Google Workspace

Security at a tipping point

Why incremental fixes no longer work

October 2024

Welcome from Google

As the business landscape continues to be reshaped by changes in how and where we work, organizations worldwide face rapidly growing security threats. The recent Mandiant M-Trends report shows that in the last year alone, we've seen an increase in state-sponsored espionage and commercially-driven ransomware attacks on large government and commercial organizations, as well as a cascade of data breaches across every industry, from telecommunications to entertainment.

To help organizations better understand how to approach the new threat landscape, we recently commissioned a global security study, in partnership with Hypothesis Group. We talked with 2,000+ decision-makers at mid-market and enterprise organizations about how they approach security, changes they're seeing, and what they hope to do in the future.

We learned that the future of work is here, bringing with it a new era of security risks. But instead of adapting, many organizations are doubling down on traditional strategies and tools. The result? Costly and growing security incidents that disrupt business operations, impact customer data, and damage reputations. The status quo for security is no longer sufficient; it's time for a fundamentally different, better approach.

Businesses don't need more security products, they need more secure products. We believe that security incidents and breaches should be the exception, not the norm. And we want to help organizations feel more confident in their ability to proactively stave off attacks through solutions that are secure by design.

We hope this research is the first step in an ongoing conversation about your organization and its security needs, and how Google Workspace can be a strategic partner in your journey to enable safer work.

Andy Wen
Sr. Director of Product Management
Google Workspace Security

Table of contents

Introduction

The landscape of work is in a state of flux. As hybrid work becomes standard for millions of employees, and AI becomes more advanced, security threats are growing in sophistication and scale to take advantage of the shift. Organizations are increasingly aware of these new and escalating risks — yet many hesitate to make the bold choices necessary to truly secure their environments.

This paper delves into a central tension in today's business environment: while some leaders feel confident in their strategies, the persistence and severity of security incidents reveals a gap between perception and reality. Embracing the need for change, rather than investing in more of the same, can help organizations bridge the gap and better meet the security moment.

To better understand the status quo and what you can do to raise the security posture of your organization, Google Workspace partnered with Hypothesis Group, an insights, design, and strategy agency, on a multi-pronged research. This initiative included:

→ A quantitative survey of over 2,000 IT, business, and security decision-makers across the US, UK, India, and Brazil in mid-market (300-999 employees) and enterprise (1,000+ employees) organizations, fielded July 22–August 8, 2024.

→ Qualitative interviews with six US decision-makers conducted between August 22–26, 2024.

→ Conversations with industry experts about current trends and the future state of security including:

John McCumber
Former NIST Co-Chair and Gartner Director; Security Columnist

Dr. Joshua Scarpino
VP Information Security, TrustEngine
CEO, Assessed Intelligence

Rachel Tobac
CEO of SocialProof Security, Women in Security and Privacy Board of Director Chair, Volunteer on the CISA Technical Advisory Council

Key insights

Security is at a precipice: With current approaches proving unsustainable and costly, there's an urgent need for organizations to embrace change to stay ahead of evolving threats.

The rapidly growing threat landscape demands a new approach to security, but few have invested in transformative change.

1. **The status quo is unsustainable.** While organizations express confidence in their security posture, risky behavior abounds, and security leaders are increasingly worried.

2. **Organizations know they need to improve security — and doing more of the same isn't cutting it.** In their effort to enhance security, leaders are making additive changes (adding tools, increasing investment, increasing insurance premiums). Yet security incidents remain frequent and costly.

3. **Change is needed to meet the future.** Leaders display a clear desire for streamlining their security approach and utilizing AI to protect their organizations. Those who have addressed underlying inefficiencies fare better than those who limit themselves to band-aid solutions.

An organizational approach to meeting the security moment will vary by organization size and region — but all recognize the need for change.

4. **The mid-market (300-999) segment is primed for transformation.** Burdened by legacy technology and organizational complexity, leaders are highly anxious about the future. However, most are actively reconsidering their security approach and are open to a pivot.

5. **Globally, each region has distinct challenges, and consequently must chart a unique approach to meet the security moment.** Although leaders worldwide recognize the work landscape will continue to evolve, not all countries have a successful or sustainable security strategy, prompting widespread reassessment.

1

The status quo is unsustainable

While organizations express confidence in their security and ways of working, actual behavior exposes many chinks in the armor — keeping security decision-makers up at night.

Confidence abounds, but shifts in ways of working undermine security

Most organizations think they're doing fine when it comes to security — at least in theory. A full **96%** of decision-makers, including IT, business, and security leaders, express high confidence in their ability to manage security for data, applications, devices, and emerging technologies such as generative AI. But that confidence belies significant changes in how people actually work. Changes we heard about encompass everything from increased hybrid work to the introduction of new and different tools, particularly generative AI.

74%

say their ways of working have shifted dramatically

"We are living in a transition time. You have access to an enormous number of tools. But I have a lot of concerns because I feel like we don't have policies, and we don't have any plan to deal with all of these new tools."

— Research Director, Pharmaceuticals

Risky tools and behaviors are commonplace

Most decision-makers report numerous practices that expose organizations to risk:

- Only **56%** say they follow IT policies

- **19%** of tools used within organizations are unlicensed (i.e., tools that are not vetted and sanctioned by the organization)

- Nearly half (**44%**) believe unlicensed tools are "completely safe"

- Two-thirds (**63%**) report that unlicensed gen AI tools are used on a weekly basis

- And half (**48%**) of decision-makers trust unlicensed gen AI tools

That gap between what organizations say and what they do highlights the inherent risks in their current security postures. On top of that, the use of Shadow IT services — which is common and hard to secure — increases risk of not only incidents but compliance violations.

> *"Organizations don't always understand how risks evolve with new technologies, which can present challenges for security leaders because they're always playing catch-up."*

— **Dr. Joshua Scarpino**
CEO of Assessed.Intelligence

Anxiety is mounting among security leaders

Security decision-makers (SDMs) aren't oblivious to these risks.

63%

believe that their organization's technology landscape is less secure than it was in the past

1-in-4 tools are considered risky

> *"I would suspect [the belief of the landscape being less secure] has to do with a feeling of lack of control, lack of knowledge. It's a challenge for all of us to keep up and understand all the tools that are being used, where they're being used, how they're being applied, and how they're being leveraged against us in many ways."*

— **John McCumber**
Former NIST co-chair and Gartner Director; Security Columnist

This risky behavior is creating a climate of anxiety, with **93%** of SDMs worrying about security incidents. The sources of that anxiety are clear. While SDMs are most concerned about vulnerabilities and external attacks, whether it's a gen AI attack or the next data breach, they're also concerned about user inattention, whether intentional or inadvertent.

> *"Decision-makers are telling me they're worried and kept up at night. Technical tools aren't perfect, and they require a lot of human oversight, so decision-makers are very stressed out."*

— **Rachel Tobac**
CEO of SocialProof Security

⚠️ 93%
of SDMs worry about security incidents

Top attack/breach concerns

Gen AI attacks	**31%**
Data breaches	**30%**
Cyber extortion	**26%**

Top concerns with end users

Unauthorized access	**24%**
Employee negligence	**20%**
Compromised credentials	**17%**

2

Organizations know they need to improve security — and doing more of the same isn't cutting it

The need for enhanced security measures has never been more urgent. SDMs are acutely aware that their current strategies are coming up short, and they recognize that widespread improvements are necessary. But the approach taken by many is proving insufficient — and often counterproductive.

A clear call for enhanced security

Eighty-two percent of SDMs say they need to improve security measures. **Over half** say the complexity of modern work environments hampers their ability to keep their organizations secure. And **59%** admit that reliance on outdated technology has left them less prepared for future security needs.

> *"We have a full stack of security solutions over the years and some are really old tools that need to be replaced or reevaluated at the least."*
>
> — VP of IT, Media & Entertainment

82%
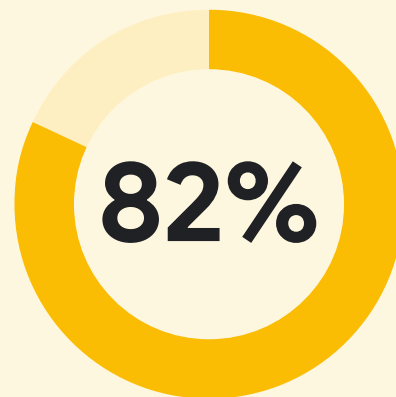
of security decision-makers say their organization needs to improve security measures

Incremental changes aren't enough

While half of SDMs say their cybersecurity strategies have undergone significant changes in the past two years, those changes are often incremental rather than transformative. In fact, most organizations appear to simply be doing more of the same.

Top security changes in past two years

Increased cybersecurity insurance	**37%**
Spent more on cybersecurity	**35%**
Upgraded licenses	**34%**
Added new cybersecurity providers	**31%**

While these adjustments may be beneficial to some extent, they represent more of an increase in existing practices rather than a fundamental change in strategy.

> *"People will throw money at the same thing to have multiple layers. I hear from my colleagues and customers, 'We've tried throwing so much money at it, and we're not actually helping the problem.' They'll throw money at some really expensive platform, but then they don't have a password manager for the team. It's like spending money on ballistic windows, but your door is wide open."*

— **Rachel Tobac**
CEO of SocialProof Security

62%

of SDMs say they expand their tools when new features are needed (vs. replacing old tools)

10

security tools used on average for enterprise organizations

61%

of organizations are using more security tools than they did two years ago

27%

of security tools are duplicative

The pitfalls of excess — and the need for a more cohesive strategy

Over two-thirds of organizations are investing more time and money than ever in securing their environments — but still experiencing a plethora of expensive incidents.

However, those with fewer tools fare better. Organizations using 10+ security tools report a higher frequency of security incidents while incurring greater costs.

81%
of organzations are seeing at least one incident a year

8 incidents reported per year on average

$4.88M USD
global average total cost of a breach reached in 2024[1]

Organizations with 10 or more security tools

Organizations with fewer than 10 security tools

Number of security incidents in a year

| 14 | vs | 6 |

Spent $250K+ on security incidents in a year

| 34% | vs | 19% |

"It's extremely difficult to manage and not cost-effective when you need a different vendor for every aspect of security. So, we do need to consolidate — the number of vendors we have is unsustainable."

— VP of IT, Media & Entertainment

1. IBM – Cost of a Data Breach Report 2024

3

The future demands change

Our research reveals that SDMs are open to approaching security differently — and those who actively pursue new strategies and technologies are coming out ahead.

A desire for change

The current climate is prompting a shift in how organizations are thinking about their security strategies.

78%
are reconsidering their organization's approach to security given the current cybersecurity climate

73%
are open to new security approaches, regardless of cost

Decision-makers are increasingly drawn to streamlined security solutions, with **65%** expressing interest in unified security systems. They agree that a platform that consolidates different sources of data within a single interface would offer tangible benefits, including streamlined processes, enhanced operations, removing the burden of managing multiple tools, and time savings.

Gen AI is also gaining traction, with **59%** of security decision-makers seeing it as a key tool in combating evolving threats.

> *"The biggest impact in security with AI is going to be the ability to respond to events, use the tools that you currently have, and orchestrate those in a way that's going to be able to respond, report, and clean up."*

— **John McCumber**
Former NIST co-chair and Gartner Director; Security Columnist

59%
of SDMs see gen AI as a key tool for data security

Top reasons for adopting gen AI

Boosting data privacy	**43%**
Enhancing threat intelligence	**37%**
Improving security operations	**36%**
Threat prevention	**33%**

The benefits of investing in change

Despite strong interest in new approaches, only **38%** of SDMs are actively replacing outdated tools, while **62%** are expanding their current setups.

SDMs that replace older tools (vs. those that expand)...

Report **20% fewer security incidents** per year

Are more likely to **use the same or fewer** security tools than 2 years prior
(44% VS. 36%)

Say they **spend less time** securing their environment than they used to
(33% VS. 28%)

"Teams need to audit their purchased tools to gain an understanding of which capabilities they already have before buying the same protection again and again. Understanding which capabilities are available and which security areas need coverage will help organizations have a better understanding of their tools, which ultimately leads to fewer security incidents and issues."

— **Rachel Tobac**
CEO of SocialProof Security

4

The mid-market is primed for transformation

Mid-market organizations (300-999 employees) are falling short of their full security potential — and they know it. As they grapple with the complexity of modern work environments, their concerns far outpace enterprise organizations (1,000+ employees).

Mid-market decision-makers also express a growing sense of unease about the current technology landscape. These concerns are amplified by the rapid adoption of gen AI in the workplace.

73%

say increased use of gen AI has led to a rise in security incidents within their organizations

(VS. 58% FOR ENTERPRISE ORGANIZATIONS)

What they are up against

	GAP TO ENT
71% say legacy technology has left them less prepared for the future	+23 pp
63% say complexity of how they work hinders their security	+11 pp
73% say gen AI usage has contributed to rise in security incidents	+15 pp

How they feel

	GAP TO ENT
63% feel a large amount of anxiety about a potential security incident	+13 pp
63% say the technology landscape is less secure than it used to be	+12 pp
36% say their security team is overwhelmed by security threats	+16 pp

An openness to new approaches

Eighty-two percent of mid-market security decision-makers report that their organizations are actively reconsidering their approach to security. Mid-market decision-makers demonstrate a growing belief in the benefits of cloud-native solutions, with **81%** of mid-market security decision-makers saying that cloud-native apps are more secure than traditional desktop applications. That confidence in cloud technologies suggests that mid-market companies are not only aware of the need for change but are ready to embrace more innovative solutions.

> *"Mid-market organizations are unique because they're prepping for going up market quickly — they're scaling. This is where they need to get foundations in place, because if they don't, they're going to be so far behind and the concerns they have are going to become realized."*

— **Dr. Joshua Scarpino**
CEO of Assessed.Intelligence

82%

of mid-market security decision-makers are actively reconsidering their approach to security

5

Globally, each region has a distinct approach to meet the security moment

While decision-makers universally acknowledge that the ways they work have changed significantly in the past year, the approach to addressing these changes, especially in terms of security, varies greatly across countries.

Across all regions, decision-makers report that their work environments have been transformed compared to a year ago, and security decision-makers in every market are rethinking their approach to security.

"The way we work is extremely/somewhat different compared to 12 months ago"

🇮🇳	INDIA	**85%**
🇧🇷	BRAZIL	**74%**
🇬🇧	UK	**73%**
🇺🇸	US	**62%**

"Our organization is reconsidering our approach to security"

🇮🇳	INDIA	**83%**
🇧🇷	BRAZIL	**76%**
🇬🇧	UK	**82%**
🇺🇸	US	**71%**

INDIA

Overwhelmed by complexity, but eager for change

India's security landscape stands out due to its sheer complexity and proliferation of tools. But there's a strong desire for change with organizations in India being very open to improving security and exploring new options. India is clearly at a tipping point, with decision-makers recognizing the need for a more streamlined and effective security strategy.

Security snapshot

	GAP TO GLOBAL AVG ↓
35 tools used on average (e.g. products, services, apps)	+11
19 security tools used on average	+9
67% say complexity of how they work hinders their security	+10 pp

Desire for change

	↓
82% believe their organization's security needs improvement	+8 pp
81% are open to exploring new security approaches, regardless of cost	+8 pp

BRAZIL

High levels of anxiety, but less focused on specific threats

Decision-makers in Brazil express elevated levels of anxiety about security incidents and their outcomes. Yet, they also are less concerned about specific causes of security issues, revealing a tension in fear of outcomes, but not the vulnerabilities that cause incidents. Organizations in Brazil voice a desire for change — showing some of the strongest interest in deploying gen AI (71% vs. 62% global average).

Anxiety over security

	GAP TO GLOBAL AVG ↓
41% say they worry constantly about security incidents	+19 pp
42% worry about loss of trust (from an incident)	+8 pp
37% worry about loss of customers (from an incident)	+7 pp
39% worry about brand damage (from an incident)	+5 pp

Lower concern of specific issues

	↓
40% say legacy tech has left them less prepared for the future	-19 pp
48% say gen AI usage has contributed to rise in incidents	-17 pp
44% say complexity of how they work hinders their security	-13 pp

🇬🇧 UNITED KINGDOM

Concerned about emerging tech, but slow to act

UK decision-makers are deeply concerned about the impact of emerging technologies on security, especially in relation to legacy systems and gen AI threats. However, the UK has been slower to implement policies to mitigate these risks and decision-makers report a higher level of burnout. Despite these challenges, UK organizations are less open to new security approaches and more likely to view security breaches as inevitable.

Worried about tech

	GAP TO GLOBAL AVG ↓
75% say legacy tech has left them less prepared for the future	+16 pp
77% say gen AI usage has contributed to rise in incidents	+12 pp

Less open to change, despite challenges

	↓
43% say their security team is overwhelmed/burned out by security threats	+15 pp
44% view security breaches as inevitable	+14 pp
27% introduced gen AI-specific security policies	-14 pp
60% are open to exploring new security approaches, regardless of cost	-13 pp

🇺🇸 UNITED STATES

Overconfidence may mask underlying risks

US decision-makers display a high level of confidence in their security posture — they are less likely to worry about breaches, particularly in relation to gen AI. While that optimism is commendable, it raises questions about whether US organizations are underestimating the rapidly growing threat landscape — especially because the cost of data breaches in the US is the highest in the world. Without a clear focus on emerging risks, overconfidence could leave some organizations vulnerable to future attacks.

Confident about security landscape

	GAP TO GLOBAL AVG ↓
10% say they worry constantly about security incidents	-12 pp
55% say gen AI usage has contributed to rise in incidents	-10 pp
52% say that the technology landscape is less secure than it used to be	-4 pp

Highest data breach costs

	↓
$9.36M USD average cost of a data breach in 2024[1]	+$5M

1. IBM – Cost of a Data Breach Report 2024

Key takeaways

"It's critical to get the whole organization to understand security risks; executive leadership often doesn't understand the value prop of security. But security professionals need to be able to explain things simply - be able to say 'Here's the risk and here's the solution.'"

Dr. Joshua Scarpino
CEO of Assessed.Intelligence

① Security and business leaders need to work together

Security decision-makers and senior executive leaders need to work together with open communication and have a strong risk management process to have a successful security strategy. For SDMs, getting buy-in from stakeholders and forming deeper partnerships can mean the difference between security functioning productively versus as a tension point.

② Transformation shouldn't have to wait for a breach

Using a crisis (such a data breach) can be a great catalyst for security decision-makers to get approval for needed security measures. However, the fact that cyber attacks such as ransomware can physically disrupt operations for virtually any business overnight, makes it increasingly important to proactively make the necessary changes today. For most businesses, it's a matter of when and not if a breach is going to happen.

③ Focus on where the attacks start

According to Mandiant's latest M-Trends report, 72% of successful intrusions in 2023 started with a compromised identity (e.g., phishing or stolen credentials) or software exploit. This means that simple improvements in those areas can bring outsized benefits for organizations. For example, using products like Google Workspace, which offers a phishing-resistant two-factor authentication, automatically blocks more than 99.9% of spam, phishing attempts, and malware from ever reaching your users, and does not have desktop client apps or on-premises that need to be patched or updated.

> *"People think, 'I've got to buy this big, expensive program or tool. It has to cost hundreds of thousands of dollars in order for it to be efficacious.' In reality, some of the largest changes they can make are institutional policy based and cultural at their company."*
>
> **Rachel Tobac**
> CEO of SocialProof Security

> *"AI is going to be incorporated into security tools to enhance our ability to respond to incidents and threats. It's going to have some really impactful capabilities. I think the promise of it is still to be realized, but there's a lot more that's going to come."*
>
> **John McCumber**
> Former NIST co-chair and Gartner Director; Security Columnist

④ Change can be made in small steps

Modernizing your entire legacy software ecosystem can seem daunting, but meaningful security gains can be achieved in a phased approach with a minimal impact on end users. For example, by deploying Chrome Enterprise for your users, you can provide them with a secure browsing experience with built-in phishing & malware defenses, zero trust access without VPN, and data protection controls with a web browser that many already know and love.

⑤ Gen AI can add risks — but also offer protection

It's important to use gen AI tools that are safe and compliant with industry standards, such as Gemini, to reduce data loss risks. Gen AI can also help to protect organizations against emerging threats. For example, AI defenses in Gmail already use large language models (LLMs) to better defend against spam and phishing attempts. In fact, thanks to LLMs, 20% more spam is blocked in Gmail and 1000x more user-reported spam can now be evaluated by Gmail each day. This is a meaningful quality of life improvement for billions of Gmail users thanks to AI.

Research Objectives

01
Understand the current security landscape (unique priorities, mindsets, concerns, challenges)

02
Assess the impact of security and technology on organizations, particularly in relationship to the rise of gen AI

03
Explore the future of security, which trends are emerging, how organizations intend to invest in the future

Methodology

QUANTITATIVE SURVEY
A 20-minute online survey conducted July 22–August 8, 2024, among 2,025 respondents in the US, UK, Brazil, and India.

To meet the screening criteria, respondents needed to be:

- Employed at organizations with 300+ employees; range of sizes
  - Business or IT decision-makers with purview over organization or team level tech/productivity products OR
  - Security decision-makers with purview over organization security products
- Mix of industries, regulated and non-regulated

REGION	(n=)
United States	**501**
United Kingdom	**523**
Brazil	**501**
India	**500**
ORGANIZATION SIZE	
Mid-market (300-999 employees)	**834**
Enterprise (1,000+ employees)	**1,191**
ROLE	
IT decision-makers	**673**
Business decision-makers	**762**
Security decision-makers	**590**
TOTAL	**2,025**

IN-DEPTH INTERVIEWS
Six (6) one-hour virtual in-depth interviews in the US conducted August 22-26, 2024. Participants were C or C-1 executives at a 300+ size organization (mix of ITDMs, BDMs and SDMs).

EXPERT INTERVIEWS
At key project milestones, 3 security experts were consulted to offer insight, expertise, and thought partnership (John McCumber, Dr. Joshua Scarpino, Rachel Tobac).

Research & design by **hypothesis**