



Google Workspace

How Google Workspace helps protect your organization

Safely connect, create, and collaborate while protecting your information in the new world of work.



Table of contents

Executive summary	3
The way we work has fundamentally changed	4
How legacy tools expose you to increased security risks	5
How Workspace is architected for the modern threat landscape	6
Detect and prevent spam, phishing, and malware powered by Google AI	8
Enable safer work from anywhere	9
Achieve compliance and digital sovereignty	13
Keep your data safe in the era of generative AI	16
Gemini for Workspace privacy and security controls in practice	17
What customers are saying about Workspace Security and Sovereignty	20
Transform the way work is done and securely unleash the full potential of your employees	21



Executive summary

Designed with the modern threat landscape in mind, Google Workspace is the world's most popular and secure cloud-native communication and collaboration suite. With Workspace, organizations no longer need to patch thick desktop apps, worry about the loss of local files stored on end user devices, or keep infrastructure secure and up-to-date. This in turn helps IT and security teams to reduce security risks, costs, and their workload.

Main points:

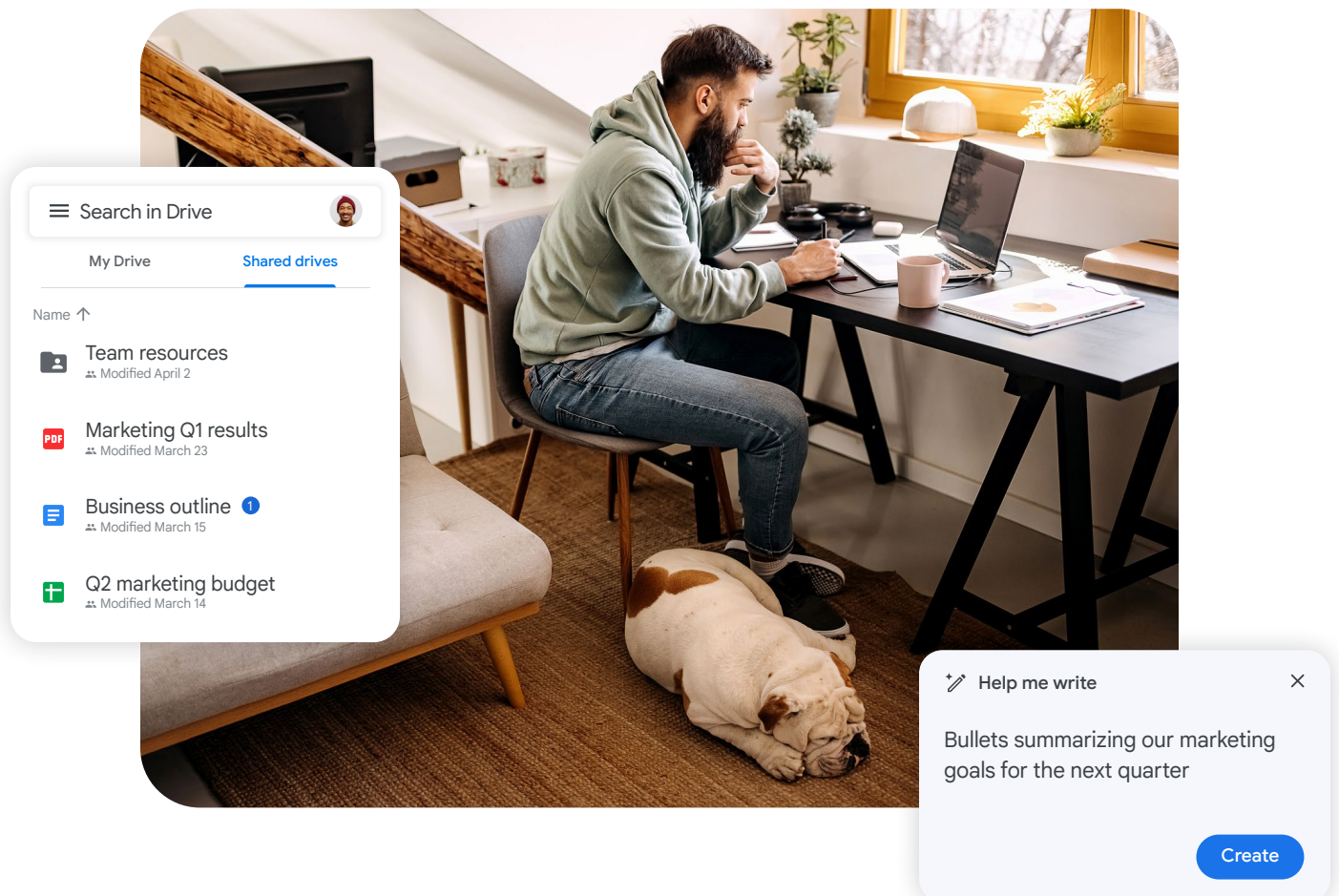
-  **Legacy tools leave organizations vulnerable to security threats:** legacy collaboration tools are increasingly targeted by hackers, due to the reliance on on-premise infrastructure and software patching.
-  **Google Workspace is certified for the most rigorous standards:** it supports various compliance requirements like FedRAMP High, DoD IL4, HIPAA, GDPR, and many more, and offers additional controls for digital sovereignty.
-  **Google Workspace is structurally more secure:** Google Workspace is cloud-based, works in any browser and mobile app, and is automatically updated, making it less susceptible to vulnerabilities and data breaches. It also offers advanced security features like AI-powered threat detection, zero-trust access controls, and strong account protection.
-  **Gemini for Workspace helps boost your productivity while keeping your data private:** whether you ask Gemini for Workspace to summarize an email, take notes in a meeting, write a blog post, or add a unique image to your slide, your data is yours and under your control. In simple terms, this means that Gemini for Workspace only uses your content to provide more useful responses to your prompts and does not use your content to train or improve Gemini for Workspace or any other generative AI models.

Main benefits:

- ✓ Helps prevent threats before they emerge
- ✓ Enables safer work for your organization from anywhere, on any device
- ✓ Helps you stay compliant with regulations and maintain sovereignty over your data
- ✓ Saves you time and boosts your creativity while keeping your data private and under your control

The way we work has fundamentally changed

Generative AI is accelerating work. Organizations and users are accessing, creating, and sharing more sensitive data and information than ever before, and much of this data is now stored in the cloud for easy access anywhere in the world. It is frequently shared with internal, external, and now, generative AI collaborators like Gemini for Google Workspace. This modern way of working and the rapid advancement of generative AI in the workplace have many benefits, but it also creates new security challenges — challenges that legacy collaboration tools aren't equipped to handle.



How legacy tools expose you to increased security risks

A growing number of successful attacks target legacy tools

277
days

average time to identify and contain a data breach¹

\$9.48
million

average cost of a data breach in the United States.
\$4.45M on average globally¹

73
days

mean time to patch a vulnerability in third-party software¹

Legacy tools simply weren't built for today's modern collaboration. The continued use of local desktop software, local files, and on-premise identity directories increases security risks. At the same time, IT teams struggle to keep up with the rapidly increasing quantity and sophistication of the latest cyber attacks, made even more difficult by distributed workforces, temporary workers, and hybrid work arrangements.

These outdated approaches and vulnerabilities result in increased security risks and higher costs for customers. Coalition, a cyber insurance company, conducted an independent analysis based on their 40,000 customers and uncovered the following benefits of choosing Workspace over Microsoft 365 or Exchange:

- **More than 2x as likely** to experience a security claim with Microsoft 365 vs Google Workspace²
- **Nearly 3x as likely** to experience a security claim with Microsoft Exchange vs Google Workspace²
- **2.33x as likely** to experience a funds transfer fraud (FTF) or business email compromise (BEC) claim with Microsoft 365 or Exchange vs Google Workspace²

How Workspace is architected for the modern threat landscape

Workspace is architected differently — and it matters. As a cloud-native service with automated threat defenses powered by Google AI, Workspace is designed for the modern threat landscape and can help commercial, education, and government organizations defend against harmful content, prevent account takeovers, and identify, triage, and respond to threats.

Google keeps your business safe — no matter its size — with a zero trust security model built for modern collaboration. Unlike the legacy choices that require more time and money on a separate cloud to meet data security and privacy requirements, Workspace is a single cloud that is always up-to-date with the latest productivity and security capabilities. Our defense-in-depth infrastructure was developed by top security experts through decades of learnings and security best practices.



Prevent threats

Protect your organization and its data by implementing login protections and controls to guard against targeted attacks and prevent account takeovers from phishing, malware, and social engineering scams.



Enable safer work from anywhere

Built-in controls and a zero trust approach for least-privilege access to sensitive data that is granted to the right people under the right conditions so your workforce can work safely from anywhere and on any device.



Achieve digital sovereignty and compliance

A comprehensive set of sovereignty features and controls provide visibility into your cloud provider's access to your data and meet your compliance and regulatory requirements.



Help keep your data private in the era of generative AI

Gemini for Workspace only uses your content to provide more useful responses to your prompts and does not use your content to train or improve Gemini for Workspace or any other generative AI models without your permission.

This approach to security is corroborated by a very solid track record of protecting customers from a wide range of modern cyber threats:

0

Google Workspace common vulnerabilities and exposures (CVE) over the last 3 years³

0

Google systems were affected by the SolarWinds event.⁴

0

evidence of a successful phishing attempt on accounts enrolled in Advanced Protection Program⁵

And that results in benefits both technical and financial for Workspace customers, as evidenced by an independent analysis conducted by At-Bay, an insurance company, and based on the number of insurance claims submitted by their customers:

- **50%** fewer security incidents for organizations using Workspace vs Microsoft 365.⁶
- **62%** fewer email security incidents for organizations using Workspace vs Microsoft Exchange.⁶
- **50%** could be saved on cyber security insurance premiums by using Workspace.⁶



Reduce costs while lowering security risks

We commissioned a [Forrester Total Economic Impact™](#)⁷ study on how companies can realize benefits and savings by switching to Workspace. Four measurable benefits were identified, including revenue growth, employee efficiency, risk mitigation, and IT support services.

Forrester found that enhanced security coming from Workspace results in security tool **cost savings of \$1.8M** over three years for organizations on average.

Detect and prevent spam, phishing, and malware with Google AI

Workspace benefits from AI-powered security features, so you can minimize worries about malware or spam slipping through the cracks. And no costly add-ons are needed to fix any new vulnerabilities that are constantly being identified.

Every day, Gmail's AI-powered defenses:

- [Stop more than 99.9% of spam](#), phishing, and malware from reaching inboxes
- [Block nearly 15 billion unwanted emails](#)
- [Block over 100 million phishing attempts](#)

Prevent account takeovers and protect your organization

Google keeps your users and data safe, everywhere and on every device.



Implement login protections and controls

Guard against targeted attacks and help prevent account takeovers with [login protections and controls](#)



Transition to passwordless logins

Implement [passkeys](#), a simpler and more secure authentication method than passwords



Provide added safeguards to accounts at high risk for targeted attacks

Enroll admins or business leaders into Google's [Advanced Protection Program](#)

Enable safer work from anywhere

The zero trust security model has become an essential part of reducing security risks for a distributed workforce. Workspace was built with this model in mind from the get-go with its cloud-only architecture and learnings from Google's own [BeyondCorp implementation](#).

Traditional productivity solutions often rely on desktop apps that typically need to be patched, local files stored on end user devices that can put sensitive data at risk, and vulnerable corporate networks and VPNs.

With Workspace, we took a different approach by making it available directly in the browser and mobile apps, storing your data in the cloud, and using zero trust controls to help ensure that only the right people under the right conditions can access your data.

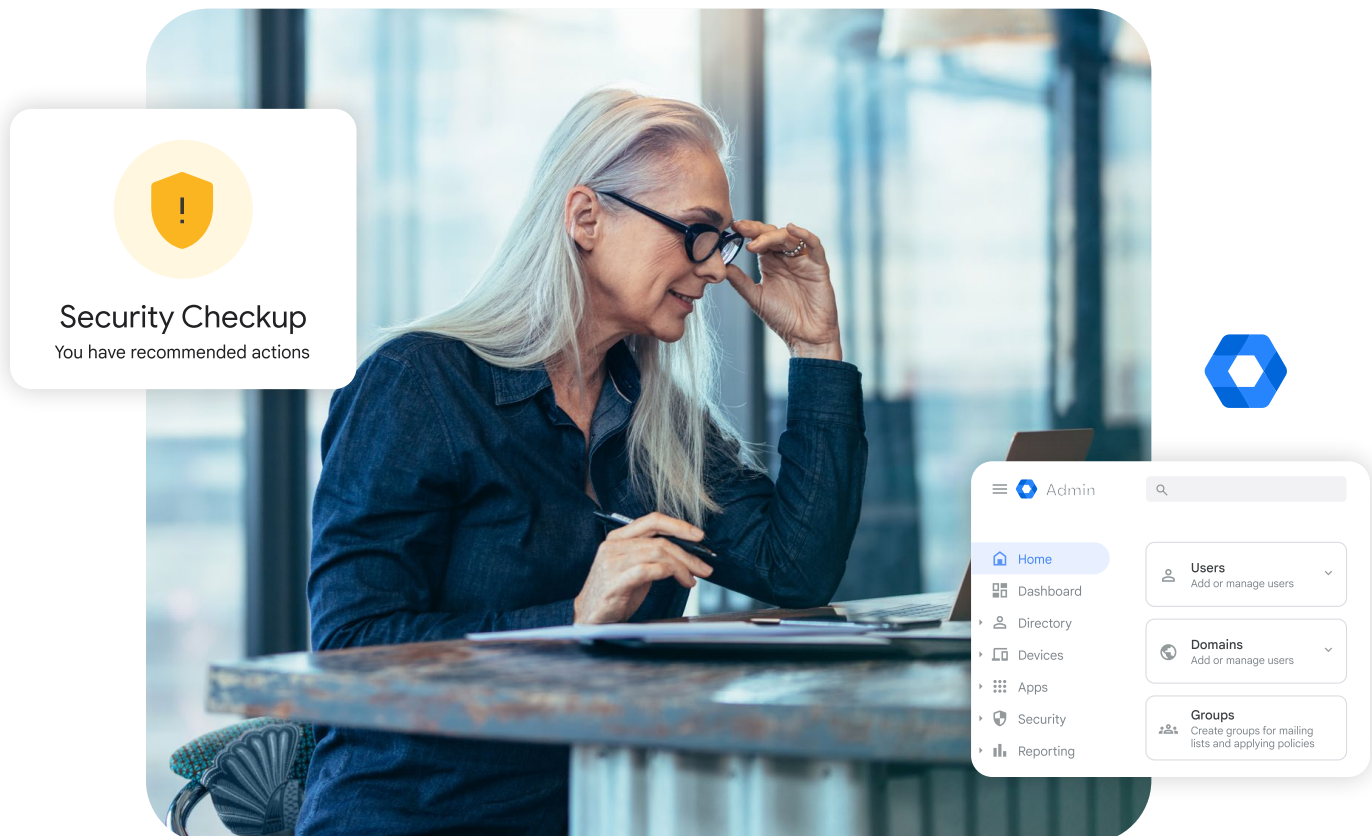
With its modern architecture and security controls, Workspace can help organizations accelerate their zero trust adoption and meet industry frameworks, such as [CISA's Zero Trust Maturity Model](#), by helping to:

- **Enforce contextual access with zero trust controls**
- **Guide users to do the right thing**
- **Protect company data on virtually any device, anywhere**



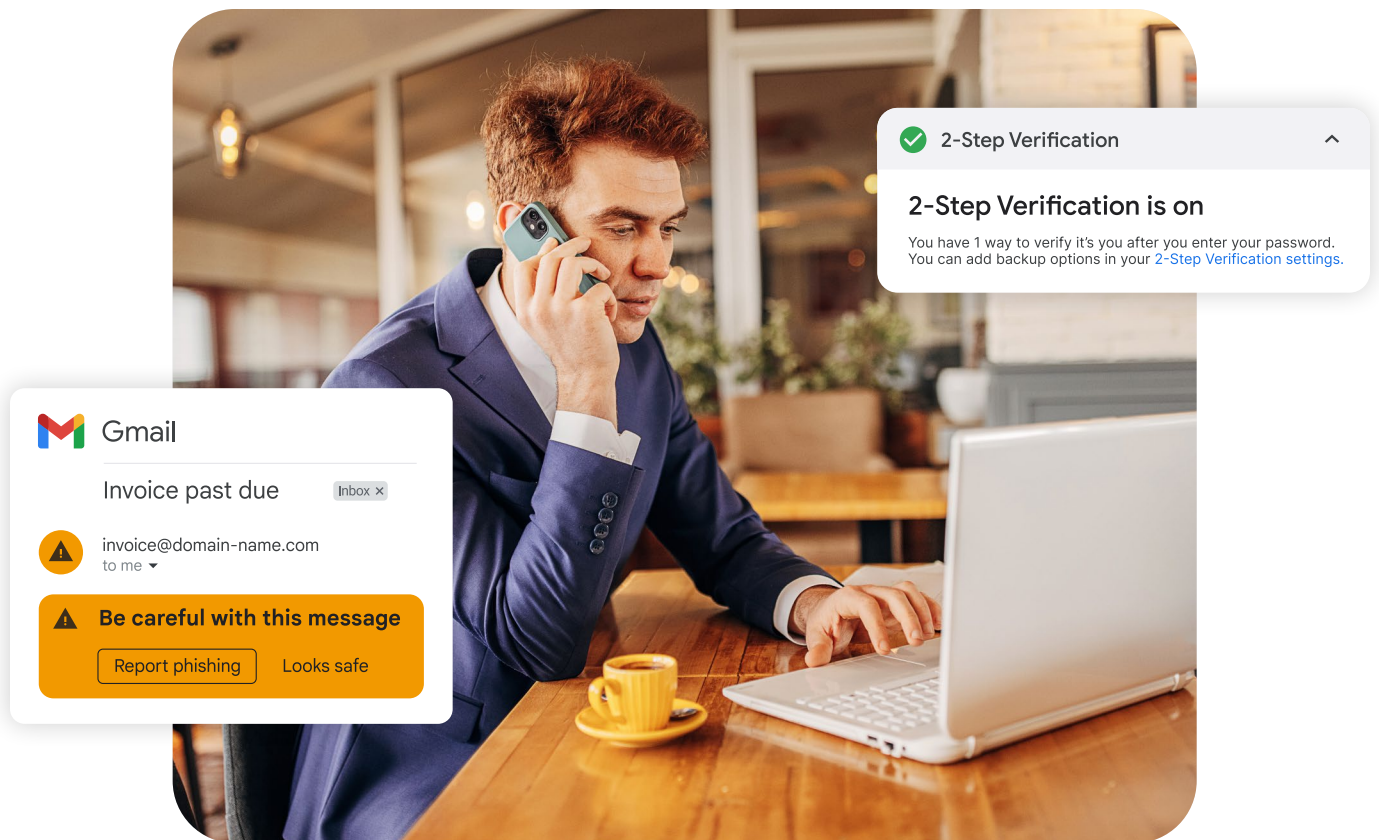
Enforce contextual access with zero trust controls

Unlike other productivity and collaboration tool providers who assume that anyone with access to the corporate network is a legitimate user, Workspace continuously validates the context of a request to protect against unauthorized access to confidential information. Admins can create granular context-aware access policies based on attributes, such as device location or security status, to help control user access to Workspace apps and APIs. They can also understand the impact of access policies before deploying them with Monitor Mode to plan and minimize disrupting work. Admins can extend the data access and protection controls for Workspace apps and APIs to other apps accessed through Chrome with BeyondCorp Enterprise to strengthen their defenses and reduce risk.



Guide users to do the right thing

Today, there is a major gap between the employees who are aware of the data sharing policies and those who are not. Admins can create tailored data loss prevention (DLP) policies to help detect confidential information and control the sharing of it inside and outside their organization. They can also combine data loss prevention policies with context-aware access policies for further protection against data loss and ensure certain criteria are met before an end user is able to share sensitive content. For another layer of protection, admins can leverage Google AI to continuously classify data and help ensure data is appropriately shared and protected from exfiltration.



Protect data on virtually any device, anywhere

Because Google Workspace is designed to enable secure collaboration in a hybrid world, admins can secure company data on almost any device type including Android, ChromeOS, iOS, and Windows. This enables various device scenarios including employee-owned (BYOD), corporate-issued, or third-party managed. Because data resides in the cloud, admins can approve, block, or delete a device's access to data or erase data on a lost or stolen device from a single location and with minimal effort. Admins can also integrate with purpose-built third-party device management solutions for unified endpoint management and mobile threat defense services.



Achieve compliance and digital sovereignty

The world's data is becoming more highly regulated. [Gartner \(2022\)](#) estimates that by the end of 2024, 75% of the world's population will have personal data covered under a modern privacy regulation. Workspace gives you control and privacy over your data, so that you can uphold data sovereignty and remain compliant.

We hear from customers that to maintain compliance, organizations have three goals for their data:

- 1 Ensuring local access to data
- 2 Preventing foreign access to data
- 3 Persistent security and privacy of data

Legacy cloud providers focus on in-country data residency, but this alone isn't sufficient to achieve those goals as your data crosses so many boundaries, networks, and providers. Meeting these goals requires a holistic approach of digital sovereignty and security built in from the ground up. We believe this is what really sets Workspace apart to support companies' digital sovereignty journeys beyond data residency:

-  We provide flexible options for customers — customer data can be stored and processed in the US or EU, and if you need more control you can store your data in a specific country with local data storage.
-  We are the only cloud provider today to provide not just contractual assurances that we won't access your data, but technical capabilities such as client-side encryption to ensure that we and foreign governments can't access your data.
-  In order to remain compliant, you need to build on a foundation of security to prevent losses and breaches.

Workspace brings a whole new approach to sovereignty and compliance, solving for structural security risks of other legacy providers:



Data loss due to locally stored files: with Workspace, your data is stored in the cloud, which means that it is they are not stored on users' devices. With data being in the cloud, access to it is verified with every request from the user and can be immediately revoked. You can also apply effective DLP, IRM, and zero trust access controls without having to rely on special agents on end user devices. It might sound simple, but the fact that the data is in the cloud, makes it much easier to control and secure than the files being spread out of thousands of end user devices.



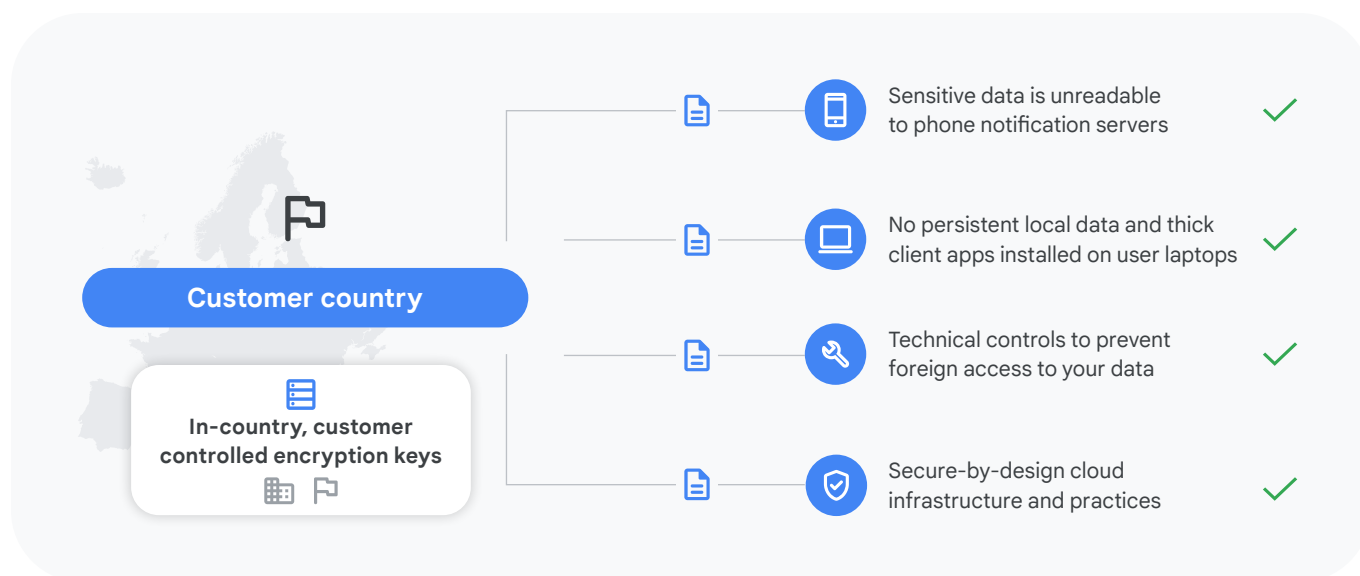
Data breaches due to vulnerabilities: with Workspace, there are no thick client apps to patch or protect from vulnerabilities. All Workspace apps can be accessed from browsers, including Chrome. This is another attack surface that you don't need to worry about.



Foreign access to your data: with Assured Controls and client-side encryption in Workspace, you can get complete control over your data. Client-side encryption allows you to store encryption keys outside of Workspace in the country of your choice, ensuring that Googlers and foreign government law enforcement agencies cannot read your data.

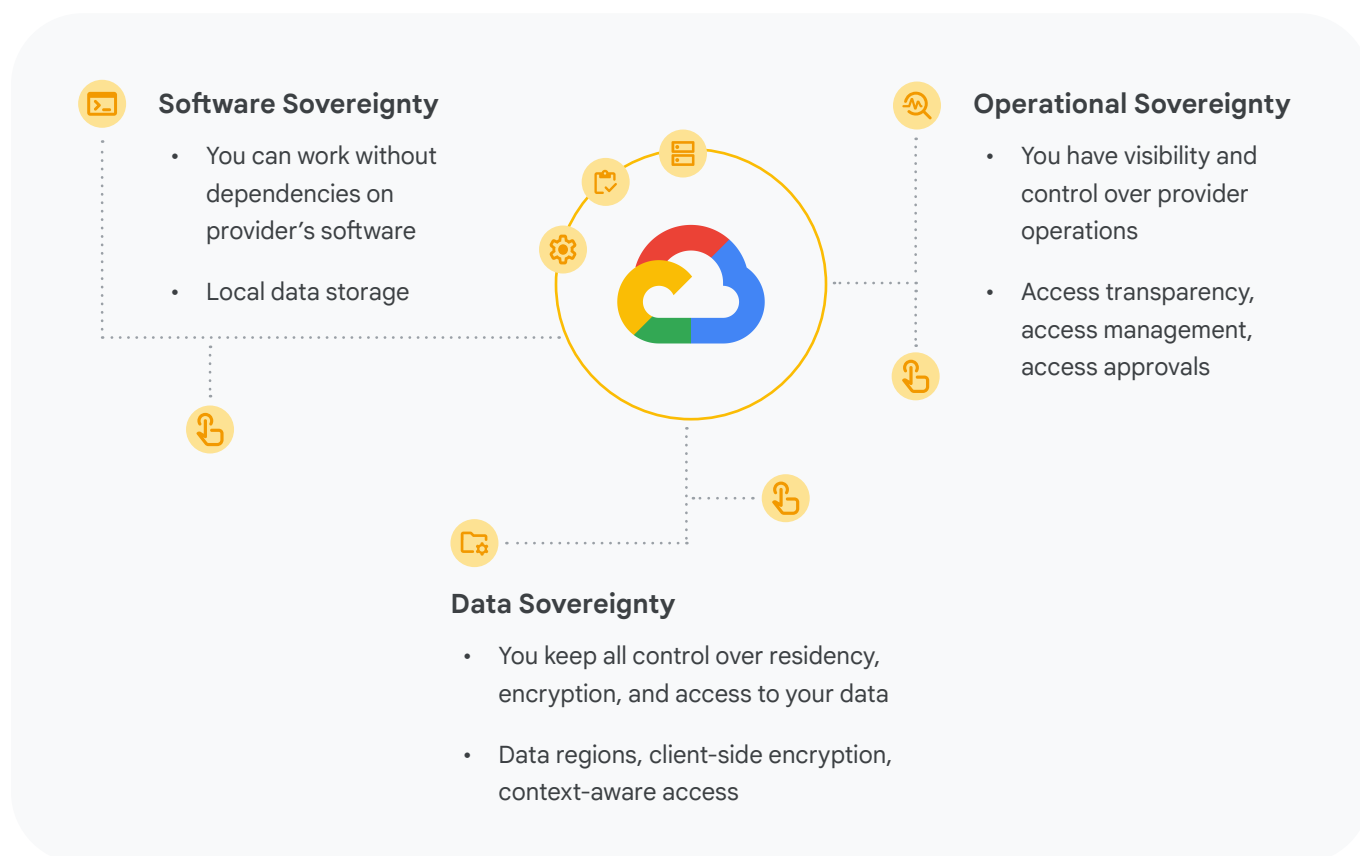


On-premises breaches due to vulnerabilities: Google Workspace does not require any on-premises infrastructure, which means that there is no on-premises infrastructure to be vulnerable to attack.



In addition to compliance, digital sovereignty is a topic that's top of mind for many of our customers and governments around the world. We've developed a comprehensive set of Sovereign Controls for Workspace that answer the call of emerging regulatory requirements. Workspace offers three pillars of digital sovereignty:

-  Software sovereignty, which ensures that customers have a copy of their data in-country, so that they are independent from a cloud provider's software
-  Data sovereignty, which provides the customer choice over where their data is stored and ultimate control over how their data is accessed.
-  Operational sovereignty, which enables customers to have control over how, when, and from where Google's support personnel access data for troubleshooting purposes.



Keep your data safe in the era of generative AI

Across Google Cloud and Workspace, we've long shared robust [privacy commitments](#) that outline how we protect user data and prioritize privacy. Generative AI doesn't change these commitments — it actually reaffirms their importance. We want to be completely clear that generative AI does not change our foundational privacy protections for giving users choice and control over their data. To that end, here are key facts about how Workspace data is handled:

- ✓ **Your data is your data.** The content that you put into Workspace services (emails, documents, etc.) is yours. We never sell your data, and you can delete your content or export it.
- ✓ **Your data stays in Workspace.** We do not use your Workspace data to train or improve the underlying generative AI and large language models that power Gemini, Search, Vertex, and other systems outside of Workspace without permission.
- ✓ **Your privacy is protected.** Interactions with intelligent Workspace features, such as accepting or rejecting spelling suggestions, or reporting spam, are anonymized and/or aggregated and may be used to improve or develop helpful Workspace features like spam protection, spell check, and autocomplete. This extends to new features we are currently developing like improved prompt suggestions that help Workspace users get the best results from Gemini for Workspace features. These features are developed with strict [privacy protections](#) that keep users in control. (See below for more detail on additional privacy, security, and compliance commitments we make for business customers).
- ✓ **Your content is not used for ads targeting.** As a reminder, Google does not collect, scan, or use your content in Workspace services for advertising purposes.

These are the privacy commitments that Workspace extends to all of its users. But they aren't just words. To ensure we continually meet these high standards, independent auditors validate our practices against international standards and best practices.

Gemini for Workspace privacy and security controls in practice

When Workspace commercial customers adopt [Gemini for Google Workspace Enterprise](#), they get the same robust data protection and security standards that come with all Workspace services, with specific protections for business, education, and government customers:

- ✓ **Your interactions with Gemini stay within your organization.** Gemini stores any prompts or generated content alongside your Workspace content and does not share them outside your organization.
- ✓ **Your existing Workspace protections are automatically applied.** Gemini brings the same enterprise-grade security as the rest of Workspace, automatically applying your organization's existing controls and data handling practices, such as data-regions policies and Data Loss Prevention.
- ✓ **Your content is not used for any other customers.** None of your content is used for model training outside of your domain without permission.



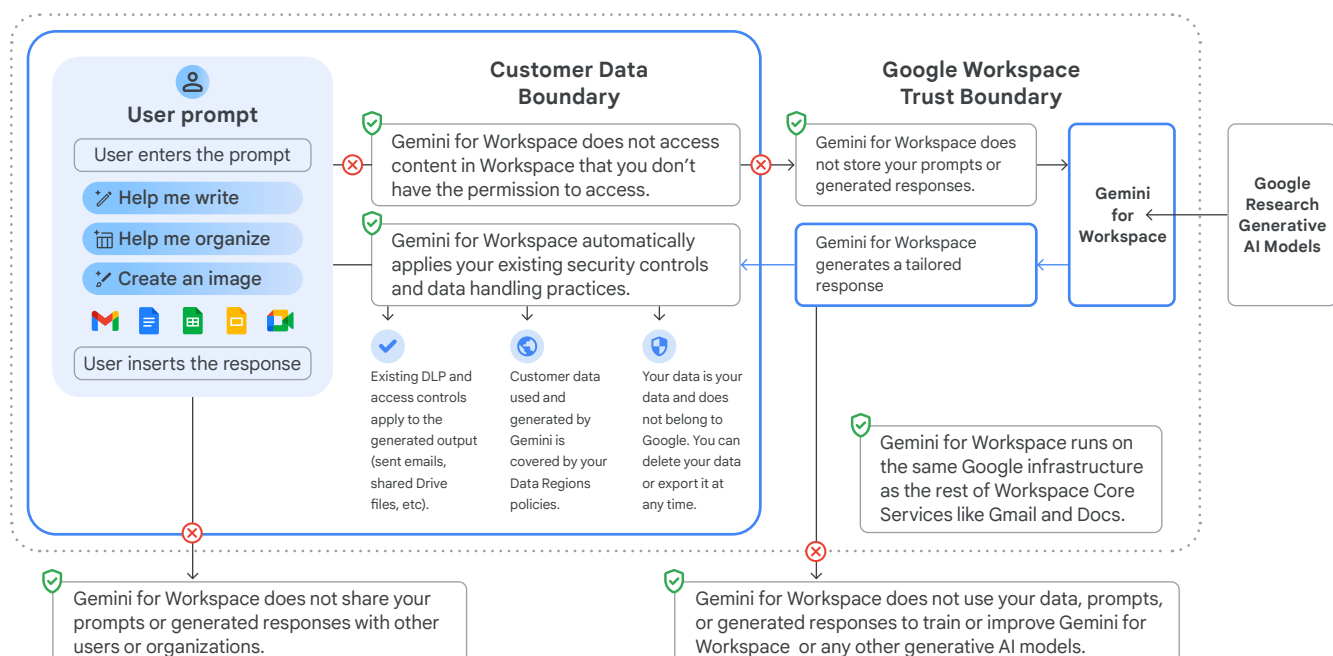
How Gemini for Workspace sits within your trust boundary

When the user issues a prompt, Gemini for Workspace only uses the documents and information for which the user has been granted access to. We do this in order to ground the prompt and make it more helpful and contextual. Gemini for Workspace does not use your data, prompts, or generated responses to train or improve Gemini for Workspace or any other generative AI models.

Gemini for Workspace runs on the same Google infrastructure as the rest of Workspace Core Services like Gmail and Docs which automatically applies all your existing Workspace security controls, helps protect your data and interactions from leaking outside of your organization, and helps address your compliance and data storage requirements. In fact, our compliance teams are already working with regulatory authorities to extend Workspace's certifications to Gemini for Workspace.

And under no circumstances, will Gemini for Workspace allow your data or prompts to leak outside your organization. We are committed to equipping customers with powerful technical solutions that help them adapt to, and stay on top of, a rapidly evolving regulatory landscape.

Gemini for Workspace Enterprise data privacy and governance



How Workspace seamlessly works with your existing first-party and third-party security tools

-  In addition to the core security and trust capabilities built into the Workspace platform, we also integrate with security products from Google and our partners to help customers strengthen their defenses and reduce risk.
-  With BeyondCorp Enterprise, you extend threat and data protection to the rest of your SaaS applications. The same policy engine that runs Workspace DLP and context-aware access also runs BeyondCorp Enterprise.
-  For security challenges outside of application security, we provide many first-party and third-party integrations, such as Chronicle, Crowdstrike, Palo Alto Networks, VMware, Okta, JumpCloud, Thales, and more.
-  Google Workspace combined with BeyondCorp Enterprise and other security products gives you virtually everything you need to enable a more secure workforce.



What customers are saying about Workspace Security and Sovereignty



Cloud collaboration capabilities provide us seamless and secure connectivity across continents and break down language barriers with our colleagues across the globe. We've improved our ability to operate anytime, and anywhere and have increased our ability to securely communicate and coordinate especially during network outages and natural disasters."

— **Peter Guo**, Chief Information Officer at U.S. Naval Ship Repair Facility and Japan Regional Maintenance Center



In just a few months, Google Workspace helped us break down geographic silos and transform our workplace into a digital-first culture that is more secure, mobile-friendly, and efficient. Thanks to Google Workspace, we were well-positioned to overcome COVID-19 challenges — and continued to deliver secure, uninterrupted customer service in more than 50 countries throughout the pandemic."

— **Gene Molloy**, VP of IT End User Technology at Iron Mountain



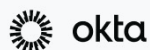
We have been searching for the capability to guarantee that our encrypted communications remain inaccessible to third -parties, including our technology providers, for some time. Google appears to be uniquely positioned with client-side encryption in providing us with complete control over our sensitive data, ensuring that we remain compliant as an organization in the ever-changing world of data regulation."

— **Shaun Bookham**, UK Operations & Technology Director at PWC



Our mission to transform credit underwriting with AI required intense global collaboration and rock-solid data security. We simply could not have succeeded without the data loss prevention tools and productivity enhancements of Google Workspace."

— **Rakesh Agrawal**, Produce & Technology Leader at Scienaptic



Transform the way work is done and securely unleash the full potential of your employees.

We're already seeing big changes in the way we all work. These changes, coupled with the increase in sensitive data being generated and stored, and generative AI becoming more pervasive in work settings, are raising security stakes. Much of this data is now stored in the cloud for easy access anywhere in the world. From there, it's shared with both internal and external collaborators who can then share it further.

All this is good for employee collaboration and productivity, but legacy collaboration suites aren't equipped to handle the security risks. Workspace is designed for security from the ground up.

[Get started today with Workspace](#), a more secure, private, and compliance-oriented collaboration suite that you can trust.



¹ Cost of a Data Breach Report 2023, IBM, 2023

² Coalition - "2023 Cyber Claims Report: Mid-year Update", 9/2023

³ https://www.cvedetails.com/product-list/vendor_id-1224/Google.html

⁴ "How we're helping to reshape the software supply chain ecosystem securely" Google Cloud Blog, 2021

⁵ Internal Google data. Google's Advanced Protection Program

⁶ At-Bay - "Ranking Email Security Solutions: A Data Analysis of Cyber Insurance Claims", 9/2023

⁷ Forrester, The Total Economic Impact™ Of Google Workspace, a commissioned study conducted by Forrester Consulting on behalf of Google, December 2023