

# The Free Cybersecurity Tools Hidden in Google Workspace

Google's concentration on cybersecurity can give your business a strong front line against cyberthreats



**GREG OTTO**

Sr. Security Writer

[at-bay.com](https://at-bay.com)



# Table of Contents

---

Introduction	3
Gmail Malware Scanning	4
Google Security Checkup	6
Advanced Protection Program	8
Enhance with Stance	10

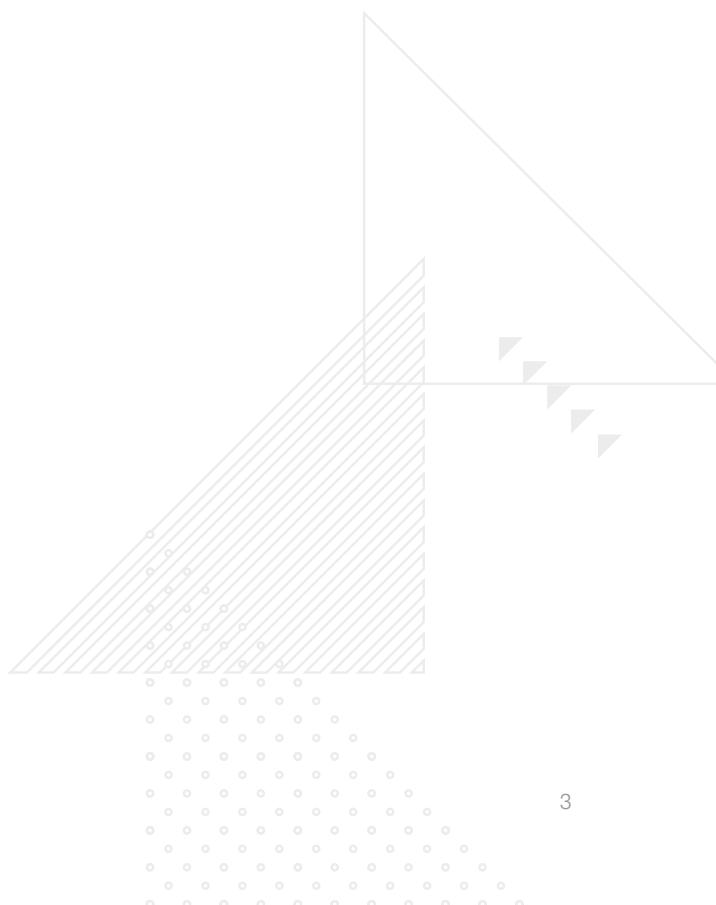
---

# Introduction

Businesses often face an uphill battle when creating a robust cybersecurity posture. The powerful tools that large enterprises wield can be effective; however, they are beyond the reach of many businesses due to the steep costs and need for continuous oversight by a specialized team.

Yet, there are ways businesses can improve their posture by using features in the software platforms they already own. Google Workspace, [which has more than 3 billion users](#), includes a wide range of free security features within its core products. For business owners and IT specialists looking to bolster their defenses, learning how to use these built-in tools could be a cost-effective way to enhance their security posture and avoid a harmful cybersecurity incident.

From Gmail's multi-layered malware scanning to the Security Checkup feature that audits your account's safety, here's how the security features in Google Workspace can help ensure that your company's communications and data remain uncompromised.



---

# Gmail Malware Scanning

By default, Gmail's malware scanning process employs a combination of machine learning, signature-based detection, and behavior analysis to identify and block malware. Here's what that means:

- ➔ **Signature-Based Detection:** Google compares files in your inbox against a vast database of known malware signatures — unique strings of data or characteristics of known malicious software. If the signatures are a match, Gmail flags the content as dangerous.
- ➔ **Heuristic Analysis:** Heuristics are like signatures, but focused on how software behaves. Gmail analyzes email attachments for traits common to known malware or unusual activity that could signify a new, unknown malware. For instance, executable files (computer files that run a program when you click on them) are often scrutinized more closely because they contain code that can launch potentially harmful programs.
- ➔ **Machine Learning:** Over time, Gmail has improved its filtering and detection systems, learning from prior scans and user feedback. This continuous learning helps Gmail recognize evolving malware threats.
- ➔ **Sandboxing:** Gmail uses an advanced technique called sandboxing for high-risk attachments. Sandboxing involves opening the attachment in a secure, isolated environment within Google's servers to monitor its behavior. This process helps to identify harmful actions such as downloading malware or connecting to suspicious servers.

## Attachment Restrictions

Gmail blocks certain files that are commonly used to deliver malware, including:

- Executable files (.exe, .dll, etc.)
- Scripts (.bat, .cmd, etc.)
- Archive files that may contain harmful content (.zip or .tar.gz files with password protection or that contain a compressed executable)

When a potentially dangerous attachment is detected, Gmail prevents the user from downloading it to reduce the risk of infection. Users are notified with a warning message explaining why the file was blocked for safety purposes.

## Safe Browsing Integration

Gmail's security checks are integrated with Google's Safe Browsing technology, which identifies unsafe website addresses. If a message contains a link known to lead to malicious websites, Gmail will display a warning or prevent the message from being received.



---

# Google Security Checkup

Google's Security Checkup allows users to check the security integrity of Google accounts, including associated services like Gmail, Google Drive, and other applications within the Google Workspace. The process is user friendly and provides actionable recommendations to enhance account security. (We cover how to start a security checkup below.)

## What is Covered in a Google Security Checkup?

Gmail's security checks are integrated with Google's Safe Browsing technology, which identifies unsafe website addresses. If a message contains a link known to lead to malicious websites

- **Recent Security Events:** This section allows you to see all security-related changes to your profile, so you can quickly verify the ones you authorized and identify the ones you didn't.
- **Third-Party Access:** Google lists all external applications and services that have access to your account. This can include apps that you have given permission to view your Google Drive, use your Gmail, or interact with other aspects of your Google Workspace. It provides an opportunity to review these permissions and revoke access to applications that are no longer used or needed, or that appear suspicious.
- **Your Devices:** The checkup shows a list of devices that have accessed your Google account, helping to verify that all of them belong to your company or have been used by authorized personnel. If you spot a device you don't recognize, you can secure your account by changing your password and signing out of that device.
- **Sign-In and Recovery:** This section prompts you to update recovery information, such as phone numbers and backup email addresses. Accurate and current recovery information is crucial for reacquiring access to your account in case of a forgotten password or a lockout, as well as for receiving critical security alerts.



**Multi-Factor Authentication (MFA):** The Security Checkup assesses the status of MFA settings for your account. You may be urged to set up or update MFA settings using methods like text message codes, authentication apps, or backup codes.

## How to Conduct a Security Checkup

Follow these simple steps to start the Security Checkup process:

- 1 Go to the Google Account page ([myaccount.google.com](https://myaccount.google.com)).
- 2 Click on the 'Security' tab on the left-hand side.
- 3 Look for the "Security Checkup" section, and click 'Get Started' to begin the guided process digit code, or ask for biometric confirmation (like a fingerprint or face recognition).




A best practice would be to set up a routine (e.g., monthly or quarterly) checkup on all business-related Google accounts. Regular reviews are essential as permissions and account settings can change over time. Train your team on the importance of these checks. Ensure that they are familiar with the process, the kinds of issues they're looking for, and how to address them.

# Advanced Protection Program

Google's Advanced Protection Program (APP) is the company's strongest security offering for users at a higher risk of targeted online attacks. Small business owners, IT specialists, and individuals with significant business or personal data online can benefit from the additional layers of security provided by APP. The program is built to defend against phishing and account hijacking, and it provides extra protection for the data stored in Google services.

## Advanced Protection Program Features

Let's break down the key elements of the Advanced Protection Program that enhance your account's security posture:

-  **Stronger Account Verification:** Google mandates the use of physical security keys for account access under the program. These keys are small physical devices that conform to universal standards ([FIDO](#)) and are used as part of the multi-factor authentication (MFA) process. They communicate with the computer or mobile device in a variety of ways (USB, NFC, or Bluetooth), requiring users to physically tap the key in response to a prompt when signing in.
-  **Restricted Third-Party Access:** To prevent unauthorized access through connected applications, APP severely limits which third-party apps can access your Google account data. Only Google apps and selected third-party apps that meet Google's security standards can access sensitive Gmail and Drive data. This means a reduced risk of data being siphoned off by potentially compromised third-party apps and a smaller surface area for criminals to launch attacks.
-  **Enhanced Scanning for Email Threats:** The program's subscribers benefit from Google's most stringent email scanning protocols. Gmail will automatically perform additional checks to block phishing attempts, and prevent malicious content and untrusted attachments from reaching the inbox.



## How to use Google's Advanced Protection Program

To safeguard your sensitive information, follow these steps to use Google's Advanced Protection Program effectively:

### Enrollment

- ➔ **Acquire Security Keys:** Users must first obtain two FIDO-compliant security keys. One will serve as the primary key, and the other acts as a backup. Google [makes their own](#), but there are [many other options](#).
- ➔ **Enroll in the Program:** Visit [Google's Advanced Protection landing page](#) and sign in with the Google account you want to protect. Follow the directions on screen, during which you will register your security keys.

### Post-Enrollment Adjustments

- ➔ **Review Device Access and Third-Party Apps:** Inspect the generated list and make sure that all devices and third-party applications accessing the Google account are known and trusted. You can remove those that are unknown, unnecessary, or not compliant with company rules and regulations with one click.
- ➔ **Integrate With Business Infrastructure:** Determine from your Admin console if you want this program to work alongside any other security measures, software, or systems already in place.

Cybersecurity can seem daunting and costly, but it doesn't have to be. Google Workspace comes with a robust array of security features that protect at no additional cost. These free tools are designed to seamlessly integrate into your everyday workflow, providing powerful defenses while keeping simplicity and accessibility front and center.

---

# Enhance With Stance

The tools and services above offer a solid way to strengthen your Google Workspace. However, cyberthreats evolve rapidly, making it challenging for any business to stay ahead of cybercriminals. This is where the At-Bay Stance™ Exposure Manager steps in. With two clicks, it can be integrated into your Google Workspace and keep an eye on vulnerabilities so you can focus on your business. Based on claims data from our policyholders, Stance informs companies what security controls matter the most and which actions can reduce the risk of attacks.

Stance Exposure Manager is a key part of [InsurSec](#), which combines top-notch cybersecurity tools with insurance protection. The digital platform scans for new security risks throughout the life of your At-Bay insurance policy and alerts you when action is needed. With this tool, you'll be well-informed about when and how to tackle security issues, and you can reach out to cybersecurity experts whenever you need extra assistance.

Our Stance integration with Google Workspace isn't just an extra piece of InsurSec — it's a key part of a full defense plan. By using this integration alongside Google's built-in security tools discussed above, you can have a cybersecurity plan that won't slow down your business.

**Already an At-Bay Stance Exposure Manager user?** Learn more about how the Google Workspace integration in [At-Bay Stance Exposure Manager](#) can supercharge your cybersecurity strategy.

**Not yet using Stance Exposure Manager?** Now's the perfect time to start. Get unprecedented visibility into your cybersecurity posture, where your business is vulnerable, and what to do. To learn more, contact our [Stance Advisory Services team](#) or send us an email at [security@at-bay.com](mailto:security@at-bay.com).

at  
— bay