THREATMATE™

YOUR NEXT MOVE

Microsoft 365 Security Baseline:

How to Effortlessly Achieve Microsoft 365 Security at Scale with CISA ScubaGear



Executive Summary

Microsoft 365 has become the backbone of SMB operations, powering email, authentication, collaboration, and business continuity for more than 345 million paid users worldwide (Microsoft Security Blog, 2024). Its ubiquity also makes it a prime target, eg., nearly 90 percent of cyberattacks begin with email or identity compromise, and a single tenant breach can expose sensitive communications, financial data, intellectual property, and administrative controls.

Yet most Microsoft 365 environments remain dangerously under-secured. Default settings often persist, and misconfigurations such as legacy authentication or missing MFA on admin accounts create hidden exposures that attackers exploit with ease. Managed Service Providers (MSPs) face a scaling challenge: existing frameworks like CIS Controls lack specificity, while Microsoft Secure Score blends licensing priorities with security guidance. Auditing tenants manually is slow, inconsistent, and nearly impossible to sustain across dozens or hundreds of clients.

To address this gap, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) introduced ScubaGear, a defensible, threat-informed baseline for Microsoft 365 now required across U.S. government agencies. ScubaGear offers specific configuration checks, binary pass/fail results, and clear scoring—but running it manually doesn't scale. This white paper explores why Microsoft 365 is such a high-value target, the most common misconfigurations, and why existing approaches fall short. Most importantly, it shows how ThreatMate automates the ScubaGear baseline, enabling MSPs to deliver scalable, profitable, and defensible Microsoft 365 security services.

To address these challenges, this white paper explores:

- Why Microsoft 365 is such a high-value target.
- The most common misconfigurations attackers exploit.
- Why existing approaches (Secure Score, CIS Controls) fall short.
- How ScubaGear provides a defensible baseline for MSPs.
- And most importantly, how ThreatMate automates the ScubaGear baseline, enabling MSPs to deliver scalable, profitable, and defensible Microsoft 365 security services.

1. The Strategic Importance of Microsoft 365 Security

For SMBs, Microsoft 365 is no longer just an email and office suite — it is the digital backbone of business continuity. It integrates communication, collaboration, authentication, and storage into a single cloud platform. MSPs have embraced it as a standard offering, bundling licensing and management into their service catalogs.

But with ubiquity comes risk. Attackers view Microsoft 365 as a crown jewel target: compromise one tenant, and they gain a one-stop shop of sensitive assets. Stolen email accounts provide entry points for Business Email Compromise (BEC) scams. Misconfigured sharing permissions expose confidential files to the public internet. Compromised global admin accounts allow attackers to escalate privileges and move laterally into other systems.

Recent statistics underscore the urgency:

- **345 million paid Microsoft 365 users globally** (Microsoft Security Blog, 2024).
- **90% of cyberattacks begin with email or identity compromise** (Microsoft Security Blog, 2024).
- **82% of breaches involve the human element**, including phishing and credential misuse (Verizon DBIR, 2024).

For MSPs, these numbers aren't just abstract. They translate into real-world client pain: ransomware incidents, lost data, regulatory fines, reputational damage, and, in many cases, lost contracts. Clients may forgive downtime. *They will not forgive a breach that exposes their financials or client communications.*



Figure 1: Microsoft 365 as the SMB Backbone

That's why securing Microsoft 365 is no longer optional or "nice to have." It's a strategic imperative. MSPs must show clients they can defend their tenants against the most common, most preventable exposures; and they need a way to prove it.

2. Common Misconfigurations That Hackers Exploit

Even in organizations that consider themselves "secure," Microsoft 365 tenants are often riddled with misconfigurations. These aren't obscure, edge-case vulnerabilities—they are basic gaps that attackers routinely exploit.

2.1 Legacy Authentication Still Enabled

Legacy protocols like IMAP and POP3 don't support modern security controls like Multi-Factor Authentication (MFA). When left enabled, attackers can bypass MFA entirely and brute force accounts using stolen or weak passwords. Despite Microsoft's push to deprecate these protocols, **over 80% of tenants still allow legacy authentication** (Proofpoint Cloud Threat Report, 2024).

2.2 Missing MFA on Admin Accounts

It's one thing for an end user to lack MFA. It's another for global administrators, who can reset passwords, modify permissions, or create new accounts. Shockingly, **only 26% of SMBs enforce MFA across all cloud services** (Datto SMB Security Report, 2024). That leaves crown-jewel accounts dangerously exposed.

2.3 Audit Logging Disabled

Audit logs are critical for forensics after an incident. Yet in many tenants, logging is disabled by default or never reviewed. This creates blind spots that make it impossible to trace attacker actions during or after a breach.

2.4 Overly Permissive External Sharing

Microsoft 365 makes it easy to collaborate externally, but without proper restrictions, files can be shared publicly without oversight. Sensitive data can leak outside the organization with no alerts and little recourse.

2.5 Auto-Forwarding Rules

Attackers who compromise accounts often set up forwarding rules that silently send email to external addresses. These rules enable Business Email Compromise (BEC) scams and persist even after passwords are changed.

These misconfigurations are rarely intentional. They emerge because tenants are complex, licensing is inconsistent, and MSPs juggle dozens of environments with different defaults. The result is a patchwork of security postures where attackers only need to find one weak link.

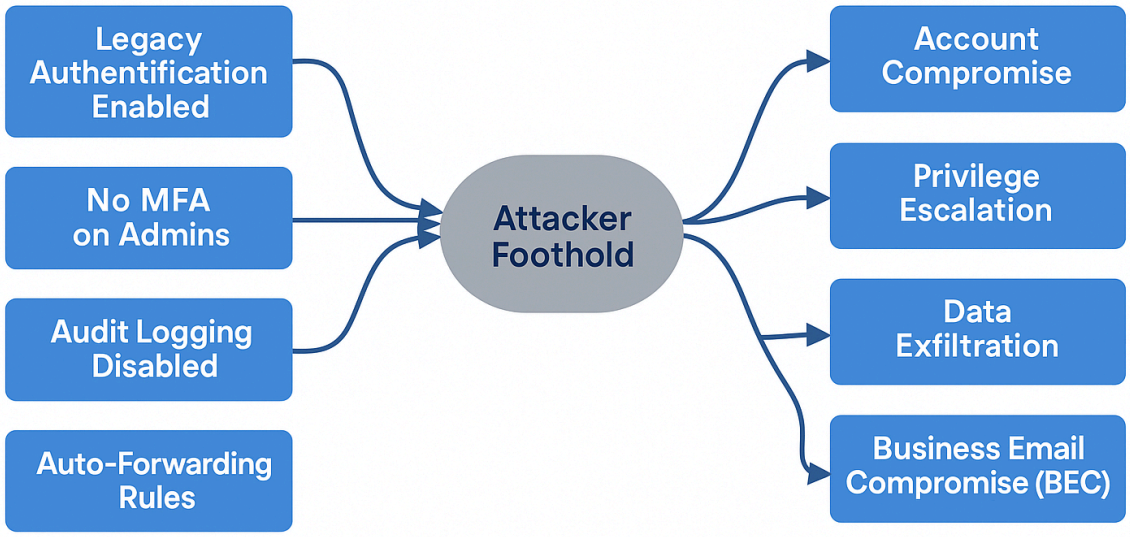


Figure 2: Attack Pathways from Common M365 Misconfigurations

3. Why Existing Approaches Fall Short

MSPs aren't ignoring Microsoft 365 security. Most already rely on frameworks and tools to guide their assessments. The real problem is that the two most common references—**Microsoft Secure Score** and the **Center for Internet Security (CIS) Controls**—are either incomplete or ill-suited for the realities of managing dozens of client tenants.

The result? MSPs are left improvising with manually intensive approaches or stuck translating generic recommendations into specific actions, or defending "scores" that don't hold up under scrutiny after a breach. This lack of a clear, defensible standard creates unnecessary friction with clients and leaves tenants exposed.

3.1 Microsoft Secure Score: Helpful but Biased

Secure Score has become the default measurement for many MSPs. It is accessible directly in the Microsoft 365 admin portal, provides a numeric grade, and outlines suggested improvements. At first glance, it feels like a ready-made baseline.

But Secure Score is built through Microsoft's own lens, and that introduces several challenges:

- **License-driven priorities.** Some improvements are only available in higher-tier SKUs. As a result, the "path to a better score" often looks like a licensing upsell, not a security necessity.

- **Convenience over security.** Secure Score recommendations balance usability against risk reduction. For example, some tenant defaults remain lenient because tightening them could frustrate users.

- **No defensible threshold.** A client who sees a score of 55 might reasonably ask, *"Is that good enough?"* Secure Score doesn't answer that question in a way MSPs can stand behind when justifying additional remediation.

In short: Secure Score is useful as a visibility tool, but not as a defensible, security-first baseline.

3.2 CIS Controls: Credible but Too Generic

The **CIS Controls** are widely respected. They've been around for decades and are recognized globally as a best-practice framework for general IT security. For MSPs, adopting CIS has advantages: it shows alignment with an independent authority, and it can provide a broad roadmap for improving client environments.

The problem lies in specificity. CIS Controls were never designed with SaaS platforms like Microsoft 365 in mind. Their recommendations—though sound—are intentionally broad. Consider a few examples:

- **Control 6.3: Require MFA for all users.** This is excellent advice, but in practice, what does this mean for M365 tenants? Should MFA be applied only to global admins, or to every user, and does that include every mailbox? How should MSPs handle service accounts that don't support MFA? Without clear SaaS-specific guidance, MSPs are left to interpret.

- **Control 8.11: Collect detailed audit logs.** Again, no one disputes the value. But in Microsoft 365, logging configurations vary by license level. Some logs require E5-level subscriptions to access. CIS doesn't address how MSPs should balance client budgets against audit requirements.

- **Control 13.1: Monitor for unauthorized email forwarding.** A solid principle, but CIS doesn't spell out that in M365, attackers often create auto-forwarding rules to external domains—a specific misconfiguration ScubaGear flags directly.

This vagueness leads to inconsistency and inconsistency leads to opportunity for attackers. One MSP may enforce MFA only on admins. Another may push for tenant-wide enforcement. Both

could argue they are “aligned with CIS,” but the risk reduction achieved is dramatically different. For SMB clients, that inconsistency translates into uneven protection.

	Microsoft Secure Score	CIS Controls	CISA ScubaGear
Specificity	Medium — Tenant-level cnecks but influenced by license tier and usability trade-offs	Low — Broad, generic security principles that require interpretatiom for SaaS	High — Tactical, configurration-specific checks for Microsoft 365
Credibility	Medium — Vendor-provided influenced by product roadmap	High — Independent, globally recognized security authority	High — Government-issued, threat-informed, unbiased
Actionability	Medium — Improvement tasks often tied to licens-ing or optioral controls	Medium — Guidance is sound but abstract; requires translation into	High — Binary pass/fail controls with clear remediation steps
Operational Value	Medium — Useful visibility, but not defénsible as a baseline	Low — Not SaaS-native, inconsistent across MSPs and clients	High — Standardized, automatable, scalable across tenants

Figure 3: Comparison of different frameworks for securing Microsoft 365

CIS Benchmarks do exist for Microsoft 365, but they remain high-level, with long documents that often feel abstract or overwhelming. They are difficult to operationalize across dozens of tenants without significant customization. For MSPs who must deliver scalable, repeatable services, this creates more overhead than clarity.

3.3 The Gap MSPs Face

What MSPs truly need is a baseline that is specific, defensible, and operational. Secure Score provides visibility but is biased by licensing and usability trade-offs. CIS Controls are credible but generic, requiring MSPs to bridge the gap between principle and implementation.

Neither solves the real problem: giving MSPs a clear, authoritative, and SaaS-native standard they can use to assess risk, drive remediation, and explain to clients why changes matter.

That is exactly the gap filled by CISA’s ScubaGear baseline.

4. Enter ScubaGear: A Defensible Security Baseline

For years, MSPs have lacked a clear and defensible answer to a simple but critical question: *what does "secure" look like in Microsoft 365?* Existing tools like Secure Score provide visibility, and frameworks like CIS Controls provide general principles, but neither offer the tenant-specific clarity MSPs need.

The Cybersecurity and Infrastructure Security Agency (CISA) has now delivered that missing piece with ScubaGear, a tactical, operational baseline designed specifically to harden Microsoft 365 tenants against real-world threats.

4.1 What Exactly Is ScubaGear?

ScubaGear is not a whitepaper or abstract checklist. It is a practical, tactical set of configuration checks released by CISA to help organizations standardize Microsoft 365 security. At its core, ScubaGear consists of:

- **The Baseline Itself.** A JSON-based reference file that lists recommended tenant configurations, mapped to specific controls. This is also published in a human-readable format for IT teams.

- **An Assessment Tool.** A free PowerShell script published by CISA that scans a Microsoft 365 tenant against the baseline and generates results.

- **A Scoring Model.** Output includes a **numeric score (0–100)** plus a list of controls marked as pass/fail, leaving no ambiguity about compliance.

- **Machine-Readable Outputs.** Results are available in JSON format, making it possible for MSPs to integrate findings into their own dashboards, ticketing systems, or client reports.

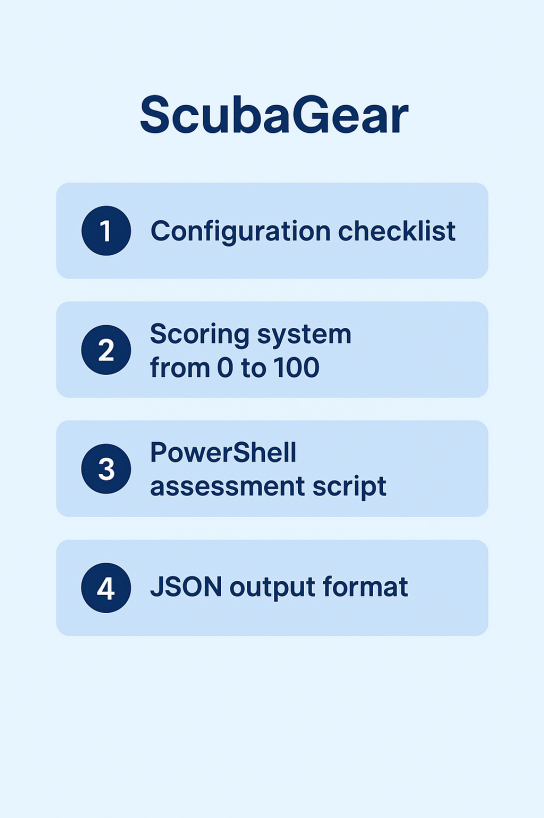


Figure 4: The nuts and bolts of ScubaGear

Together, these elements make ScubaGear not just guidance, but a usable operational tool.

4.2 The Scope of ScubaGear Controls

ScubaGear is comprehensive and targeted. It addresses the most common misconfigurations attackers exploit in Microsoft 365 environments. Among the areas covered:

- **Identity & Authentication**
    - Enforce Multi-Factor Authentication (MFA) for all admin and user accounts
    - Disable legacy authentication protocols (e.g., IMAP, POP3, SMTP AUTH)
    - Limit or eliminate shared accounts and insecure service principals
- **Logging & Monitoring**
    - Ensure audit logging is enabled for user and admin activities

    - Require mailbox auditing and alerting for suspicious forwarding rules
    - Retain logs for compliance and forensics
- **Access & Permissions**
    - Review and restrict global admin roles
    - Enforce least privilege across directory roles
    - Control guest account access and external sharing defaults
- **Data Protection**
    - Restrict auto-forwarding rules that can enable BEC attacks
    - Configure safe defaults for OneDrive/SharePoint external sharing
    - Require encryption and modern authentication for email and file access
- **Resilience & Hardening**
    - Enforce baseline policies for Exchange, SharePoint, and Teams
    - Ensure security defaults are applied consistently across tenants
    - Disable insecure protocols and legacy app configurations

Each control is binary, either the tenant meets the baseline requirement, or it doesn't. This removes ambiguity and helps MSPs explain risks in plain terms: *"This control failed; here's why it matters; here's what we need to change."*

4.3 Why ScubaGear Is Defensible

CISA's role gives ScubaGear gravitas that no vendor-driven approach can match. Key factors that make it defensible:

- **Unbiased Authority.** Unlike Microsoft Secure Score, ScubaGear is not influenced by licensing tiers or vendor sales priorities.
- **Threat-Informed.** Controls are based on how real-world attackers exploit Microsoft 365 misconfigurations — not theoretical risks.

- **National-Level Guidance.** CISA builds these baselines to protect federal agencies and critical infrastructure, which means MSPs can confidently apply the same standards to SMB clients.

- **Plain-Language Justification.** MSPs can point to CISA, the U.S. government's lead cybersecurity agency, as the source of recommendations. This shifts the burden of proof away from the MSP's opinion and onto a trusted external authority.

When challenged by a client on the necessity of a control ("Do we really need MFA everywhere?"), MSPs have a credible answer: *"This isn't just our policy; it's the U.S. government's recommended baseline."*

4.4 How ScubaGear Fits Into MSP Operations

MSPs can adopt ScubaGear at multiple touchpoints in their service delivery:

1. **Initial Assessments.** Run ScubaGear during onboarding to baseline a new tenant. Use results to highlight gaps, win trust, and prioritize remediation.

2. **Quarterly Business Reviews (QBRs).** Incorporate ScubaGear scores into client reports. Trends over time show progress and justify continued investment.

3. **Incident Response.** In the event of a compromise, use ScubaGear to demonstrate whether key baseline protections (like audit logging or MFA) were in place or missing.

4. **Regulatory Alignment.** Many SMB clients face compliance requirements (HIPAA, CMMC, FTC Safeguards Rule). ScubaGear provides a defensible way to show due diligence against federal standards.

5. **Standardized Services.** By aligning all tenants to the same baseline, MSPs can simplify their operations, reduce variance, and deliver consistent security outcomes across their client base.

4.5 ScubaGear in Action: What an MSP Sees

A ScubaGear run produces:

- A **numeric score (0–100)** showing how closely the tenant aligns to baseline.

- A **list of failed controls**, such as "Legacy authentication enabled" or "Audit logging disabled."

- **Clear remediation actions** tied directly to configuration changes in the Microsoft 365 portal.

For MSPs, this means no wasted time debating what matters. The findings are specific, actionable, and defensible.

4.6 The Limits of Manual ScubaGear Adoption

While ScubaGear is powerful, running it manually presents challenges:

- Each assessment requires PowerShell execution per tenant.
- Scores and outputs must be manually tracked, compared, and reported.
- Drift (changes made by clients or staff over time) is not automatically monitored.
- Scaling across dozens of tenants becomes cumbersome, if not impossible, without automation.

That is why ScubaGear is best seen not as the final solution, but as the foundation. MSPs need tools to automate assessments, centralize results, track changes over time, and prove value consistently.

This sets the stage for ThreatMate's role in operationalizing ScubaGear at scale**.**

5. The MSP Challenge: Scale and Consistency

ScubaGear represents a breakthrough for Microsoft 365 security. For the first time, MSPs have a defensible, tactical baseline they can use to measure tenant configurations against real-world threats. But while ScubaGear solves the "what to measure" problem, it does not solve the **"**how to operationalize**"** problem.

5.1 The Manual Burden of ScubaGear

Running ScubaGear in its raw form requires MSPs to:

- Log into each tenant individually.
- Execute the PowerShell assessment script.
- Export JSON and human-readable reports.

- Manually compare scores across clients.
- Track remediation status and tenant drift over time.

This process may be manageable for a single tenant. But MSPs rarely manage just one. A typical provider may support dozens of Microsoft 365 environments, each with unique licensing, policies, and histories of configuration drift. Running ScubaGear manually in that context quickly becomes impractical, inconsistent, and error-prone.

5.2 Inconsistency Across Tenants

Manual execution also introduces variance across technicians and clients. One engineer may run the assessment quarterly, another only when onboarding. Some clients may receive detailed remediation plans, while others get only a score. This lack of standardization undermines the value of ScubaGear and creates unnecessary risk.

Clients, however, expect consistency. Whether an MSP manages ten tenants or one hundred, every environment should be held to the same standard, reported in the same way, and remediated with the same urgency.

5.3 The Challenge of Drift

Even when MSPs remediate findings, Microsoft 365 tenants are dynamic. Admins change permissions, users adjust sharing settings, and licensing updates alter available controls. Over time, previously remediated issues can resurface. Without continuous monitoring, MSPs may find that a tenant that “passed” the baseline last quarter is suddenly out of alignment today.

Tracking this configuration drift manually across dozens of clients is nearly impossible. Without automation, MSPs risk missing regressions and losing visibility into how secure their clients actually are at any given moment.

5.4 Proof of Value Problem

Finally, MSPs must prove value to clients. It’s not enough to say “we secured your tenant.” Clients want evidence. They want reports that show progress over time, that justify their investment in managed security, and that stand up under scrutiny from regulators, auditors, or cyber insurance underwriters.

ScubaGear provides credible, binary results — but MSPs still need a way to package those results consistently into reports, QBR materials, and compliance evidence. Doing this manually adds hours of labor per tenant, per quarter.

5.5 The Bottom Line

ScubaGear gives MSPs the right framework. But without automation, it remains a tactical tool, useful for spot-checks, not scalable as a core managed security service.

To truly operationalize ScubaGear across dozens of clients, MSPs need a platform that:

- Runs assessments continuously on a schedule, not manually.
- Aggregates results into a centralized view.
- Tracks drift and highlights regressions over time.
- Prioritizes failed controls for remediation.
- Produces client-ready reports with minimal effort.

This is the gap ThreatMate fills, transforming ScubaGear from a one-off baseline into a repeatable, scalable service that MSPs can deliver across their entire customer base.

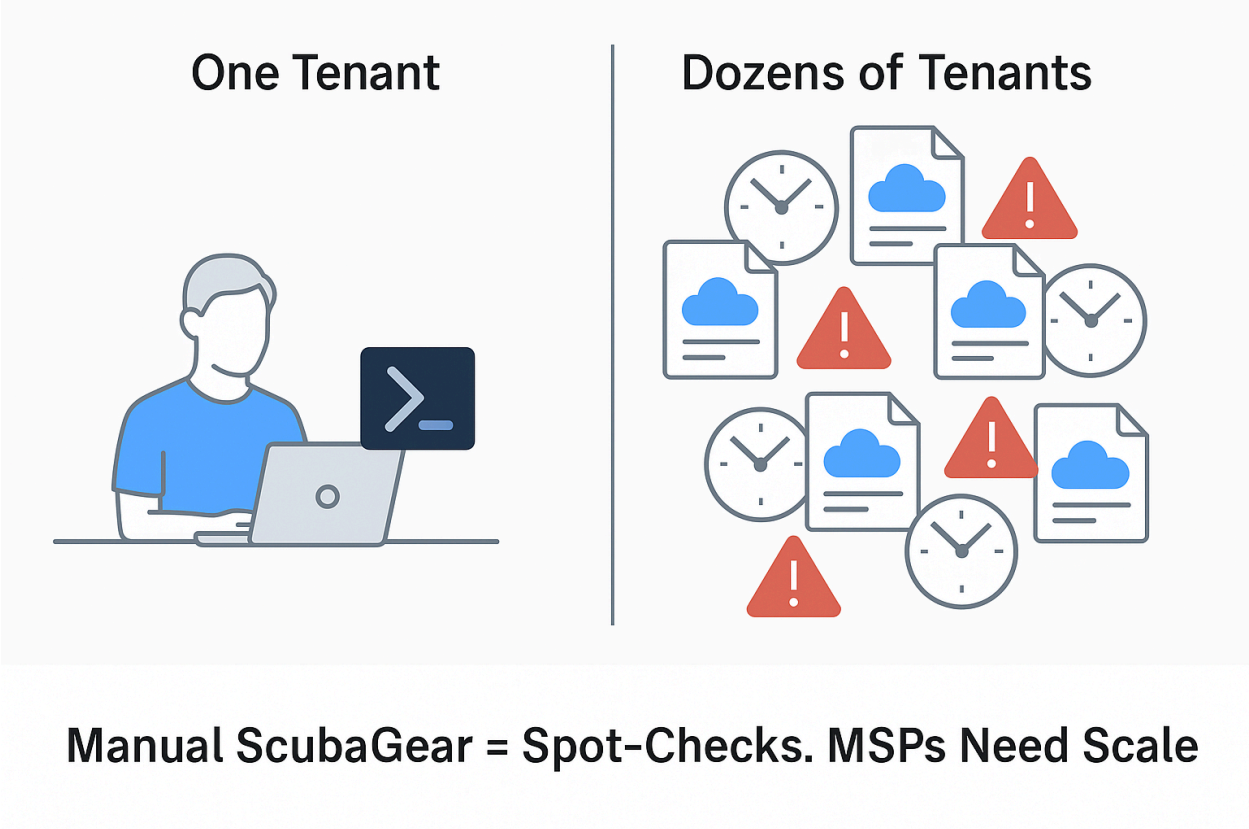


Figure 5: Scaling ScubaGear to work in a multi-tenant MSP environment

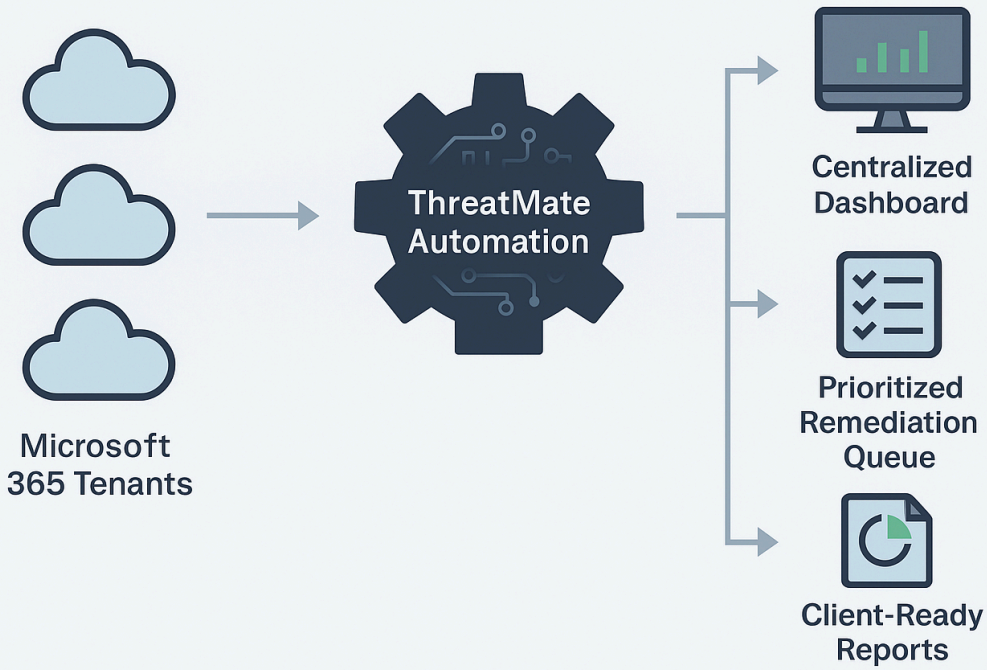
6. Automating Microsoft 365 Baseline with ThreatMate

ScubaGear provides MSPs with the clearest, most defensible baseline yet for securing Microsoft 365 tenants. But on its own, it is still a tactical tool, ie., one that requires manual execution, fragmented reporting, and significant effort to scale across a customer base.

This is where ThreatMate comes in.

ThreatMate is built to operationalize ScubaGear for MSPs, transforming a valuable one-off assessment into a scalable, repeatable, and profitable security service.

Figure 6: ThreatMate Operational Workflow



6.1 Continuous, Automated Assessments

Instead of manually running PowerShell scripts across dozens of tenants, ThreatMate automatically executes ScubaGear assessments on a scheduled basis. Results are collected without technician intervention, ensuring continuous monitoring rather than sporadic spot-checks.

6.2 Centralized Multi-Tenant Visibility

All assessment results are aggregated into a single pane of glass across all Microsoft cloud tenants. MSPs can see:

- Which tenants are aligned with the baseline.
- Which controls have failed across all clients.
- Which issues are recurring or trending.

This centralization eliminates the sprawl of disconnected reports and gives MSPs an "at-a-glance" view of their overall Microsoft 365 security posture.

6.3 Drift Tracking Over Time

ThreatMate does not just provide a snapshot. It tracks configuration changes over time. If a tenant drifts out of alignment because an admin enables legacy auth or disables logging, ThreatMate flags it. MSPs can then take proactive action before an attacker exploits the gap.

6.4 Prioritized Remediation Workflows

Failed controls are not just listed; they are prioritized based on security impact and ease of remediation. ThreatMate integrates directly into MSP workflows, generating clear action items for technicians and mapping them into ticketing systems like ConnectWise or Kaseya. This reduces noise and ensures effort is focused where it matters most.

6.5 Client-Ready Reporting

MSPs often struggle to prove value to clients. ThreatMate solves this by producing reports that:

- Show current baseline scores.
- Highlight improvements over time.
- Demonstrate alignment with a federal cybersecurity standard (CISA ScubaGear).

These reports become powerful assets in QBRs, compliance reviews, and sales conversations that can position the MSP as a proactive security partner rather than a reactive IT provider.

6.6 Building a Defensible Security Service

With ThreatMate, MSPs can finally deliver a Microsoft 365 security service that is:

- **Standardized:** All clients aligned to the same CISA baseline.
- **Scalable:** Automated assessments across dozens or hundreds of tenants.

- **Defensible:** Based on U.S. federal guidance, not subjective “best practices.”
- **Profitable:** Minimal manual labor, built into recurring service packages.

6.7 The Competitive Advantage

In a crowded MSP market, differentiation matters. By offering automated Microsoft 365 baseline enforcement with ThreatMate, providers can:

- Win trust with prospects by citing CISA-backed standards.
- Reduce operational overhead while delivering more consistent security outcomes.
- Command higher margins for a service that proves its value with every report.

6.8 Final Thought

Microsoft 365 will remain a top target for attackers. ScubaGear gives MSPs the framework to defend it; ThreatMate gives them the means to operationalize that framework at scale. Together, they enable MSPs to move beyond reactive firefighting into proactive, defensible cybersecurity service delivery at scale. Left of boom, right on the money.