TakTik Technologies

Free Cyber Security Discovery & SAM Audit

Understand Your Exposure. Protect What Matters.

Powered by Threatmatic observe mode

THE CYBER THREAT LANDSCAPE HAS FUNDAMENTALLY SHIFTED.

ARTIFICIAL INTELLIGENCE HAS INDUSTRIALISED ATTACKS THAT ONCE REQUIRED SOPHISTICATED HUMAN ADVERSARIES.

THE OLD MANUAL REALITY

AI WRITES MALWARE IN MINUTES, NOT MONTHS — AND IT LEARNS HOW TO EVADE SIGNATURE-BASED DEFENCES.

AI-GENERATED PHISHING CAN MIMIC THE EXACT WRITING STYLE OF YOUR CEO OR CFO — EMPLOYEES CAN'T TELL THE DIFFERENCE.

THE NEW AI-POWERED REALITY

AI AUTOMATES VULNERABILITY SCANNING, CREDENTIAL STUFFING, AND COMMAND-AND-CONTROL COMMUNICATION AT SCALE.

SPEED GAP: AI ATTACKS OPERATE FASTER THAN ANY HUMAN SECURITY TEAM CAN RESPOND.

43%

OF ALL OF ALL CYBERATTACKS TARGET SMALL BUSINESSES — SMBs ARE THE PRIMARY TARGET, NOT ENTERPRISES.

AVERAGE COST OF A BREACH FOR A SMALL BUSINESS:

$108,000.

THE KEY SHIFT: ATTACKS ARE NO LONGER MANUAL AND TARGETED — THEY ARE AUTOMATED AND INDISCRIMINATE. EVERY BUSINESS IS NOW IN THE CROSSHAIRS.

6 Blind Spots Every SMB Carries

Before you can defend your business, you need to see it. Most SMBs are managing security based on memory and assumption — not evidence.

Shadow IT

employees deploy apps (Dropbox, personal Google, ChatGPT plugins) without IT approval — **data leaves without anyone knowing**

Unmanaged devices

personal phones, vendor **laptops, smart TVs, IoT sensors** on the same network **as business data**

Orphaned accounts

ex-employees whose credentials were never revoked — still active in SaaS applications

Unknown traffic

data flowing in and out of your network to **destinations nobody has reviewed**

Stale policies

firewall rules written years ago that nobody has reviewed since the last IT person left

Misconfigured cloud storage

S3 buckets, SharePoint folders, and SaaS permissions set to public or over-permissioned by mistake

You cannot protect what you cannot see.

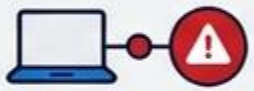
TakTik's **Free** Cyber Security Discovery & SAM Audit:

TWO COMPLEMENTARY COMPONENTS

Together they give you the complete picture.

Component 1 — Cyber Security Posture Assessment

Inbound and outbound traffic analysis: what is your network exposed to?



Malicious IP correlation: are any of your endpoints already communicating with known threat actors?

Insecure protocol detection: RDP, Telnet, unencrypted FTP — risky paths that attackers use

Shadow asset discovery: devices on your network you didn't know existed

Threat exposure score: a clear view of your attack surface

Component 2 — SAM Audit (Software Asset Management)

Every application being accessed — cloud, on-premise, personal

Every user accessing each application — with frequency and access patterns

Every device the access is coming from

Unauthorised or unvetted applications in active use

Compliance gaps against HIPAA, NIST CSF, and basic cyber hygiene standards

TOGETHER, these two components answer the two most important questions in security:

What is on my network?

Who is accessing what?

THE PROCESS IS SIMPLE, NON-DISRUPTIVE, AND COMPLETELY TRANSPARENT

The entire process is non–invasive. Your business runs normally throughout

1 ONBOARDING CALL (15 MINUTES)

TakTik walks through the scope, answers questions, and schedules the agent deployment.

2 AGENT INSTALL (MINUTES, NOT DAYS)

A lightweight Threatmatic software agent is installed on your endpoints. The agent is under 60MB on disk, uses under 30MB of memory, and consumes 0.1% CPU. Your team will not notice it is there.

3 SILENT OBSERVATION MODE (15 TO 30 DAYS)

The agent runs in pure observe mode — no enforcement, no blocking, no disruption to your business operations. It captures every traffic flow, maps every application accessed, and logs every user and device interaction. Nothing is changed on your network.

4 ANALYSIS AND REPORT

TakTik analyses the captured data in the Threatmatic console and prepares your personalised Security Posture Report.

5 DISCOVERY REVIEW CALL

TakTik walks through the findings — your assets, your risks, your SAM inventory, and your blueprint for default deny.

SECURITY POSTURE REPORT | Informed Security Decisions Delivered by TakTik

1 — ASSET INVENTORY

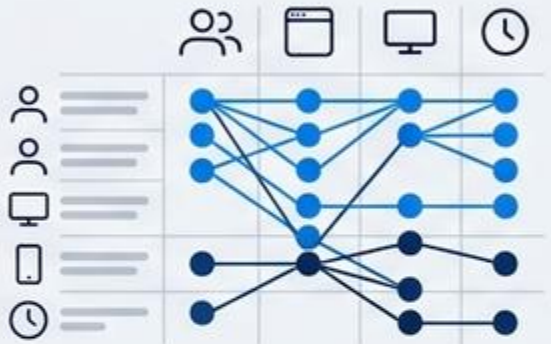
Threatmatic provides a scoped asset inventory.

On every endpoint where the agent is installed, the device is fully catalogued.

On any subnet where Threatmatic is deployed as a network access point, it discovers all devices present in that subnet — including unmanaged devices, printers, IoT sensors, and other endpoints that have no agent.

This gives you a structured, evidence-based inventory within the deployment scope.

2 — USER-APPLICATION MATRIX



Who accessed what, from which device, at what time.

A complete picture of application usage across your organisation — including personal and unauthorised apps — captured from agent-monitored endpoints.

3 — RISK EXPOSURE REPORT

Your threat surface: inbound exposure, malicious IP correlations, insecure protocols in use, open ports, and a prioritised list of risks

Your prioritised list of risks requiring action.

4 — DEFAULT DENY BLUEPRINT

An auto-generated whitelist of approved traffic flows — the exact policy you need to move to a default deny posture.

The rules are already written. You just need to decide when to enforce them.

This report is built from your actual traffic, your actual users, and your actual environment — scoped to where Threatmatic is deployed.

TRANSFORMING TO A DEFAULT DENY SECURITY POSTURE

THE JOURNEY TO STRUCTURAL IMMUNITY

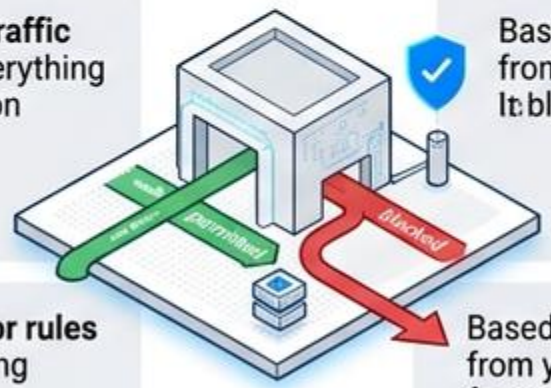
Reactive → Structurally Immune

Observe → **Map** → **Whitelist** → **Enforce** → **Default Deny**

The discovery audit is Step 1 of this journey. It is the foundation that makes default deny possible.

WHAT DEFAULT DENY MEANS

Only **explicitly approved traffic flows are permitted** — everything else is blocked by definition



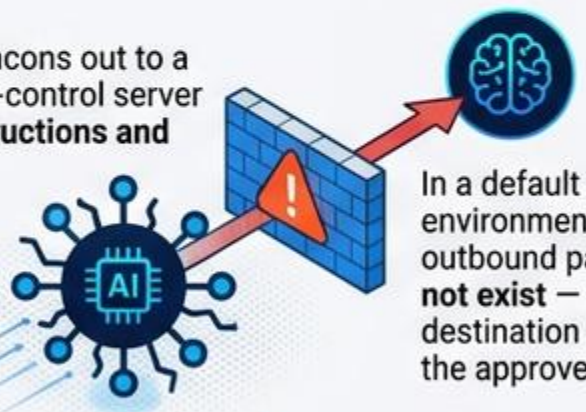
Based on **observed behaviour** from your actual network — It blokest

Not based on **signatures or rules** that need constant updating

Based on **observed behaviour** from your actual network — built from evidence, not assumptions

WHY THIS DEFEATS AI-ENABLED MALWARE

AI malware beacons out to a command-and-control server to **receive instructions and exfiltrate data**



In a default deny environment, that outbound path **does not exist** — the destination is not on the approved list.

The malware has **no approved path through your network** — it is **structurally blocked**, not signature-detected.

Zero-day malware — malware that no antivirus has ever seen — is blocked for the same reason.

THIS DISCOVERY COSTS YOU NOTHING.

WHAT YOU GET, AT NO CHARGE:

Full Security Posture Report tailored to your environment

Complete SAM audit: every application, every user, every device

Risk exposure analysis with prioritised action items

A 30-minute Blueprint: a ready-to-use policy built from your technology partner

WHAT IT COSTS:

$0

$0. No contracts. No obligations.
No commitment beyond the **15-minute** onboarding call.

WHY TAKTIK OFFERS THIS:

TakTik has served businesses in Georgia and the Southeast for over 35 years

Technology neutral. We recommend what is right for your business, not what earns us the biggest margin.

We believe every business deserves to know their real security posture before making any buying decision.

The only risk is not knowing what is on your network.

THREE SIMPLE STEPS TO GET STARTED TODAY

STEP 1: SCHEDULE YOUR ONBOARDING CALL (15 MINUTES)

Contact TakTik Technologies to **schedule a brief intro call.** Jeff Brown will walk you through the process and answer any questions.

STEP 2: AGENT INSTALL (MINUTES)

TakTik guides your IT team through the lightweight agent deployment. Most customers are live within an hour.

STEP 3: RECEIVE YOUR SECURITY POSTURE POSTURE REPORT

After **15 to 30 days** of silent observation, **TakTik delivers your full report** and walks you through the findings.

CONTACT TAKTIK TECHNOLOGIES

Jeff Brown
TakTik Technologies
Johns Creek, Georgia
Website:
taktiktechnologies.com

Capacity note: TakTik runs a limited number of free discovery engagements each month to ensure every customer receives personal attention.

The question is not whether your business has blind spots.
Every business does. The question is: do you want to see them?