TALK NERDY TO ME

INSIDE THIS ISSUE:

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!

- **Jason Horne**
CEO

IMPLEMENT ZERO TRUST FOR YOUR OFFICE GUEST WI-FI NETWORK

Guest Wi-Fi is a convenience your visitors expect and a hallmark of good customer service. But it's also one of the riskiest points in your network. A shared password that's been passed around for years offers virtually no protection, and a single compromised guest device can become a gateway for attacks on your entire business. That's why adopting a Zero Trust approach for your guest Wi-Fi is essential.

The core principle of Zero Trust is simple but powerful: never trust, always verify. No device or user gains automatic trust just because they're on your guest network. Here are some practical steps to create a secure and professional guest Wi-Fi environment.

Build a Totally Isolated Guest Network

The first and most crucial step is complete separation. Your guest network should never mix with your business traffic. This can be achieved through strict network segmentation by setting up a dedicated Virtual Local Area Network (VLAN) for guests. This guest VLAN should run on its own unique IP range, entirely isolated from your corporate systems.

Then, configure your firewall with explicit rules that block all communication attempts from the guest VLAN to your primary corporate VLAN. This strategic containment ensures that if a guest device is infected with malware, it cannot pivot laterally to attack your servers, file shares, or sensitive data.

Implement a Professional Captive Portal

Get rid of the static password immediately. A fixed code is easily shared, impossible to track, and a hassle to revoke for just one person. Instead, implement a professional captive portal, like the branded splash page you encounter when connecting to Wi- Fi at a hotel or conference. This portal serves as the front door to your Zero Trust guest Wi-Fi.

You can configure it securely in several ways. For example, a receptionist could generate a unique login code that expires in 8 or 24 hours, or visitors could provide their name and email to receive access. For even stronger security, a one-time password sent via SMS can be used. Each of these methods enforces the 'never trust' principle, turning what would be an anonymous connection into a fully identified session.

Enforce Policies via Network Access Control

Having a captive portal is a great start, but to achieve true guest network security, you need more powerful enforcement, and that is where a Network Access Control (NAC) solution comes into play. NAC acts like a bouncer for your network, checking every device before it is allowed to join, and you can integrate it within your captive portal for a seamless yet secure experience. If the guest's device fails posture checks, the NAC can redirect it to a walled garden with links to download patch updates or simply block access.

Apply Strict Access Time and Bandwidth Limits

Trust isn't just about determining who is reliable, it's about controlling how long they have access and what they can do on your network. Use your NAC or firewall to enforce strict session timeouts, requiring users to re-authenticate after a set period, such as every 12 hours.

Similarly, implement bandwidth throttling on the guest network. It is also a good business practice to prevent network congestion by activities that do not align with your business operations.

Create a Secure and Welcoming Experience

Implementing a Zero Trust guest Wi-Fi network is no longer an advanced feature reserved for large enterprises, but for all business sizes.

Do you want to secure your guest Wi-Fi without the complexity?
Contact us today to learn more.

SUPERNOTE NOMAD

Boost your productivity with the Supernote Nomad.

This ultra-portable digital notebook features a 7.8-inch glass E Ink screen and weighs just 266 grams. The device runs on a specialized Android 11-based OS, supports a wide range of document formats and offers a natural writing feel.

Whether you're brainstorming in a café or outlining your next big project, Supernote Nomad is your essential companion with being on the go

HOW TO USE MICROSOFT ENTRA CONDITIONAL ACCESS TO GRANT AND REVOKE CONTRACTOR ACCESS

Managing contractor logins can be a real headache. You need to grant access quickly so work can begin, but that often means sharing passwords or creating accounts that never get deleted. It's the classic trade-off between security and convenience, and security usually loses. Let's see how to use Microsoft's Entra Conditional Access to create a self-cleaning system for contractor access in roughly 60 minutes.

Set Up a Security Group for Contractors

The first step to taming the chaos is organization. Applying rules individually is a recipe for forgotten accounts and a major security risk. Instead, go to your Microsoft Entra admin center (formerly Azure AD admin center) and create a new security group with a clear, descriptive name, something like 'External- Contractors' or 'Temporary- Access'.

Add each new contractor to the group when they start and remove them when their project ends. This single step lays the foundation for clean, scalable management in Entra.

Build Your Set-and-Forget Expiration Policy

Conditional Access does the heavy lifting so you don't have to. In the Entra portal, create a new Conditional Access policy and assign it to your "External- Contractors" group. Then, define the conditions that determine how and when access is granted or removed.

In the "Grant" section, enforce Multi-Factor Authentication to add an essential layer of security. Next, under "Session," locate the "Sign-in frequency" setting and set it to 90 days, or whatever duration matches your contracts. This not only prompts regular logins but ensures that once a contractor is removed from the group, they can no longer re-authenticate, automatically locking the door behind them.

Lock Down Access to Just the Tools They Need

Think about what a contractor actually does. Your next policy ensures they only get the keys to the rooms they need.

Next, create a second Conditional Access policy for your contractor group. Under "Cloud apps," select only the applications they are permitted to use or a specific SharePoint site. Then, set the control to "Block" for all other apps. It's a powerful way to reduce risk, applying the principle of least privilege.

Add an Extra Layer of Security with Strong Authentication

For an even more robust setup, you can layer in device and authentication requirements. You are not going to manage a contractor's personal laptop, and that is okay. The goal is to make it very difficult for an attacker to misuse their credentials. You can configure a policy that requires a compliant device, then use the "OR" function to allow access if the user signs in with a phishing-resistant method.

Take Back Control of Your Cloud Security

With a little upfront setup in Conditional Access policies, you can create a system that's highly secure and effortlessly automatic. It's a win for security, productivity, and your peace of mind.

HOW TO PREVENT LEAKING PRIVATE DATA THROUGH PUBLIC AI TOOLS

Most public AI tools use the data you provide to train and improve their models. This means every prompt entered into ChatGPT or Gemini could be part of their training data. A single mistake by an employee could expose client information, proprietary code and processes. As a business owner, it's essential to prevent data leakage before it turns into a serious liability.

Establish a Clear AI Security Policy

Your first line of defense is a formal policy that clearly outline show public AI tools should be used. This policy must define what counts as confidential information and specify which data should never be entered into a public AI model, such as social security numbers, financial records, or product roadmaps.

Implement Data Loss Prevention Solutions with AI Prompt Protection

You can prevent leakage of personal information by implementing data loss prevention (DLP) solutions that stop data leakage at the source. Cloudflare DLP and Microsoft Purview offer advanced browser-level context analysis, scanning prompts and file uploads in real time before ever reaching the AI platform.

Conduct Continuous Employee Training

Conduct interactive workshops where employees practice crafting safe and effective prompts using real-world scenarios from their daily tasks. This hands-on training enables them to de-identify sensitive data, turning staff into active participants in data security while still leveraging AI for efficiency.

Make AI Safety a Core Business Practice

Integrating AI into your business workflows is no longer optional, it's essential for staying competitive and boosting efficiency. That makes doing it safely and responsibly your top priority. The four strategies we've outlined provide a strong foundation to harness AI's potential while protecting your most valuable data.

POWER AUTOMATE FOR CLOUD RESOURCES

Prevent unmanaged growth of cloud resources by following these:

1. Automate the Shutdown of Development VMs:
Create a Power Automate flow that triggers daily and queries Azure for all virtual machines with a specific tag. The flow then checks the machine's performance metric and turns off power for unutilized VMs.

2. Identify and Report Orphaned Storage Disks:
Build a schedule that runs weekly. The flow will list all unattached managed disks in your subscription and will then compose a detailed report.

3. Terminate Expired Temporary Resources:
Set up a flow triggered by a custom date field. When you create a temporary resource, add the tag. The flow runs, checks for tagged resources, and deletes them on the date.

3 STEPS TO A FORMAL IT ASSET DISPOSITION POLICY

You can't protect what you don't plan for. Start with a straight forward IT Asset Disposition (ITAD) policy that clearly outlines the steps and responsibilities, no need for pages of technical jargon. Simply put, ITAD is the secure, ethical, and fully documented way to retire your IT hardware. At a minimum, it should cover:

- The process for retiring company-owned IT assets.
- Who does what; who initiates, approves, and handles each device.
- Standards for data destruction and final reporting.

A clear policy keeps every ITAD process consistent and accountable through a defined chain of custody. It turns what could be a one-off task into a structured, secure routine, helping your business maintain a strong security posture all the way to the end of the technology lifecycle.

THE SMARTER WAY TO VET YOUR SAAS INTEGRATIONS

Here are some smart and systematic SaaS evaluation processes that protect your business from third-party risk.

- Scrutinize the SaaS's Security Posture: Your first steps should be examining their certifications and, in particular, asking them about the SOC 2 Type II report.
- Chart the Tool's Data Access and Flow: You need to understand what data the integration will touch by asking a simple, direct question: What access permissions does this app require?
- Examine Their Compliance and Legal Agreements: Carefully review their terms of service, compliance, privacy policies, and how data is stored.
- Analyze the SaaS Integration's Authentication Techniques: Choose integrations that use modern and secure authentication protocols such as OAuth 2.0.
- Plan for the End of the Partnership: Every technology integration follows a lifecycle and will eventually be deprecated, upgraded, or replaced. A responsible vendor will have clear, well-documented offboarding procedures.

We hope you all had a wonderful Christmas and an even better New Year!