Google Workspace

A more secure alternative

In the wake of significant cybersecurity incidents with Microsoft, Google Workspace offers a safer choice.

Contents

- Executive Summary 03
- Microsoft's pattern of security issues 04
  - How did Microsoft get breached?
  - Were these just accidents?
- A different, safer path with Google Workspace 06
  - A fundamentally different, more secure approach
  - A strong, security-focused culture
  - Deeply embedded zero trust controls for customers
- It's not just the technology; it's also the research & investment mindset 12
- Innovation that takes us to the future 13

Executive Summary

Microsoft's ongoing security struggles recently came to a head with a series of high-profile incidents that put its customers at risk. One such incident in the summer of 2023 by the group known as Storm-0558 resulted in the compromise of senior U.S. and U.K. government official accounts, including 22 organizations, over 500 individuals, and tens of thousands of emails. This prompted the Department of Homeland Security's Cyber Safety Review Board (CSRB) to issue a detailed report identifying the company's "cascade of security failures"[1] that led to the data breach. The details in this report speak to prolonged systemic issues and a "corporate culture that deprioritized both enterprise security investments and rigorous risk management."[2]

On the heels of the Storm-0558 compromise, CISA issued Emergency Directive ED 24-04 in response to a separate Microsoft data breach that occurred just a few months later in November of 2023: "state-sponsored cyber actor known as Midnight Blizzard has exfiltrated email correspondence between Federal Civilian Executive Branch (FCEB) agencies and Microsoft through a successful compromise of Microsoft corporate email accounts."[3]

The repeated security challenges with Microsoft call for a better alternative for enterprises and public-sector organizations alike. We believe Google Workspace is a safer alternative, with a proven track record of engineering excellence, deep investment in cutting-edge defenses, and a transparent culture that treats providing security for our customers as a profound responsibility.

This belief is rooted in battle-tested experience. We know that no organization is immune from highly sophisticated adversaries. In fact, these same nation state actors attacked Google in 2009, and those attacks led us to make far-reaching security improvements that were recognized in the CSRB report: "Google also undertook a comprehensive overhaul of its infrastructure security."[4]

In this whitepaper, we share some of the history of how our security strategy has evolved as well as more details about the controls and security benefits of using Google Workspace, including apps like Gmail, Google Drive, Slides, Docs, Meet, Chat and more.

Note: This white paper applies to Google Workspace products described at workspace.google.com. The content contained therein is current as of May 2024 and represents the status quo as of the time it was written. References to forthcoming features are annotated as such and do not constitute a commitment to a specific release schedule. Google's security policies and systems may change going forward, as we continually improve protection for our customers. The availability of the product features and capabilities described in this paper are subject to license availability of various Google Workspace editions product offerings.

Microsoft's pattern of **security issues**

How did Microsoft get breached?

In the summer of 2023, a state-sponsored adversary associated with the government of the People's Republic of China, known as Storm-0558, compromised Microsoft's environment and stole a signing key that "permitted Storm-0558 to gain full access to essentially any Exchange Online account anywhere in the world."[5] This breach resulted in unauthorized access to email accounts belonging to senior U.S. government officials working on matters of U.S. national security, including the State Department, Department of Commerce, House of Representatives, the U.S. Ambassador to the People's Republic of China, and 22 other organizations and 500 individuals across the world.

The signing keys that Storm-0558 obtained are "...used for secure authentication into remote systems, [and] are the cryptographic equivalent of crown jewels for any cloud service provider."[6] The keys are like those master keys that unlock all the rooms of a hotel. Once obtained, they can provide sweeping access. Because Microsoft allowed the same key to be trusted across different account types, it meant that a single compromise impacted consumer, enterprise, and government accounts alike. "As of the date of this report, Microsoft does not know how or when Storm-0558 obtained the signing key."[7]

As the CSRB remarked: "The loss of a signing key is a serious problem, but the loss of a signing key through unknown means is far more significant because it means that the victim company does not know how its systems were infiltrated and whether the relevant vulnerabilities have been closed off."[8] This incident represents one of the most consequential data breaches of a prominent cloud services provider to date. The CSRB referred to the event as the "espionage equivalent of gold."[9]

Just a few months later, in November 2023, another hacking group—a Russian state-sponsored adversary known as Midnight Blizzard—utilized a password spray attack to compromise Microsoft's corporate email accounts, including those of senior leaders, security, legal, and other teams.[10] This group gained access to email correspondence with U.S. government officials. In March 2024, Microsoft stated that the Midnight Blizzard attack that started in November 2023 was still ongoing five months later, without a reported timeline for resolution: "In recent weeks, we have seen evidence that Midnight Blizzard is using information initially exfiltrated from our corporate email systems to gain, or attempt to gain, unauthorized access. This has included access to some of the company's source code repositories and internal systems."[11]

Were these just accidents?

The severity of such attacks cannot be underestimated. Foreign adversaries with access to government communications and systems may have the ability to commit espionage or attack critical infrastructure in the event of geopolitical conflict, with potentially severe implications for governments and civilians.

Failure to prioritize security and risk management

In the case of the Storm-0558 compromise, the CSRB concluded that "this intrusion was preventable and should never have occurred"[12] citing "Microsoft's security culture was inadequate and requires an overhaul, particularly in light of the company's centrality in the technology ecosystem and the level of trust customers place in the company to protect their data and operations."[13]

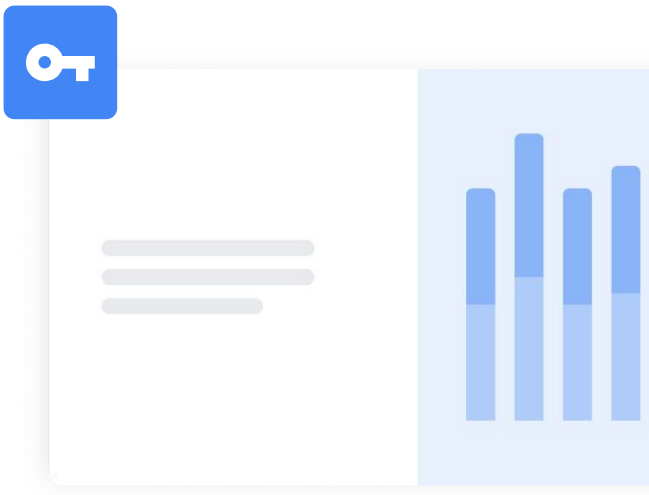
Failure to correct inaccurate public statements

The CSRB also noted significant concerns with Microsoft's handling of the incident, including a "decision not to correct, in a timely manner, its inaccurate public statements about this incident"[14] until "the Board was concluding its review and only after the Board's repeated questioning about Microsoft's plans to issue a correction."[15] As a result, "Microsoft's customers did not have essential facts needed to make their own risk assessments about the security of Microsoft cloud environments in the wake of this intrusion."[16]

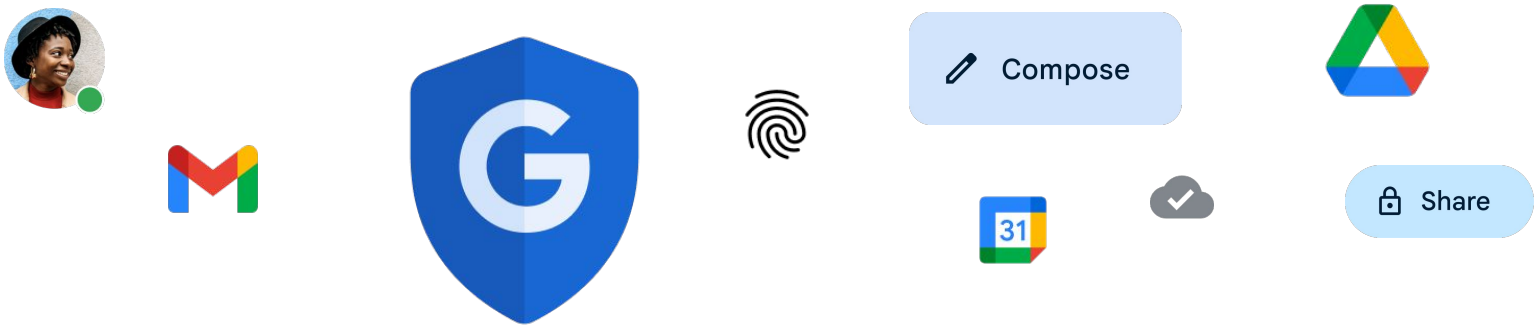
Failure to verify the means of key loss

In fact, it's uncertain whether Microsoft is able to prevent this type of incident from occurring again because the root cause has not been verified. "At the conclusion of the Board's review, even in the context of Microsoft's March 12 update, Microsoft has not identified a crash dump that contains the 2016 MSA key, or any other evidence of the key having been moved inappropriately."[17] Furthermore, "the Board assesses that Microsoft does not know how Storm-0558 obtained the 2016 MSA key."[18]

While no organization is immune to being the target of highly sophisticated adversaries, there is a clear pattern of evidence that suggests Microsoft is unable to keep their systems and therefore their customers' data safe.



A different, **safer path** with Google Workspace



A fundamentally different, **more secure approach**

Google Workspace is designed to support stringent privacy and security standards based on industry best practices:

- A cloud-first, browser-based approach that is constantly updated – no need for local devices, native apps, or email attachments.
- Built in controls, encryption, and verification with a Zero Trust approach that enables employees to work from anywhere and eliminates the need for VPNs.
- Operating on a global scale to protect your organization's information from phishing, malware, ransomware, and supply chain attacks – no add-ons required. Gmail blocks more than 99.9% of spam, phishing attempts, and malware from reaching your inbox. Gmail also detects two times more malware on average than third-party standard antivirus products alone.
- Making everyone safer with secure endpoints (company-provided or BYOD) that don't require patching and strong account takeover protections. — secure by design, secure by default.

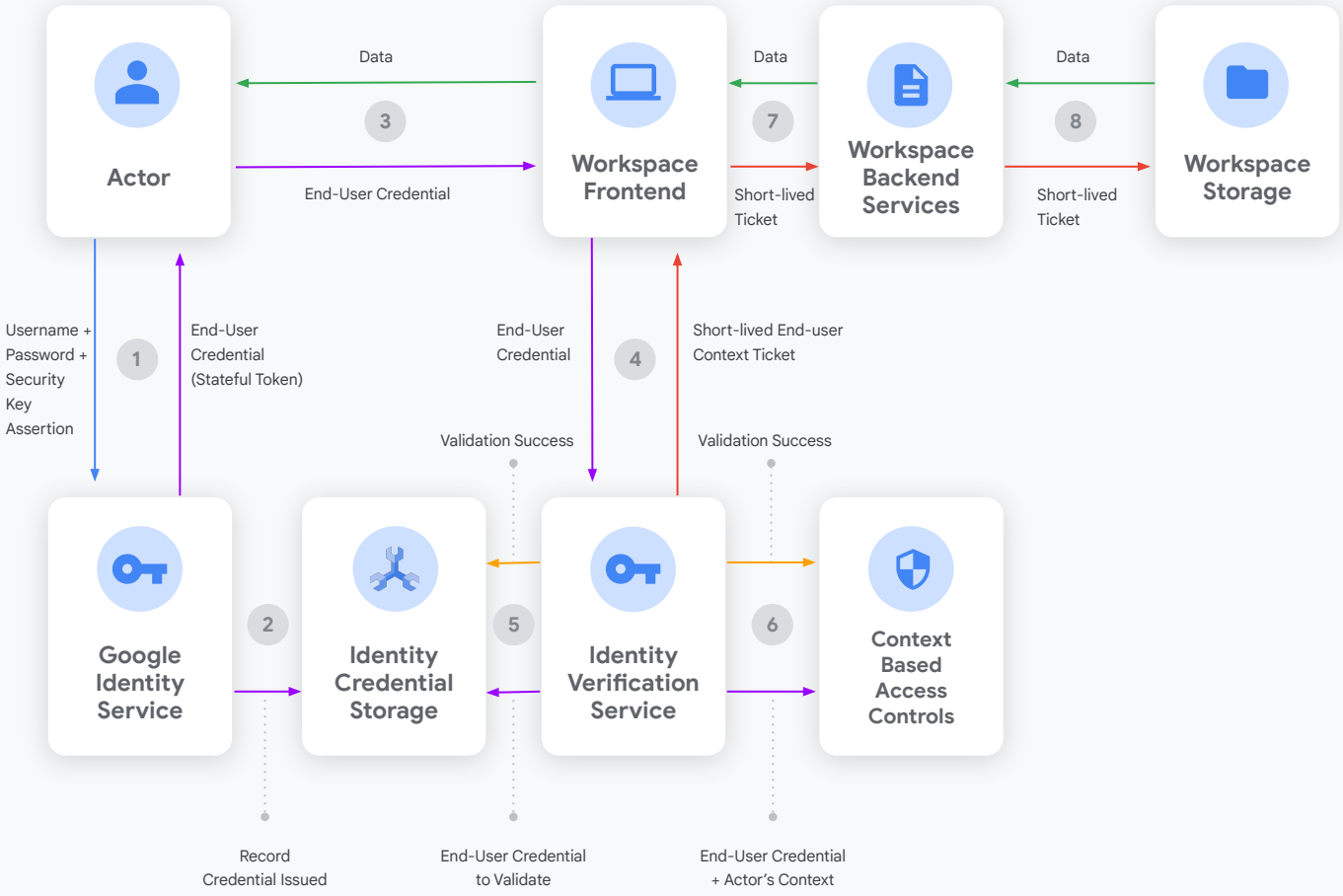
As an example of Google's differentiated approach to security, the CSRB report acknowledged the significant efforts we've taken over the over time to make our systems and products resilient to these types of attacks: "Google re-worked its identity system to rely as much as possible on stateful tokens, in which every credential is assigned a unique identifier at issuance and recorded in a database as irreversible proof that the credential Google receives is one that it had issued. Google also implemented fully automatic key rotation where possible and tightened the validation period for stateless tokens, reducing the window of time for threat actors to locate and obtain active keys. Google also undertook a comprehensive overhaul of its infrastructure security including implementing Zero Trust networks and hardware-backed, Fast IDentity Online (FIDO)-compliant two-factor authentication (2FA) to protect these identity systems."[19]

As the CSRB noted, Google leverages stateful tokens as much as possible. Expanding on this concept a bit further:

- The Google identity service verifies the user sign-in and then issues a user credential, such as a cookie or an OAuth token to the user's device. This credential is recorded in Google identity credential storage and considered stateful. Every subsequent request from the device to our infrastructure must present that user credential.
- When a service receives a user credential, the service passes the credential to the identity service for verification against the list of issued and valid credentials. If the user credential is verified, the identity service returns a short-lived user-context ticket that can be used for remote procedure calls (RPCs) related to the user's request. From that point on, for any cascading calls, the calling service can send the user-context ticket to the callee as a part of the RPC. Those tickets are only usable internally in the Google production environment.

Google's secure-by-design stateful identity tokens safeguard user accounts by preventing credential forgery. Even if cryptographic keys are compromised, they cannot be directly used by external attackers to access user data. Instead, the tokens are verified through a separate process that checks whether they were issued by Google before granting access to any user information.

Conceptual architectural flow of stateful tokens



The adoption of stateful tokens is not the only protection keeping our customers' data safe. Our Google infrastructure security design whitepaper describes, in detail, the security considerations made at each layer of our stack, from hardware to client, including physical security and employee controls. This includes BeyondProd, Google's approach to implementing zero trust principles in infrastructure—where trust depends on characteristics like code provenance, trusted hardware, and service identity, rather than the location in the production network, such as IP address or hostname. With BeyondProd, there is no inherent mutual trust between services, network edge protection isolates workloads from network attacks, and policy enforcement is consistent across services. We further describe our evolution toward this infrastructure model in our BeyondProd whitepaper.

A strong, **security-focused culture**

In 2009, Google was one of the targets of Operation Aurora, a China-backed series of cyberattacks that we link to the same Storm-0558 group that compromised Microsoft in the summer of 2023: "Industry links Storm-0558 to the 2009 Operation Aurora campaign that targeted over two dozen companies, including Google."[20]

The difference between the recent events impacting Microsoft and their customers and the compromise that impacted Google over a decade ago is that, based on our responsibility for keeping billions of people safe, we fundamentally changed how we think about cybersecurity.

> "Operation Aurora was a series of cyberattacks from China that targeted U.S. private sector companies in 2010. The threat actors conducted a phishing campaign that compromised the networks of Yahoo, Adobe, Dow Chemical, Morgan Stanley, Google, and more than two dozen other companies to steal their trade secrets. Google was the only company that confirmed it was a victim and disclosed to the public that the Gmail accounts of certain Chinese human rights activists had been compromised. Google also publicly attributed the incident to China, something companies were reluctant to do for fear of jeopardizing their access to the Chinese market. The incident is viewed as a milestone in the recent history of cyber operations because it raised the profile of cyber operations as a tool for industrial espionage. It led Google to cease its operations in China, though it continues to operate a localized version of its search engine in Hong Kong. As a result of the Gmail compromise, Google began notifying users if it believed their accounts had been targeted or compromised by a state-sponsored actor. This practice later spread to other email providers." [21]
>
> **Operation Aurora - Council on Foreign Relations**

In our blog Transparency in the shadowy world of cyber attacks, we shared our learnings that "Aurora not only taught us the need to embrace transparency, it also taught us a second, and even more important lesson: What works and what doesn't when it comes to security architecture."[22]

Our approach, which predates CSRB recommendations, enables customers, organizations, and governments to react promptly, reducing the window for exploitation by threat actors. This culture governs how we engage with customers, prioritize engineering decisions, and determine product investments.

Specifically, in this case, we launched an internal initiative called BeyondCorp, which pioneered the concept of zero trust and defense in depth and allowed every employee to work from untrusted networks without the use of a VPN. Today, organizations around the world are taking this same approach, shifting access controls from the network perimeter to the individual and the data.

Deeply embedded zero trust controls for customers

Taking the concepts of BeyondCorp a step further, Google Workspace enables customers to configure additional layers of data protection on top of the depth of controls implemented by Google.These protections were designed to closely align with the CISA Zero Trust Maturity Model and include:

Passkeys & security keys:

Combating user credential compromise, passkeys are a passwordless sign-in method that can offer a convenient and secure authentication experience across websites and apps, allowing users to sign in with a fingerprint, face recognition, or other screen-lock mechanism across phones, laptops, or desktops. Security keys provide hardware-based, phishing-resistant, two-factor authentication (2FA) to help protect high-value users.

Context-Aware Access (CAA) & BeyondCorp Enterprise (Chrome Enterprise):

Granular access control security policies for apps based on attributes, such as user identity, location, device security status, and IP address. With CAA, you control user access based on their context, such as whether their device complies with your IT policy.

Strong data controls:

Customers can benefit from tools like DLP and data classification to uniquely identify confidential information for their organization. Once the risk profile of the data has been established, customers can apply the appropriate controls (prevent sharing, downloads) that are required for their workforce.

We partner closely with CISA on their Secure Cloud Business Applications (SCuBA) project, which offers baseline configuration guides. To learn more about Google Workspace zero trust controls, we encourage you to review our Zero trust best practices guide for U.S. public sector agencies and the Google Workspace security and trust webpage.

It's not just the technology; it's also the **research** & **investment mindset**

Security is deeply ingrained in the fabric of our operations. Our dedicated security teams include some of the world's most prolific researchers in the areas of information and application security, cryptography, network security, and threat modeling. In adherence with leading standards, and in partnership with regulatory bodies and the scientific community, we develop internal processes that govern all aspects of how we work.

We have an enterprise-wide approach toward defending our systems and keeping our customers' data safe and secure. As an example, we leverage Chrome Enterprise controls and require all employees to use security keys for system access. Google invests significantly in the advancement of security, including a commitment to invest $10 billion over the next 5 years to strengthen cybersecurity, expand zero-trust programs, help secure the software supply chain, and enhance open-source security.

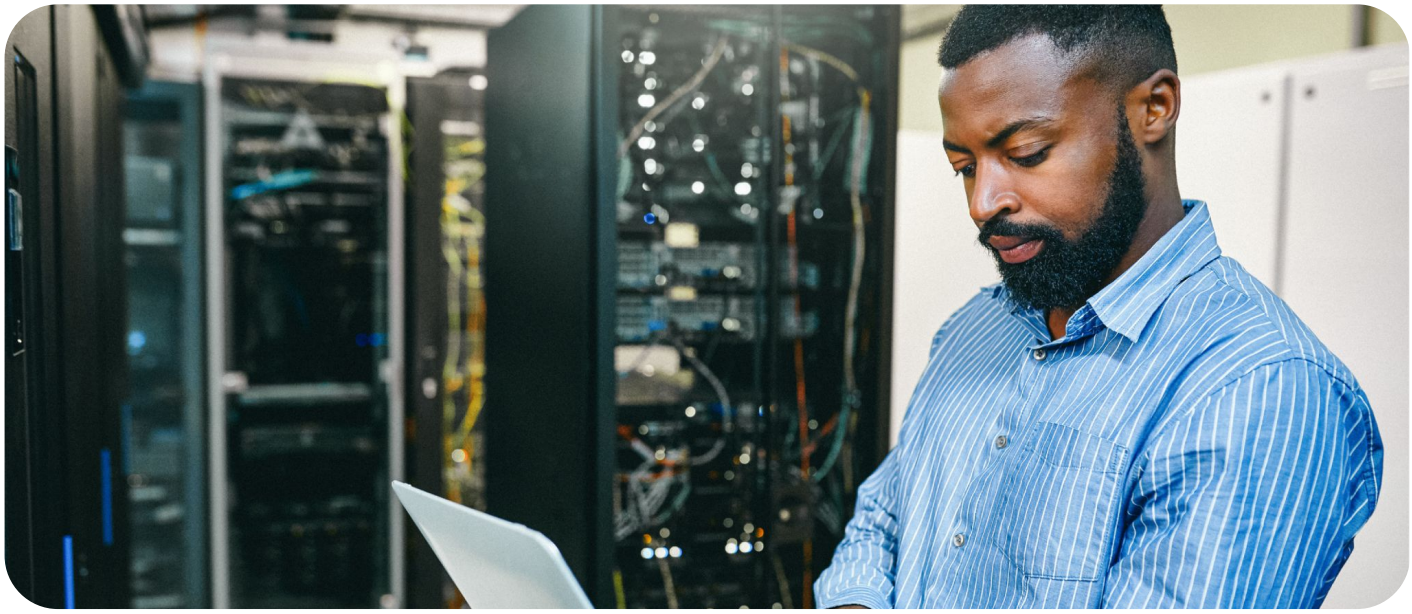
Our research:

Google Research supports numerous projects on security, privacy, and abuse prevention. The research includes publications, such as Building Secure and Reliable Systems,[23] Security by Design,[24] and Develop ecosystems for software safety.[25] Security researchers at Google also run Project Zero, a program dedicated to the study of zero-day vulnerabilities in hardware and software systems. Google's intelligence and security teams, including Google Cloud's Office of the CISO, Google's Threat Analysis Group, Mandiant, and various Google Cloud product teams, regularly publish their insights in Google's Threat Horizons Report.

Community engagement:

In addition to publishing our research for the collective benefit of the community, Google's Security Engineering team runs the Bug Hunter program that engages the external community in testing for vulnerabilities in Google systems. This program includes monetary rewards to incentivise community engagement. The Bug Hunter program Tsunami iis an open-source, general-purpose, network-security scanner with an extensible plug-in system for detecting high-severity vulnerabilities with high confidence. Tsunami is one of Google's many open-source security projects.

As we've noted, no organization is immune from being the target of highly sophisticated and unrelenting adversaries. In the more than 14 years since Project Aurora, we have conducted an overhaul of the fundamental architecture of our platforms, our defense-in-depth approach, and our culture around core security principles in efforts to protect our internal systems and customers from such compromises.



Innovation that takes us to the **future**

As noted above, several of CSRB's recommendations are already a core part of Google's approach to security. In addition, Google proactively addresses issues that the industry is facing at large and strives to provide industry-first solutions to the ever-evolving security challenges. Noted below are a couple of examples:

Device-bound session controls:

To substantially reduce the impact of cookie theft, Google has announced a new open standard to cryptographically bind web sessions to device hardware. By binding authentication sessions to the device, device bound session controls disrupt the cookie theft industry because exfiltrating these cookies will no longer have any value.

Innovations in AI:

Today, Gmail's advanced AI protections already block more than 99.9% of spam, phishing attempts, and malware from reaching your inbox. With the use of large language models, we've further reduced spam in Gmail by an additional 20% and can evaluate 1,000 times more user-reported spam in Gmail every day. Recently, we brought the power of large language models to classify documents through AI classification, which enables customers to use custom, privacy-preserving models to identify and protect sensitive data. We'll continue to infuse new layers of AI defenses into our products, with cutting edge technologies to better protect our customers.

How Google Workspace can help

We continue to be laser focused on keeping our customers safe and providing safer alternatives for work. To discover how you can provide your organization with a more secure way to work, please speak with your customer representative or start here.

Appendix: Footnotes

Footnotes Number	Source
1	CSRB, Review of the Summer 2023 Microsoft Exchange Online Intrusion, ii, (CSRB, 2024).
2	Ibid., iv
3	CISA, ED 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System, (CISA, 2024).
4	CSRB, Review of the Summer 2023 Microsoft Exchange Online Intrusion, Page 20, (CSRB, 2024)
5	Ibid., iii
6	Ibid., iii
7	Ibid., iii
8	Ibid., 18
9	Ibid., ii
10	CISA, ED 24-02
11	Microsoft Security Response Center, Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard, (Microsoft, 2024).
12	CSRB, Review of the Summer 2023 Microsoft Exchange Online Intrusion, Page iii, (CSRB, 2024)
13	Ibid., iii
14	Ibid., iii
15	Ibid., iii
17	Ibid., 16
18	Ibid., 5
19	Ibid., 20
20	Ibid., iii
21	Council on Foreign Relations, Operation Aurora, (Council on Foreign Relations, 2010)
22	Kent Walker, Transparency in the shadowy world of cyberattacks, (Google, 2022)
23	Heather Adkins, Betsy Beyer, Paul Blankinship, Ana Oprea, Piotr Lewandowski, Adam Stubblefield, Building Secure and Reliable Systems, (O'Reilly Media, 2020)
24	Christoph Kern, Secure by Design at Google (Google, 2024)
25	Christoph Kern, Developer Ecosystems for Software Safety (Google, Feb. 2024)