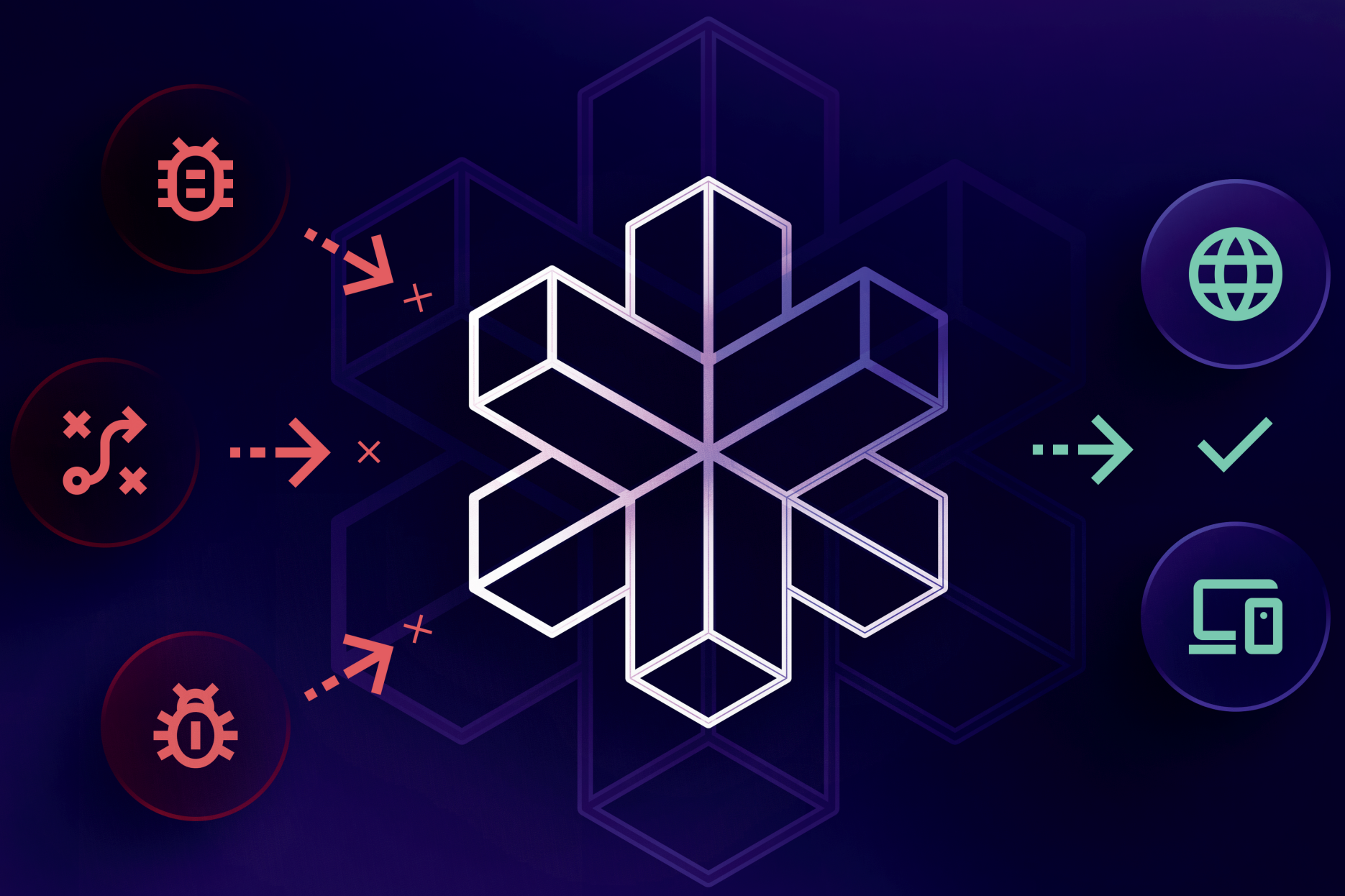
timus SASE

How MSPs Use Timus SASE to Solve Their Biggest Challenges



Common Security Challenges for MSPs

Timus SASE for Cloud Perimeter Protection

Purpose-built SASE for MSPs serving SMB and mid-market clients.

timus SASE

Who is Timus Built For?

Your three biggest challenges — solved through one scalable platform.

MSPs

Purpose-built by network security experts to give MSPs unmatched protection for SMB and mid-market clients.

Mid-market

With users and data everywhere, MSPs face tougher challenges and clients expect seamless security.

SMBs

Timus helps you take back control, gain full visibility and secure your environment. All from a single, easy-to-deploy platform.

Seamless Security

Centralized Control

Actionable Insights

timus SASE

Challenge

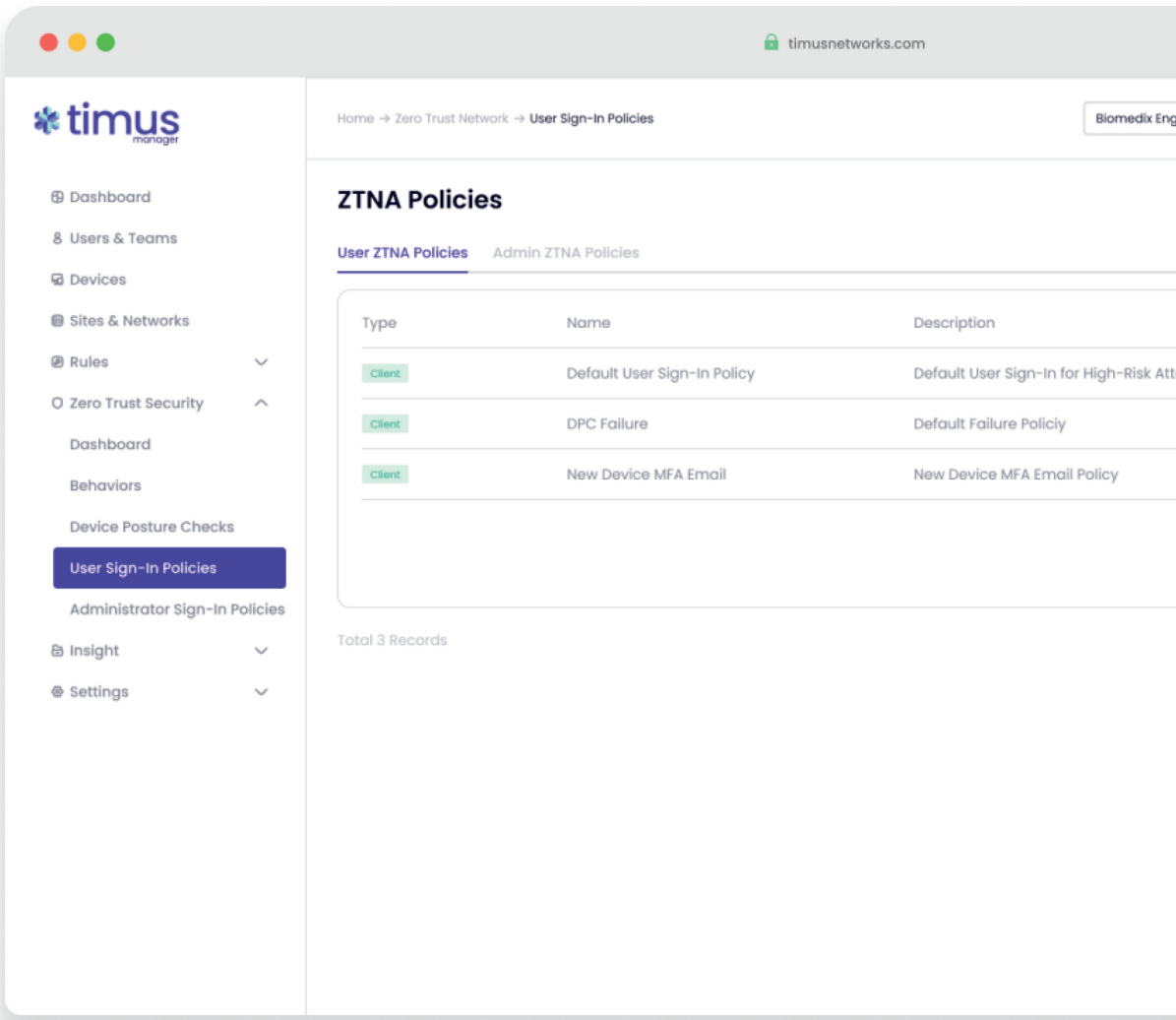
“How do I keep users secure anywhere, anytime?”

Solution

Always-On Zero Trust Network Access

Legacy VPNs are clunky, inconsistent and leave security gaps.. Timus replaces them with passwordless, always-on ZTNA — secure access, everywhere.

- Always-on agent — no drops, no toggles
- Identity-first, context-aware access
- Dedicated static IPs for allowlisting
- Device posture checks and geolocation blocks
- Built-in secure web gateway with SSL inspection



How MSPs lock down PaaS access for software developers

One of our partner’s clients needed to ensure that only verified team members could access their PaaS tool. The MSP used Timus’s static private IP to allowlist and secure access to the client’s environment.

Now, even if credentials are stolen, only users who pass Timus’ zero trust verification can get in.

timus SASE

Challenge

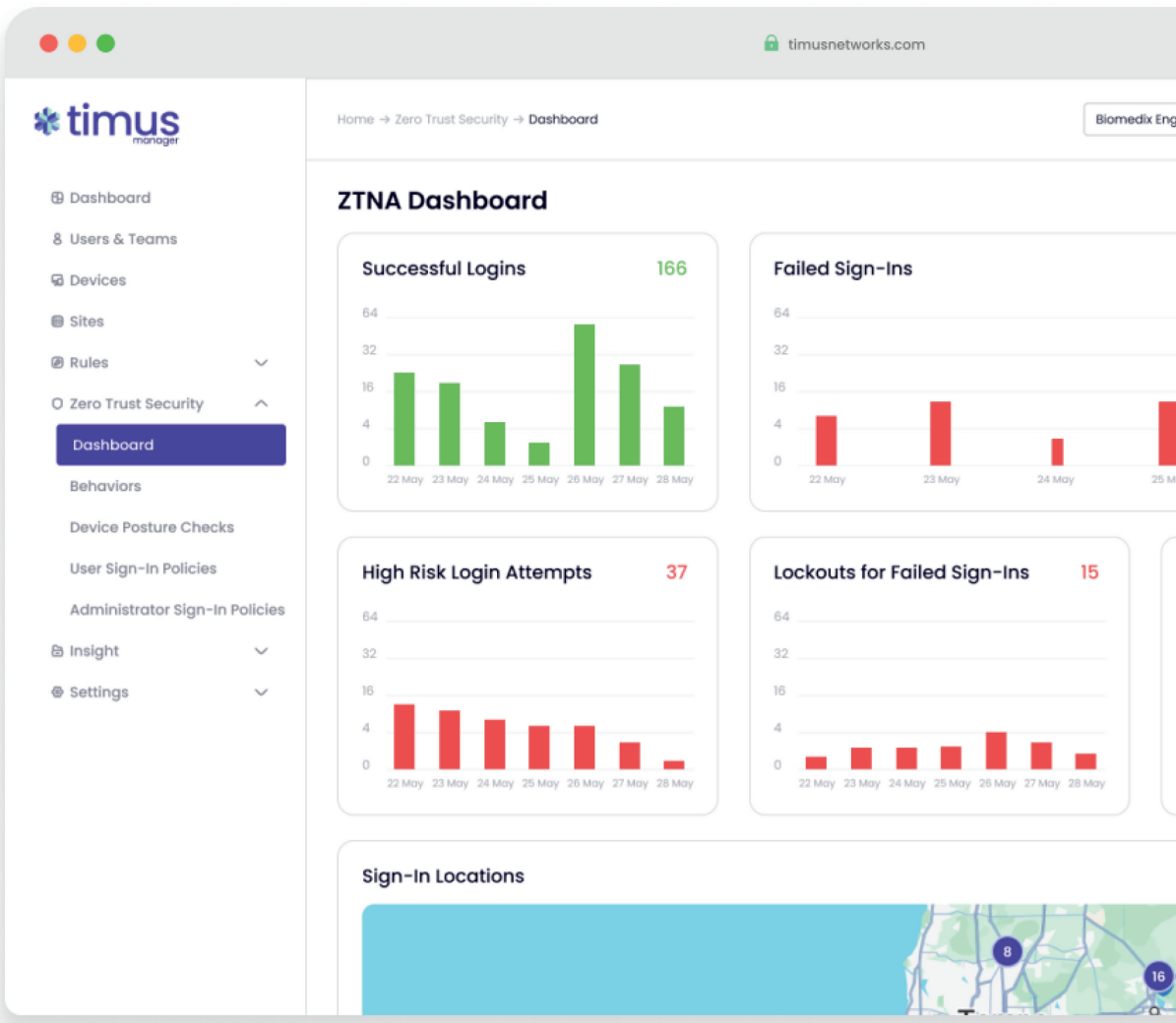
“I can’t see or control what users are doing.”

Solution

One Pane of Glass for Total Control

Security shouldn’t suffer in hybrid environments. Timus gives you centralized, policy-based control over every user, device, and application — all in one place.

- Real-time posture checks and EPP integrations
- Dynamic tagging adjusts access automatically based on context.
- Role and risk-based policy enforcement
- Full client visibility via Partner Portal



Smarter access policies for hybrid users

A client’s hybrid workforce used both personal and company-issued devices. The MSP used Timus to enforce dynamic device posture checks to ensure only secure, compliant devices could connect while maintaining full accessibility.

Now the client enjoys seamless access without compromising security, reducing risk across every device.

timus SASE

Challenge

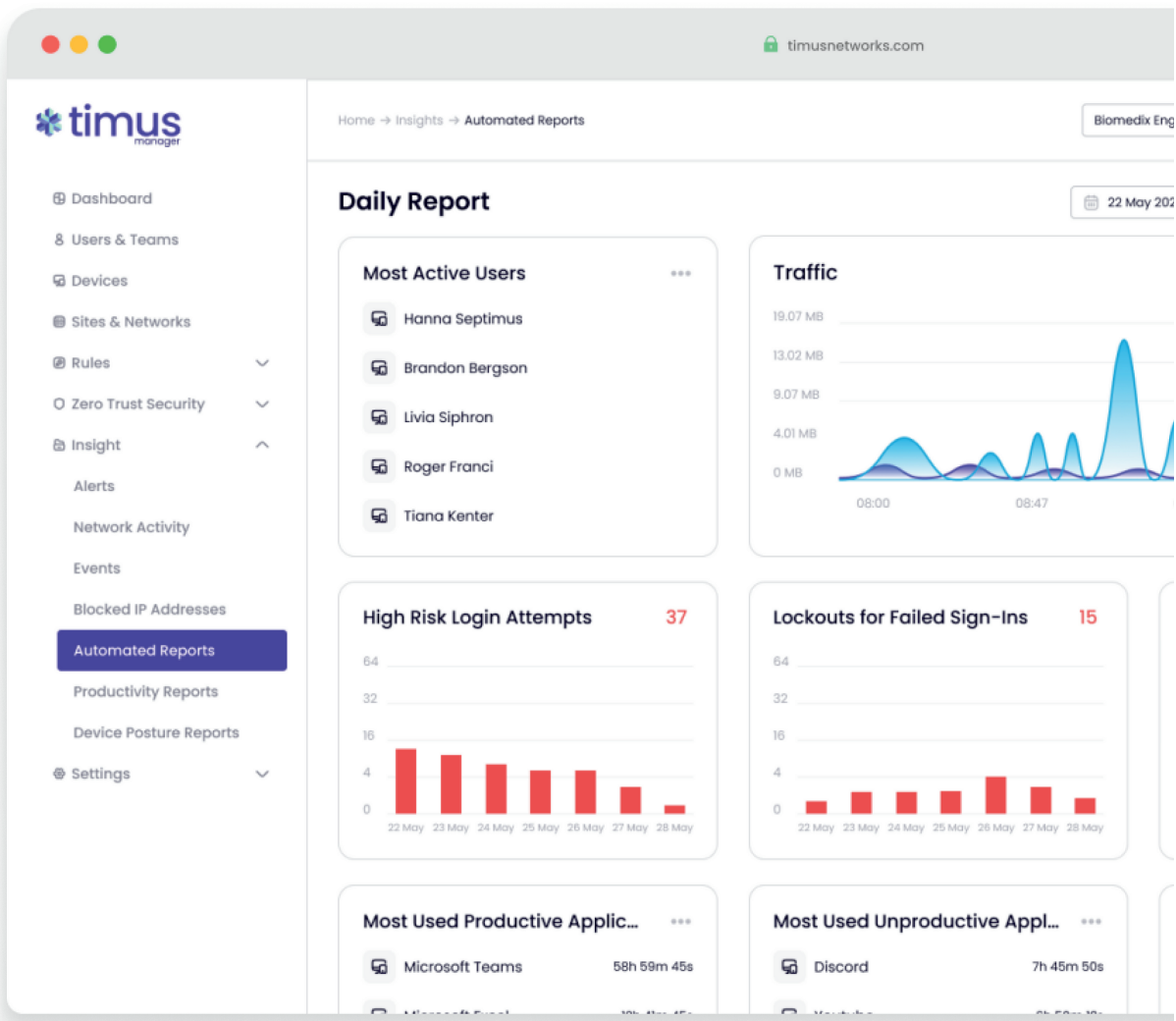
“I don’t have the visibility I need to protect my clients effectively.”

Solution

Actionable Insights without the Noise

Timus gives MSPs real-time visibility without alert fatigue. See threats, usage, and trends across every client environment.

- Live access and threat logs to quickly identify and respond to incidents
- Compliance-ready exports (SOC2, HIPAA) to simplify audits and reporting
- Productivity tracking for hybrid teams
- SLA-friendly reporting for building client confidence



MSP diagnosed a connectivity issue in minutes using Timus reports, exceeding SLA expectations.

Another partner leveraged productivity reports to justify new endpoint investments and deepen client trust.

MSPs turn data into decisions that improve security, efficiency, and client satisfaction with Timus.

timus SASE

How Does Timus Help Your MSP?

- Protect users with seamless Zero Trust Network Access
- Enforce smarter access and device control for every environment
- Turn insights into action and show measurable proof of value

Why MSPs Choose Timus

<30
Minutes to Deploy

30%
Fewer Support Tickets

≤70%
IT Budget Saving

That kind of attention is rare. You feel like they're invested in your success, not just your subscription.

Tyler Baker CEO of Northrock Systems

Ready to Simplify Security?

Scan to book your 30-Minute Demo today!