NEWSLETTER

RJ2 Technologies Monthly Newsletter
June 2025

1701 Golf Road
Suite T3-300
Rolling Meadows, IL 60008

(847) 303-1194

www.rj2t.com

In this newsletter:

Shadow IT: How Employees Using Unauthorized Apps Could Be Putting Your Business At Risk

Your employees might be the biggest cybersecurity risk in your business – and not just because they're prone to click phishing e-mails or reuse passwords. It's because they're using apps your IT team doesn't even know about.

This is called Shadow IT, and it's one of the fastest-growing security risks for businesses today. Employees download and use unauthorized apps, software and cloud services – often with good intentions – but in reality they're creating massive security vulnerabilities without even realizing it.

These unsactioned tools operate outside the visibility and control of the IT department, making it nearly impossible to monitor data flows, enforce compliance, or respond effectively to breaches. Left unchecked, Shadow IT can lead to data leaks, compliance violations, and increased exposure to cyberattacks. Addressing this challenge requires a combination of employee education and modern security tools that provide visibility into all digital activity across the organization.

What Is Shadow IT?

Shadow IT refers to any technology used within a business that hasn't been approved, vetted or secured by the IT department. It can include things like:

- Employees using personal Google Drives or Dropbox accounts to store and share work documents.
- Teams signing up for unapproved project management tools like Trello, Asana or Slack without IT oversight.
- Workers installing messaging apps like WhatsApp or Telegram on company devices to communicate outside of official channels.
- Marketing teams using AI content generators or automation tools without verifying their security.

Why Is Shadow IT So Dangerous?

Because IT teams have *no visibility or control* over these tools, they *can't secure them* – which means businesses are exposed to all kinds of threats including:

- **Unsecured Data-Sharing** – Employees using personal cloud storage, e-mail accounts or messaging apps can accidentally leak sensitive company information, making it easier for cybercriminals to intercept.
- **No Security Updates** – IT departments regularly update approved software to patch vulnerabilities, but unauthorized apps often go unchecked, leaving systems open to hackers.
- **Compliance Violations** – If your business falls under regulations like HIPAA, GDPR or PCI-DSS, using unapproved apps can lead to noncompliance, fines and legal trouble.
- **Increased Phishing And Malware Risks** – Employees might unknowingly download malicious apps that appear legitimate but contain malware or ransomware.
- **Account Hijacking** – Using unauthorized tools without multifactor authentication (MFA) can expose employee credentials, allowing hackers to gain access to company systems.

Why Do Employees Use Shadow IT?

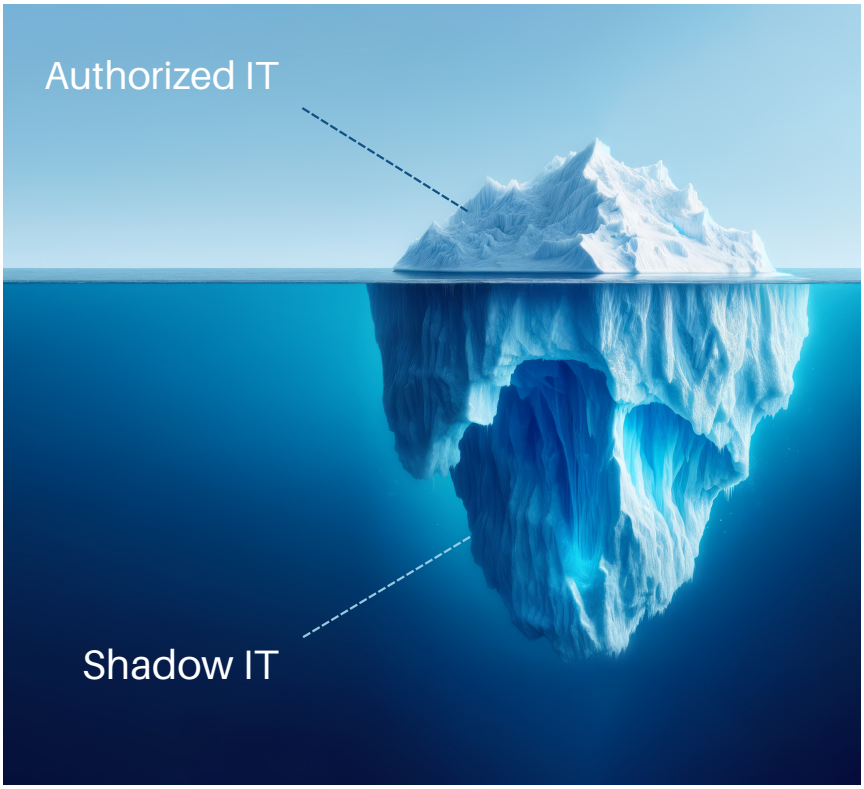
Most of the time, it's not malicious. Take, for example, the "Vapor" app scandal, an extensive ad fraud scheme recently uncovered by security researchers IAS Threat Labs.

In March, over 300 malicious applications were discovered on the Google Play Store, collectively downloaded more than 60 million times. These apps disguised themselves as utilities and health and lifestyle tools but were designed to display intrusive ads and, in some cases, phish for user credentials and credit card information. Once installed, they hid their icons and bombarded users with full-screen ads, rendering devices nearly inoperative. This incident highlights how easily unauthorized apps can infiltrate devices and compromise security.

But employees can also use unauthorized apps because:

- They find company-approved tools frustrating or outdated.
- They want to work faster and more efficiently.
- They don't realize the security risks involved.
- They think IT approval takes too long – so they take shortcuts.

Unfortunately, these shortcuts can cost your business BIG when a data breach happens.



How To Stop Shadow IT Before It Hurts Your Business

You can't stop what you can't see, so tackling Shadow IT requires a proactive approach. Here's how to get started:

1. Create An Approved Software List
Work with your IT team to establish a list of trusted, secure applications employees can use. Make sure this list is regularly updated with new, approved tools.

2. Restrict Unauthorized App Downloads
Set up device policies that prevent employees from installing unapproved software on company devices. If they need a tool, they should request IT approval first.

3. Educate Employees About The Risks
Employees need to understand that Shadow IT isn't just a productivity shortcut – it's a security risk. Regularly train your team on why unauthorized apps can put the business at risk.

4. Monitor Network Traffic For Unapproved Apps
IT teams should use network-monitoring tools to detect unauthorized software use and flag potential security threats before they become a problem.

5. Implement Strong Endpoint Security
Use endpoint detection and response (EDR) solutions to track software usage, prevent unauthorized access and detect any suspicious activity in real time.

Don't Let Shadow IT Become A Security Nightmare

The best way to fight Shadow IT is to get ahead of it before it leads to a data breach or compliance disaster.

Want to know what unauthorized apps your employees are using right now? Start with a Network Security Assessment to identify vulnerabilities, flag security risks and help you lock down your business before it's too late. **Call RJ2 Technologies at (847) 303-1194 or email marketing@rj2t.com to claim your FREE network security assessment.**

Get Fresh IT News Weekly with RJ2 Technologies!

Follow us on our social media pages for more IT content, latest tech trends, company updates, tech tips and more. Connect with the RJ2T family and show your support!

@RJ2Technologies @RJ2Technologies @RJ2Technologies

@RJ2Technologies @RJ2Technologies532

Think Paying The Ransom Will Fix Everything? Think Again

Imagine logging into your system one morning and finding everything locked down. A message demands thousands to get your data back. The pressure is intense. The temptation to just pay up and move on is real.
But here's the hard truth: Paying the ransom doesn't guarantee anything. And it often makes things worse.

Ransomware attacks are on the rise, and they're only getting smarter. These days, it's not just about locking up your files. Attackers also steal your data and threaten to leak it unless you pay. They'll even go after your backups, so you can't just restore and carry on.

Many business owners think paying the ransom is the quickest way to get back to normal. But it's rarely that simple.

Studies show that the true cost of recovering from a ransomware attack is ten times higher than the ransom itself. That's because even after you pay, there's no guarantee you'll get all your data back. Or that it hasn't been tampered with. You could still face weeks of downtime, lose customer trust, or get hit with regulatory fines if sensitive information is leaked.

And then there's the bigger picture. Every ransom paid helps fund the next attack. It's a vicious cycle. The more profitable ransomware becomes, the more motivated cyber criminals are to keep going… and keep improving their techniques.

So, is there a better approach? Yes.

Focus on recovery, not ransom. That means investing in strong, secure backups that can't be touched by ransomware. It means regularly testing your recovery plans. Training your team to respond quickly. And making sure your systems can be restored safely if disaster strikes.

You can't always stop ransomware from getting in. But you can make sure it doesn't stop your business.
Contact RJ2 Technologies by calling(847)-303-1194 or email marketing@rj2t.com to learn more.

Vendor Partner Highlight - SentinelOne®

This month we are excited to highlight SetinelOne, a world leader in cybersecurity. SentinelOne has grown and enhanced their platform for decades to create the world's most advanced cybersecurity platform. With a mission to defeat ever cyber attack, every second of the day, we appreciate their dedication to safeguarding data against cyber threatas.

RJ2 Technologies is proud to be in partnership with SentinelOne as it provides our clients advanced and reliable security solutions. By using their Endpoint Detection and Response (EDR) solution, powered by AI, RJ2 can provide real-time visibility into endpoint activities, threat detection, and automated response.

To learn more about this partnership please call RJ2 Technologies at (847)-303-1194 or email marketing@rj2t.com

5 Reasons To Be Wary of AI

Artificial intelligence (AI) is an incredible tool. It's revolutionizing industries, advancing medical research, and making businesses more productive. But like any powerful technology, it can also be used for the wrong reasons – and it's important you're aware of it.

Cyber criminals have discovered that generative AI (the same kind of AI that powers tools like ChatGPT and Copilot) makes their scams faster, smarter, and more convincing than ever…

AI-generated malware
Malware (malicious software) isn't new, but AI has made it quicker to produce, harder to detect, and more effective at bypassing security measures. Cyber criminals use AI to write malware that looks like legitimate browser extensions, software downloads, and even innocent-looking files like PDFs or images.

Stay safe: Keep your security software up to date and never download software or browser extensions from unknown sources.

Fooling security systems
Most cyber security software works by spotting known malware patterns. By slightly tweaking existing malware, scammers can create thousands of unique versions that security systems don't recognize.

Stay safe: Regularly update your security software to keep up with evolving threats. AI-powered security tools can also help to detect suspicious activity.

AI-powered password cracking
Cyber criminals are now using AI to break into accounts faster than ever. AI can test millions of password combinations per second, analyze leaked passwords, and even predict passwords based on common patterns.

Stay safe: Use strong, unique passwords for every account and enable multi-factor authentication (MFA) to add an extra layer of security.

Smarter phishing scams
Phishing emails used to be easy to spot – bad grammar, weird phrasing, and suspicious links were all giveaways. But with AI, scammers can create perfectly written, highly personalized messages that look exactly like they came from a trusted colleague or supplier.

Stay safe: Always verify unexpected emails, especially if they request payments, login details, or sensitive information. Hover over links before clicking and double-check sender addresses.

Deepfake impersonation
Imagine getting a video call from your CEO asking you to process an urgent payment. You recognize their voice and face… but it's not actually them. AI-generated deepfakes can clone voices and faces to trick employees into transferring money or sharing sensitive data.

Stay safe: If something seems unusual or too urgent, verify the request by calling on a known number or confirming in person.

AI-powered scams are evolving fast, but you don't have to be an easy target. A strong security culture, smart policies, and the right tools can help keep your business safe. If you're not sure whether your cyber security is up to date, RJ2 Technologies can help with a security audit. **Get in touch today by calling 847-303-1194 or email marketing@rj2t.com**.