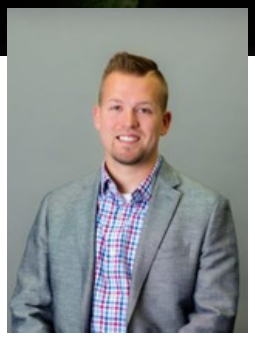
Virtual DataWorks

TECH BYTES

April 2026

APRIL IS FOR GROWTH.
SECURE IT.



This April, refresh your approach to cybersecurity. Use advanced tools, stay informed, and lead confidently as threats continue to evolve.

Matthew DeWees
-President

Ransomware isn't the moment the screen flashes and files stop opening. That's just the part you notice. The real story usually starts earlier with something that looks harmless. It's one login that slips through, one admin account with too much reach, one "we'll patch it later" system that stays open a little too long.

Here's the frustrating truth: by the time encryption begins, you're no longer in prevention mode. You're in damage control mode.

That's why the goal isn't "buy better ransomware protection". It's building a ransomware defense plan that breaks the chain before it gathers momentum.

The plan is surprisingly simple, and it's mostly about consistency. Strong sign-ins that hold up under phishing. Least privilege access so one compromised account can't roam freely. Patching that closes known holes fast. Early detection that catches suspicious behavior before it spreads. And backups you've actually tested, so recovery is a process, not a debate.

Ransomware doesn't create chaos out of nowhere. It exploits the chaos that's already there.

If permissions are messy and recovery is untested, you get a long, expensive week. If your basics are standardized and rehearsed, you get a contained incident you can handle.

Want to move from "hope we're covered" to a baseline you can trust? Contact us at everythingit@virtualdataworks.com for a technology consultation. We'll help you prioritize the first fixes and roll out a ransomware defense plan that holds up under pressure.

Matthew DeWees

President

WHAT'S INSIDE?

DID YOU KNOW?

In April 2005, the very first YouTube video, "Me at the zoo" was uploaded. It was just 19 seconds long... and it launched an entire internet era.

Virtual DataWorks

475 Wolf Ledges Parkway
Akron, Ohio 44311

virtualdataworks.com

(330) 800-2186

STOP RANSOMWARE IN ITS TRACKS: A 5-STEP PROACTIVE DEFENSE PLAN

Ransomware isn't a jump scare. It's a slow build.

In many cases, it begins days, or even weeks, before encryption, with something mundane, like a login that never should have succeeded.

That's why an effective ransomware defense plan is about more than deploying antimalware. It's about preventing unauthorized access from gaining traction.

Here's a five-step approach you can implement across smallbusiness environments without turning security into a daily obstacle course.

THE 5-STEP RANSOMWARE DEFENSE PLAN

Each step is practical, MSPfriendly, and repeatable across small-business environments.

Step 1: Phishing-Resistant Sign-Ins

"Phishing-resistant" sign-ins are authentication methods that can't be easily compromised by fake login pages or intercepted onetime codes. It's the difference between "MFA is enabled" and "MFA still works when someone is specifically targeted."

- Enforce strong MFA across all accounts, with priority given to admin and remote accounts
- Eliminate legacy authentication methods that weaken your security baseline
- Implement conditional access rules, such as step-up verification for high-risk sign-ins, new devices, or unusual locations

Step 2: Least Privilege + Separation

"Least privilege" means each account gets only the access it needs to do its job, and nothing more. "Separation" means keeping administrative privileges distinct from everyday user activity, so a single compromised login doesn't hand over control of the entire business.

- Keep administrative accounts separate from everyday user accounts
- Eliminate shared logins and minimize broad "everyone has access" groups
- Limit administrative tools to only the specific people and devices that genuinely require them

Step 3: Close known holes

"Known holes" are vulnerabilities attackers already know how to exploit, typically because systems are unpatched, exposed to the internet or running outdated software.

- Set clear patch guidelines: critical vulnerabilities addressed immediately, high-risk issues next, and all others on a defined schedule
- Prioritize internet-facing systems and remote access infrastructure
- Cover third-party applications

Step 4: Early detection

Early detection means identifying ransomware warning signs before encryption spreads across the environment. Think alerts for unusual behavior that enable rapid containment.

A strong baseline includes:

- Endpoint monitoring that can flag suspicious behavior quickly
- Rules for what gets escalated immediately vs what gets reviewed

Step 5: Secure, Tested Backups

"Secure, tested backups" are backups that attackers can't easily access or encrypt, and that you've verified you can restore successfully when it matters most.

Both NIST's ransomware guidance and the UK NCSC emphasize that backups must be protected and restorable. NIST specifically calls out the need to "secure and isolate backups."

- Keep at least one backup copy isolated from the main environment.
- Run restore drills on a schedule
- Define recovery priorities ahead of time, what needs to be restored first, and in what sequence

If you'd like help assessing your current defenses and building a practical, repeatable ransomware protection plan, contact us to schedule a consultation.

A SMALL BUSINESS ROADMAP FOR IMPLEMENTING ZERO-TRUST ARCHITECTURE

Most small businesses aren't breached because they have no security at all. They're breached because a single stolen password becomes a master key to everything else.

That's the flaw in the old "castle-and-moat" model. Once someone gets past the perimeter, they can often move through the environment with far fewer restrictions than they should.

And today, with cloud apps, remote work, shared links, and BYOD, the "perimeter" isn't even a clearly defined boundary anymore.

Zero-trust architecture for small businesses represents the shift that breaks that chain reaction. It's an approach that treats every access request as potentially risky and requires verification every time.

What Is Zero-Trust Architecture?

Zero Trust is a model that moves defenses away from "static, network-based perimeters." Instead, it focuses on "users, assets, and resources." It also "assumes there is no implicit trust granted to assets or user accounts" based only on network location or ownership.

Microsoft sets the idea down into a simple principle: the model teaches us to "never trust, always verify." In practice, that means verifying each request as though it came from an uncontrolled network, even if it's coming from the office.

IBM reports that the global average cost of a data breach is over $4 million, which is why reducing blast radius isn't a nice-to-have.

So, what does "Zero Trust" actually do differently day to day?

Microsoft frames it around three core principles: verify explicitly, use least privilege access, and assume breach. In small-business terms, that usually translates to:

- **Identity-first controls:** Strong MFA, blocking risky legacy authentication, and applying stricter policies to admin accounts.
- **Device-aware access:** Evaluating who is signing in and whether their device is managed, patched, and meets your security standards.
- **Segmentation to limit impact:** Breaking your environment into smaller zones so access to one area doesn't automatically grant access to everything else. Cloudflare describes microsegmentation as dividing perimeters into "small zones" to prevent lateral movement between systems.

Your Zero-Trust Roadmap

Zero Trust architecture for small businesses doesn't begin with a shopping list. It begins with a clear, focused plan.

If you're ready to move from "good idea" to real implementation, start with a single protect surface and commit to the next 30 days of measurable improvements. Small steps, consistent execution, and fewer unpleasant surprises.

If you'd like help defining your protect surface and building a practical Zero Trust roadmap, contact us for a consultation. We'll help you prioritize the right controls, align them to your environment, and turn Zero Trust into steady progress, not complexity.

HOW TO RUN A "SHADOW AI" AUDIT WITHOUT SLOWING DOWN YOUR TEAM

It usually starts small. Someone uses an AI tool to refine a difficult email. Someone enables an AI add-on inside a SaaS app because it promises to save an hour a week. Someone pastes a paragraph into a chatbot to "make it sound better."

Then It Becomes Routine.

And once it's routine, it stops being a simple tool decision and becomes a data governance issue: what's being shared, where it's going, and whether you could prove what happened if something goes wrong. That's the core of shadow AI security.

The goal isn't to block AI entirely. It's to prevent sensitive data from being exposed in the process.

Shadow AI Security in 2026

Shadow AI is the unsanctioned use of AI tools without IT approval or oversight, often driven by speed and convenience. The challenge is that the "helpful shortcut" can become a blind spot when IT can't see what's being used, by whom, or with what data Shadow AI security matters in 2026 because AI isn't just a standalone tool employees choose to use. It's increasingly embedded directly into the applications you already rely on. At the same time, it's expanding through plug-ins, extensions, and third-party copilots that can tap into business data with very little friction.

And there's a human reality in it: 38% of employees admit they've shared sensitive work information with AI tools without permission. It's people trying to work faster, but making risky decisions as they go.

That's why Microsoft sees the issue as a data leak problem, not a productivity problem.

Stop Guessing and Start Governing

If you'd like help building a practical shadow AI audit for your organization, contact us. We'll help you gain visibility, reduce exposure, and put guardrails in place without slowing your team down.

THE ESSENTIAL CHECKLIST FOR SECURING COMPANY LAPTOPS AT HOME

Remote work security gets easier when the basics are standardized. Use this quick checklist as a minimum baseline:

- Lock the screen every time you step away.
- Store work laptops securely when not in use.
- Don’t share work laptops with family members or guests.
- Use strong sign-ins and MFA on work accounts, with no exceptions for admins.
- Patch fast: enable automatic updates and restart when prompted.
- Secure home Wi-Fi like it’s part of the office.
- Keep security tools switched on (firewall + endpoint protection).
- Keep work data in approved work storage, not your personal cloud.

THE 2026 GUIDE TO UNCOVERING UNSANCTIONED CLOUD APPS

Build a practical workflow you can run quarterly (or continuously) using these quick moves to get visibility without triggering a wave of workarounds

- **Start with discovery:** build an inventory from identity logs, endpoints, and network/DNS data.
- **Investigate usage patterns,** not just app names (public sharing, personal accounts, unusual downloads).
- **Prioritize by risk:** sensitive data, weak authentication options, and poor admin visibility rise to the top.
- **Tag apps** as approved, restricted, replaced, or blocked so decisions are repeatable.
- **Warn before you block** when possible and always provide an approved alternative.
- **Review quarterly;** new apps and features show up faster than policy updates.

5 SECURITY LAYERS YOUR SMALL BUSINESS IS LIKELY MISSING (AND HOW TO ADD THEM)

If your security stack has grown organically over time, these are the gaps that often show up first.

- **Phishing-resistant authentication:** enforce strong MFA everywhere, then tighten admin and remote access first.
- **Device trust and usage policies:** define what a compliant device is, and what happens when it isn't.
- **Email and user risk controls:** reduce exposure by default with filtering, warnings, and easy reporting.
- **Continuous vulnerability and patch coverage:** measure patch latency and include third-party apps.
- **Detection and response readiness:** define what gets escalated, document runbooks, and practice containment steps.
- **Recovery that's proven:** run restore drills and define recovery priorities before you need them.
- **Governance that sticks:** publish clear "approved" standards and make exceptions time-bound and owned.

When you strengthen these five layers, you turn your business' security into a repeatable, measurable baseline you can be confident in.

Thank You!

Thanks for spending a few minutes reading our April newsletter. We hope it gave you some useful insights or ideas to help your technology run a little smoother this spring.

As always, if you have questions, or just want a second set of eyes on anything IT-related, we're only a phone call or email away.

CONTACT US BELOW

(330) 800-2186

everythingit@virtualdataworks.com

www.virtualdataworks.com

475 Wolf Ledges Parkway
Akron, Ohio 44311

VirtualDataWorks