCLUSION

See The Forest, Not The Trees

In any technical field, there are bound to be a dizzying array of moving parts to account for. But in the field of security, the risks of failure are high. Focus on the wrong threat, take your eyes off a vulnerability for one second, and everything could come crashing down. It's tempting to place the complex blame on one single threat. Easy, too.



But as we've seen through this survey, that narrative doesn't hold up. Enterprises definitely have AI on their radar, but it's not quite the ultimate threat it's often made out to be. They're similarly focused on regulations, cloud upgrades, data health – and, perhaps counter to expectations, the very real threats that humans themselves present.

Hyperfocusing on new threats, pouring money into uncertain tech, and ignoring the less glamorous safety features might

distract you, but it won't protect you. Not when it matters. The true enemy of security is imbalance.

So, don't just focus on AI. Focus on a well-rounded, robust strategy that takes all threats into account and leaves no room for weak links. Treat your security as the complex, interconnected neural network that it is. When you reject the scapegoat and embrace a balanced strategy, you'll be prepared for whatever comes your way.

About Storyblok

Storyblok is a headless CMS that enables marketers and developers to create with joy and succeed in the AI-driven content era. It empowers you to deliver structured and consistent content everywhere: websites, apps, AI search, and beyond.

Marketers get a visual editor with reusable components, in-context preview, and workflows to launch fast and stay on brand. Developers have freedom to use their favorite frameworks and integrate with anything through the API-first platform. Brands get one source of truth for content that is accurate, flexible, and measurable.

Legendary brands like Virgin Media O2, Oatly, and TomTom use Storyblok to make a bigger, faster market impact. It's Joyful Headless™, and it changes everything.

Get Joyful. 

**See how Storyblok can revolutionize
your content at storyblok.com.**

TRY FOR FREE 

CONTACT US 