TECHNICAL FRAMEWORK
IT SOLUTIONS FOR BUSINESS

(970) 372-4940
info@techframework.com
https://techframework.com

Season’s greetings and best wishes in 2026 from Technical Framework!

CYBERSECURITY

Catch Hackers Red-Handed with Canary Files

Most cybersecurity failures are not caused by missing tools. They happen because organizations discover problems too late. By the time ransomware appears, data has already been copied. By the time a suspicious login is noticed, the attacker has already explored the environment.

Traditional security focuses heavily on prevention: firewalls, antivirus software, and patching. Those controls matter, but none of them tell you when someone is already inside and looking around. That gap is where canary files shine.

scanning shared drives, curious insiders accessing sensitive areas, and hackers exploring systems after initial entry.

They do not block attacks. They expose them early.

HOW CANARY FILES WORK

A canary file either phones home using an embedded token and sends an alert, or it triggers an audit log event that you monitor.

THE EASIEST METHOD: CANARY TOKENS

Canary files are intentionally simple. Their purpose is not to stop an attack, but to expose unauthorized access the moment it occurs. For small and mid-sized businesses without full-time security staff, that clarity is critical. There is no interpretation or debate required. If a canary file is accessed, something is wrong.

This makes canary files especially valuable for novice business owners. They are low-cost, require minimal setup, and generate almost no noise. More importantly, they produce high-confidence alerts. A canary file should never be opened during normal business operations. If it is accessed, you treat it as an incident and respond immediately.

WHAT IS A CANARY FILE?

A canary file is a fake but believable file placed where no legitimate user should open it. If the file is accessed, you assume improper access and investigate immediately.
There are no false positives by design.

WHAT CAN CANARY FILES DETECT?

Canary files are effective at catching stolen or compromised user accounts, malware

A canary token is a small invisible beacon embedded into a file. When the file is opened, the beacon makes a network request and sends you an alert.

STEP-BY-STEP CREATION

1. Generate a canary file using a canary token service.
2. Rename the file realistically (Payroll_2025.xlsx, Vendor_Wire_Instructions.pdf).
3. Place it where no legitimate user would open it.
4. Test the alert.

ALTERNATIVE: WINDOWS FILE AUDITING

Create a fake file, enable NTFS auditing, enable File System auditing in Group Policy, and monitor Event ID 4663.

CLOUD STORAGE

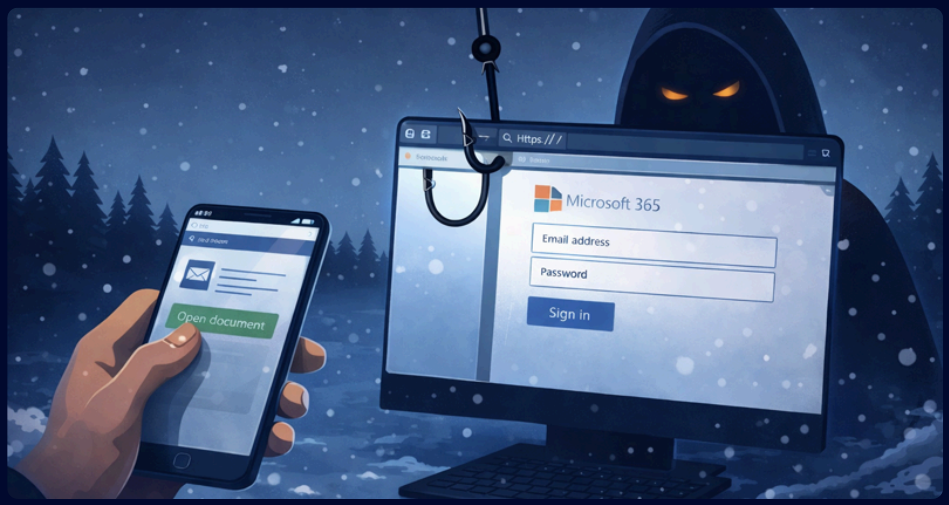
Upload a fake file to SharePoint or OneDrive and create alerts for file access.

WHEN A CANARY FIRES

Disable the account, revoke sessions, isolate the device, and preserve logs immediately.

WHY THIS WORKS

Canary files provide early detection with near-zero noise and clear proof of improper access.



CYBERSECURITY

Clicking the Link Isn’t the Mistake — Trusting the Page Is

Most cybersecurity advice tells people “don’t click links.” That advice is outdated. Modern phishing attacks succeed even when people click carefully. The real mistake is trusting what loads after the click.

Today’s phishing attacks are no longer crude emails with obvious spelling errors. They use real branding, correct language, and familiar services like Microsoft 365, Google, DocuSign, or Dropbox.

The email looks normal. The link looks normal. The page looks real. That is why they work.

HOW MODERN PHISHING ACTUALLY WORKS

A modern phishing attack usually follows this pattern:

1. An email arrives claiming to be a shared document, invoice, voicemail, or security alert.

2. The link points to a fake login page designed to look identical to a real service.

3. The victim enters their email address and password.

4. The page may redirect to the real service, making the login appear to “fail” or “succeed.”

5. The attacker now has valid credentials.

No malware is installed. Antivirus software does not detect anything. The attacker simply logs in as the user.

WHY CAREFUL USERS STILL FALL FOR IT

Even cautious employees get tricked because:

• The page looks exactly like Microsoft or Google
• The email references real coworkers or files
• The login prompt appears after clicking a legitimate-looking link
• The browser shows a lock icon, which only means encryption, not legitimacy

THE ROLE OF PASSWORD MANAGERS

Password managers are one of the most effective phishing defenses.

They work because:

• They only auto-fill credentials on the correct website
• They do not rely on visual appearance
• They recognize subtle domain differences humans miss

If a login page looks real but your password manager does not offer to fill in the password, that is a strong warning sign.

WHAT BUSINESSES SHOULD TRAIN EMPLOYEES TO DO

Instead of “don’t click links,” teach this:

• Be suspicious of login prompts reached through email.
• If asked to log in, open a new browser tab and go directly to the service.
• Never re-enter passwords from email links.
• Use the password manager as a trust signal.

TECHNICAL CONTROLS THAT HELP

Businesses can reduce risk by:

• Enforcing multi-factor authentication (MFA), meaning a second proof like a phone app or hardware key
• Restricting logins from new locations or devices
• Alerting on unusual login behavior
• Blocking legacy authentication methods that bypass MFA

WHY THIS MATTERS
Small businesses are targeted because they have fewer security layers, trust familiar brands, and move quickly under pressure.

THE TAKEAWAY
Clicking a link is no longer the core risk. Trusting a fake login page is.

ARTIFICIAL INTELLIGENCE

AI That Can “See” Without Recording Video — And How It Actually Works

Modern artificial intelligence is changing how machines interpret visual data.

Traditionally, video surveillance required storing footage on disk or in the cloud, which raises privacy concerns and storage costs. A new category of AI solutions can analyze live video streams in real time without persisting recorded video, offering actionable insights without retaining sensitive imagery.

WHAT “AI VISION WITHOUT RECORDING” MEANS

Instead of recording video and analyzing it later, these systems process camera feeds in real time and extract only metadata or alerts—such as “person entered restricted area” or “object left unattended”—while discarding visual data immediately.

This separates detection from storage and reduces privacy risk.

HOW IT WORKS

1. A camera feed is processed live.
2. AI models analyze frames in real time.
3. Events or patterns are identified.
4. Raw video frames are discarded.
5. Alerts or metadata are stored or sent.

REAL COMPANIES DOING THIS

Ambient.ai

Ambient.ai analyzes live camera feeds to detect behavior, movement

Verkada

Verkada cameras perform on-device processing. Only events and metadata are sent to the cloud, and privacy zones can exclude sensitive areas from analysis.

AnyVision (Genetec)

AnyVision provides real-time computer vision analytics designed to detect presence and movement without unnecessary video retention, often deployed on-premises.

Google Cloud Video Intelligence

Google’s Video Intelligence tools can analyze video streams and return structured insights without requiring long-term video storage when used in streaming or edge scenarios.

PRACTICAL USE CASES

- Workplace safety monitoring
- Retail traffic and dwell analysis
- Manufacturing line observation
- Security alerts without video archives

WHY THIS MATTERS

- Reduced privacy exposure
- Lower storage and bandwidth costs
- Faster real-time response
- Smaller breach impact

THE TAKEAWAY

AI systems no longer need to record everything to understand what is happening.

patterns, and security events. It focuses on real-time alerts and analytics rather than storing full video archives.

By analyzing live video and keeping only structured events, businesses gain awareness without long-term video retention.

CYBERSECURITY

Backups Fail More Often Than You Think

Most businesses believe they are protected because they “have backups.” That confidence is often misplaced.

Backups fail quietly, and many organizations discover the problem only during an emergency—ransomware, accidental deletion, or hardware failure—when recovery actually matters.

The issue is not bad intentions or neglect. It is misunderstanding what backups do, how they fail, and what “working” really means.

BACKUP DOES NOT EQUAL RECOVERY

A backup is a copy of data. Recovery is the ability to restore usable data within an acceptable time.

Many backups technically exist but still fail recovery because:

• The data is corrupted.
• The backup never completed.
• The restore process was never tested.
• The system being restored no longer matches the backup.
• Access credentials are missing or expired.

If you have never restored from a backup, you do not know if it works.

2. Backups overwrite good data with bad data

Automatic backups can overwrite clean data with encrypted or corrupted versions after ransomware or mistakes.

3. Restores are too slow

Backups may technically work but restoring systems can take days, not hours, causing unacceptable downtime.

4. Attackers can reach backups

If backups are accessible on the same network or with shared credentials, ransomware can destroy them too.

WHAT ACTUALLY WORKS

The 3-2-1 rule:
• Three copies of data
• Two different storage types
• One copy kept offsite

Immutable backups:

Backups that cannot be changed or deleted for a set period protect against ransomware and accidents.

Monitoring:
Confirm backups complete successfully and alert someone who will act.

COMMON REASONS BACKUPS FAIL

1. Backups stop running

Backup jobs fail for ordinary reasons such as storage filling up, expired credentials, software updates breaking agents, or network changes.

Without monitoring, failures go unnoticed.

Testing restores:
Restore files quarterly and test full recovery annually.

Recovery expectations:
Define acceptable data loss and downtime. If backups cannot meet these goals, they are insufficient.

THE TAKEAWAY

A backup that exists is not enough. A backup that has been restored successfully is what matters.

ARTIFICIAL INTELLIGENCE

AI That Remembers Everything You Forget — And How It Actually Works

Most work problems are not caused by a lack of intelligence or effort. They are caused by lost context.

Decisions get made in meetings, follow-ups disappear in email, and important details fade as people switch between tasks.

A new generation of AI tools is addressing this problem by doing something traditional software never did well: remembering context over time.

This is often called “AI memory,” but it does not mean human-like memory. It means systems that retain selected information from past interactions and reuse it later in a controlled way.

WHAT “AI MEMORY” REALLY MEANS

Most software is stateless. Every interaction starts fresh. AI memory systems change that by storing

Microsoft Copilot (Microsoft 365)

Copilot uses organizational context rather than personal memory.

How it works:
• Pulls data from emails, calendars, documents, and Teams
• Uses Microsoft Graph as the data layer
• Respects existing permissions

Copilot does not store conversations as memory.

Claude for Teams & Enterprise (Anthropic)

Claude provides workspace-level memory for team environments.

How it works:
• Context persists across conversations
• Memory is scoped to the organization
• Controlled by administrators

structured summaries of past interactions, not raw conversations.

They typically remember:

• User preferences
• Ongoing projects
• Prior instructions
• Important decisions or constraints

They do not remember everything. They remember what is flagged as useful.

REAL TOOLS DOING THIS TODAY

ChatGPT (OpenAI)

ChatGPT includes an optional Memory feature. When enabled, it stores short, editable memory entries such as user preferences, ongoing projects, and communication style.

How it works:
• Key facts are extracted
• Stored separately from chat history
• Used to guide future responses

Users can view, edit, or delete memory at any time.

Google NotebookLM (Google)

NotebookLM remembers documents, not people.

How it works:
• Users upload source materials
• AI maintains long-context awareness
• Answers stay grounded in provided content

WHAT THIS IS NOT
AI memory does not mean permanent recording, surveillance, or independent decision-making. Memory is selective and permission-based.

WHY THIS MATTERS
AI memory reduces repetition, lost decisions, and context rebuilding. It improves continuity, speed, and consistency.

THE TAKEAWAY
AI is moving from answering questions to continuing work. The most useful AI systems remember just enough to keep work moving forward without getting in the way.

CYBERSECURITY

The 2025 SonicWall Nation-State Hack: What Happened and What It Means

In 2025, SonicWall—a major provider of firewalls and network security appliances—was targeted by a state-sponsored hacking group that infiltrated its cloud backup service. This incident drew attention not because SonicWall products failed in the field, but because attackers targeted the cloud systems used to manage and back up firewall configurations.

On September 17, 2025, SonicWall disclosed unauthorized access to its MySonicWall cloud portal. This portal is used by customers to store firewall configuration backup files. These backups contain firewall rules, routing information, and encrypted credentials that define how a network is protected.

Initially, SonicWall reported that fewer than 5 percent of customers were affected. As the investigation continued, the company later confirmed that all customers who had used the cloud-based configuration backup feature had their backup files accessed.

HOW THE ATTACK WORKED

According to SonicWall and its incident response partner Mandiant, the attackers abused an application programming interface, or API, to gain access to the backup environment. An API is a mechanism that allows different software systems to communicate. In this case, it was misused to retrieve stored configuration files.

SonicWall stated that the attackers did not compromise firewall firmware, customer networks, or SonicWall's core production systems. The breach was limited to the cloud backup service.
However, firewall configuration files are sensitive. Even when credentials are encrypted, configuration details can reveal network design, security rules, and trusted connections. This information can help attackers plan future, more targeted attacks.

NATION-STATE ATTRIBUTION

In November 2025, SonicWall confirmed that the breach was attributed to a nation-state threat actor. While no specific country was named, nation-state attacks typically involve advanced techniques and long-term objectives rather than immediate financial gain.

WHY THIS MATTERS FOR BUSINESSES

This incident highlighted several practical risks:
• Cloud management portals are high-value targets.
• Configuration backups can be as sensitive as passwords.
• Security vendors are not immune from attack.
• Stolen data may be used months or years later.

SonicWall advised customers to reset credentials, regenerate access tokens, and review firewall configurations as a precaution.

THE TAKEAWAY

The 2025 SonicWall breach was not a failure of firewall hardware, but a reminder that supporting cloud services must be protected just as carefully. Businesses should treat configuration backups as sensitive assets and regularly review vendor security practices.
Even security tools require layered protection.

CYBERSECURITY

What RAM Is, How Your Computer Uses It, and Why Prices Are Rising

Most people hear "RAM" when buying a computer, but few understand what it actually does. RAM is not storage, it is not a hard drive, and it is not optional. It is one of the main reasons a computer feels fast—or painfully slow.

Understanding RAM helps explain both everyday performance problems and why computer upgrade prices are climbing.

WHAT RAM ACTUALLY IS

RAM stands for Random Access Memory. In simple terms, RAM is your computer's short-term working memory.

When a computer is turned on:
• The operating system loads into RAM
• Applications load into RAM
• Files you actively open are held in RAM

When the computer is turned off, RAM is empty. That's normal.

HOW RAM IS DIFFERENT FROM STORAGE

Storage (SSD or hard drive) is long-term memory. RAM is short-term.

Think of it this way:
• Storage is a filing cabinet

• RAM is desk space

If RAM runs out, the computer uses storage as temporary memory. This is called paging or swap, and it is much slower.

HOW COMPUTERS USE RAM

Every action uses RAM:
• Opening a browser
• Loading email
• Running accounting software
• Video calls
• Security software

Modern operating systems alone use several gigabytes of RAM before applications even start.

WHY MORE RAM MAKES COMPUTERS FEEL FASTER

More RAM does not make the processor faster. It prevents slowdowns caused by running out of memory.

With enough RAM:
• Applications stay open
• Switching tasks is instant
• Fewer freezes and crashes

WHY RAM PRICES ARE RISING

RAM prices are increasing for practical reasons.
AI systems require enormous amounts of high-performance memory, and manufacturers are prioritizing those markets.
Only a few companies produce most of the world's RAM, limiting supply flexibility.

Newer computers use newer RAM standards, which are more expensive and not backward compatible.
At the same time, businesses are upgrading systems, increasing demand.

WHAT THIS MEANS FOR BUSINESSES

• Underpowered systems waste time.
• RAM upgrades are often the best performance investment.
• Waiting does not guarantee lower prices.

For most business users:
• 16 GB is a practical minimum.
• 32 GB benefits heavy multitaskers.

THE TAKEAWAY

RAM is your computer's working memory. When there is not enough, everything slows down. Prices are rising because demand is growing faster than supply. Choosing the right amount now avoids frustration later.