frogworks

March 2026

Issue 03 Volume 16

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

Google Meet Questions Now Come With Gemini Answers

Google is once again reshaping how teams meet and collaborate. If you use Google Workspace, you've probably noticed how AI has quietly slipped into your everyday tools.

The latest update? Google Meet Gemini answers. This AI-powered tool is now making its way into your video calls, adding a new layer of automation that could change the way we handle meetings.

What Is "Ask Gemini in Meet"?

Google Meet is rolling out an AI assistant that acts like a real-time note-taker, meeting recap tool, and Q&A buddy all in one. The feature, called Ask Gemini in Meet, enables participants to ask questions during a call and receive instant, AI-generated answers without disrupting the conversation flow.

Here's what it can do:

- Summarize discussions in real time
- Identify key takeaways, decisions, and action items
- Recap what was just said if you zoned out or got distracted

This takes traditional meeting transcripts a step further, creating bite-sized insights that you can actually use, rather than long walls of text.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Google Meet Questions Now Come With Gemini Answers

Are Real-Time Summaries Helpful or a Shortcut?

One of the headline features is the creation of real-time summaries. If someone joins late, Gemini can quickly catch them up, assuming they turned on "Take Notes for Me" beforehand. This means no more latecomers interrupting meetings with, "Sorry, what did I miss?"

This, of course, begs the question of whether it will make employees more or less engaged. Some experts predict that with Google Meet, Gemini answers, which provide automated meeting recaps using meeting captions and other Workspace resources, as well as publicly available online information, some participants may ultimately tune out, trusting the assistant to capture the important details.

Workspace Integration That Saves (Some) Time

This isn't just another add-on; it's deeply integrated into Google Workspace. Because Gemini integrates with other productivity tools, the decisions or action items identified in Meet can easily transfer to Docs, Tasks, or even your email follow-ups.

In practice, this could enable automated delegation, thereby reducing the manual effort required for assigning follow-up tasks. However, as with any AI tool, its effectiveness depends on how well your team communicates in the first place.

Automated Responses and the Future of Meetings

The addition of automated responses to Google Meets erodes the distinction between active participation and passive listening. Imagine asking, "What were the three main decisions made today?" and getting a concise recap without needing to scroll through a transcript or rewatch the recording.

For leaders managing multiple teams, this could mean less wasted time and more focused decision-making.

Start Using AI in Google Meetings Today

The arrival of Google Meet Gemini answers is less about replacing human attention and more about shifting how attention is used. Instead of scrambling to take notes or worrying about missing something, employees can focus on the bigger picture with the help of AI assistants, real-time summaries, and productivity tools like these.

Currently, Google Meet Gemini answers are only available for English-language meetings on the desktop Workspace. It's also worth noting that all answers and interactions are individual and private to each user and not stored after the meeting ends.

Understanding Zero-Day Vulnerabilities

Procuring new software, applications, or devices for your business is always exciting. You and your team will be rearing to take advantage of all those features. Still, you have to know that they're secure.

Is there a chance your new installation contains a hidden flaw no one knows about, not even the people who built it? One glitch could allow hackers to easily breach your security defenses. That's the reality of zero-day vulnerabilities, and they're more common than you might expect.

A business owner needs to know what these vulnerabilities are so that you know what to do to close them. It could make all the difference between a secure company environment and a data breach catastrophe!

What Are Zero-Day Vulnerabilities?

A zero-day vulnerability, also called a zero-day exploit, is a security flaw that the vendor didn't know about before they released a product. The term "zero-day" means that developers haven't had any time to address the issue or release a security patch. It's an undisclosed vulnerability because it is completely unknown to the product creator.

Surprisingly, these vulnerabilities can remain undetected for a while. Occasionally, security researchers (or hackers) stumble across them by accident. At other times, cybercriminals actively look for them.

Unfortunately, if hackers get there first, they'll use zero-day vulnerabilities to:

- Steal data
- Install malware
- Hijack systems or networks
- Bypass existing security tools

If this happens, no patch or update can stop the fallout because no one even knows the vulnerability exists yet, let alone how to fix it.

Why Zero-Day Exploits Should Be on Every Business Owner's Radar

Regardless of the size of your company or industry, zero-day vulnerabilities are a threat if you use digital tools. Even seemingly "safe" gear, including routers, point-of-sale systems, smartphones, and office software, can harbor hidden flaws. Your business must outsmart them, or you'll end up with a mess on your hands, from system downtime to data breaches.

Understanding Zero-Day Vulnerabilities

How To Protect Your Business From Zero-Day Threats

You can't stop a zero-day vulnerability because you don't know it's there. However, you can make such vulnerabilities much harder to exploit by doing the following:

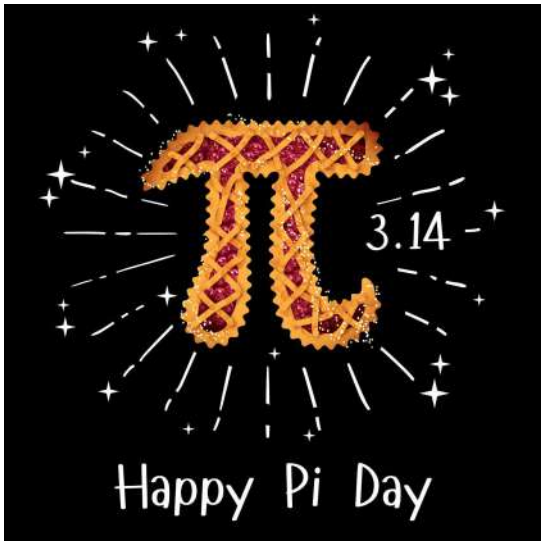
- Stay updated: Software patching addresses known vulnerabilities in hardware and software. Stay alert to update notices and immediately install them.
- Use layered security: Firewalls, antivirus tools, and advanced threat detection provide extra protection against hackers and prevent unauthorized access.
- Train your team: Many cyberattacks begin with human error, like clicking a malicious link. Training your people to detect phishing and other security-based concerns supports zero-day mitigation.
- Restrict access: Only provide employees with the access and privileges required for their specific duties. Fewer entry points mean fewer opportunities for hackers.

You could also partner with professionals. For example, managed IT and cybersecurity providers use threat intelligence to watch for suspicious activity and respond quickly.

Stay Ahead of the Unknown

Zero-day vulnerabilities can lurk in the tools your business uses every day. While you can't see them coming, you can build stout defenses.

Make it harder for attackers to succeed.



We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter