timus SASE

Adaptive Zero Trust

Continuous Protection. Zero Assumptions.

Static security assumes trust once granted. But in today's dynamic networks, trust must evolve as fast as conditions do. Timus Adaptive Zero Trust continuously validates every session — at sign-in, before connection, during use, and as behavior changes.
It unifies identity, posture, and activity into one adaptive risk engine that responds instantly to shifting threats.

Sign-In

Connect

In-Session

Response

Phase	Purpose	Adaptive Controls
Sign-In	Validate user identity and behavioral context.	New device, new geo-location, impossible travel, IP reputation, breached email checks.
Access	Confirm compliance before connection.	EDR status, AV, firewall, encryption, OS version, infection.
In-Session	Continuously assess device posture and user activity.	Detects drift, posture changes, IP shifts, or AV disabled mid-session.
Automated Response	Enforce policy actions automatically.	Force to re-authenticate; kill the session, trigger the MFA, quarantine, create alert, send webhooks.

Use Cases

For Technical Teams

- Replace static ZTNA policies with live, adaptive risk models.
- Gain one console for identity, posture, and behavioral controls.
- Automate enforcement, no waiting for tickets.
- Deliver real-time protection without performance impact.

Every detection and response is visible in Insights → Events, giving MSPs a live audit trail.

Microsoft Defender   Heimdal®   Bitdefender   SentinelOne®

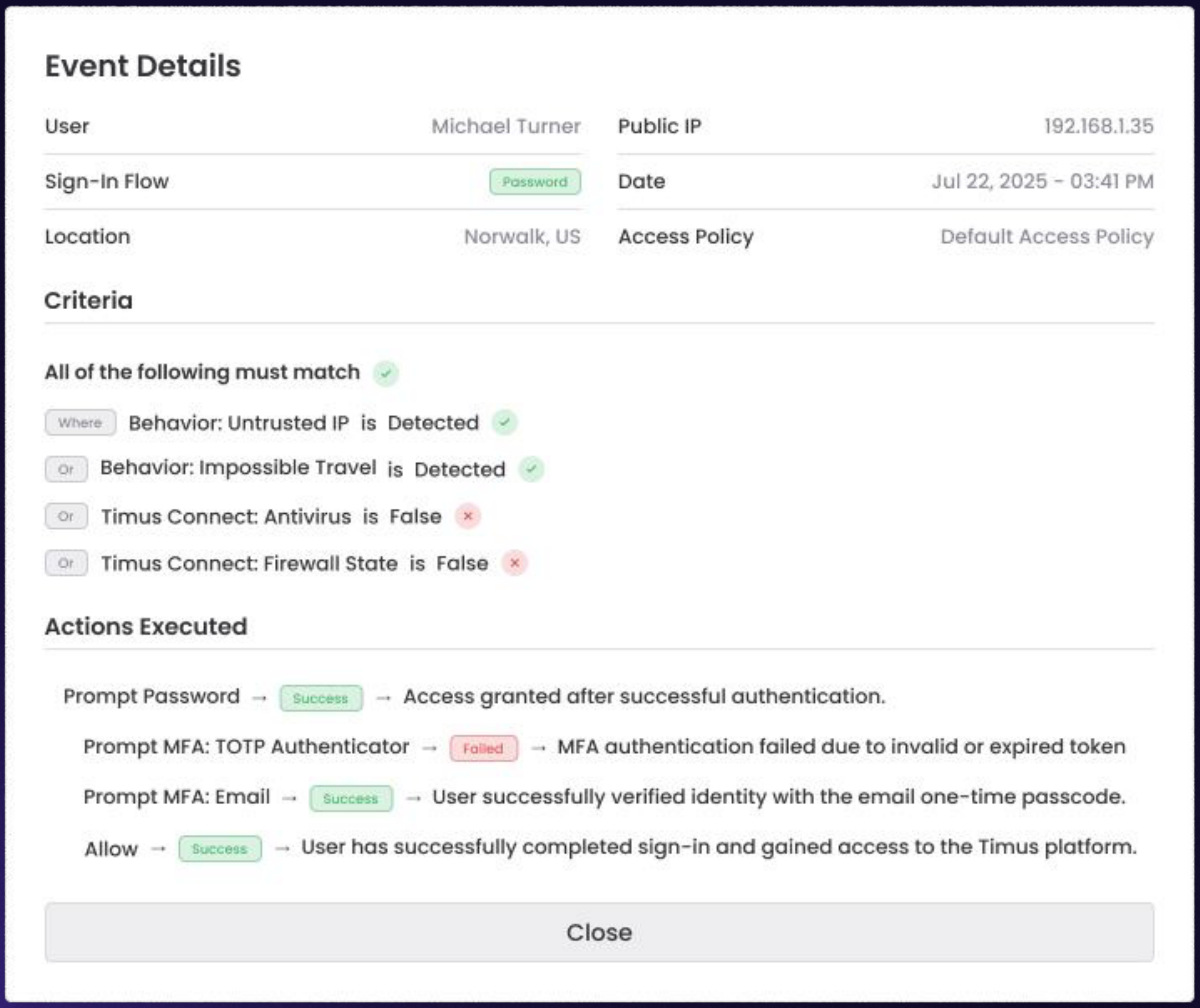
Security that thinks for the MSPs.

Adaptive Zero Trust takes the complexity out of Zero Trust management — reducing tickets, simplifying compliance, and delivering continuous protection to every client.

Area	MSP Value	How?
Continuous Protection	Real-time awareness of user, device, and behavior changes.	Detects posture drift, geo-anomalies, or risky signals mid-session and reacts instantly.
Simplified Operations	Manage dozens of clients from one unified policy set.	Multi-tenant control plane enforces adaptive policies automatically across all tenants.
Fewer Tickets	Prevents misconfigurations before they reach support.	Posture checks catch disabled AV or missing encryption before every connection.
Compliance Visibility	Always-on audit trails for every action.	Every policy action is logged. Evidence for HIPAA, FINRA, SOC 2, and cyber insurance reports generated automatically.
Revenue Growth	Adds measurable value to security service tiers.	Partners can package Adaptive Zero Trust as part of a "premium protection" offering.
Client Trust	Demonstrable, real-time protection.	Adaptive events are visible and provable during QBRs or audits — not just promised.

Why MSPs Needed This

Adaptive Zero Trust ensures that every connection is verified, every device stays compliant,
and every session remains trusted — automatically.



Event Details

User	Michael Turner	Public IP	192.168.1.35
Sign-In Flow	Password	Date	Jul 22, 2025 - 03:41 PM
Location	Norwalk, US	Access Policy	Default Access Policy

Criteria

All of the following must match ✓

Where Behavior: Untrusted IP is Detected ✓

Or Behavior: Impossible Travel is Detected ✓

Or Timus Connect: Antivirus is False ×

Or Timus Connect: Firewall State is False ×

Actions Executed

Prompt Password → Success → Access granted after successful authentication.

Prompt MFA: TOTP Authenticator → Failed → MFA authentication failed due to invalid or expired token

Prompt MFA: Email → Success → User successfully verified identity with the email one-time passcode.

Allow → Success → User has successfully completed sign-in and gained access to the Timus platform.

Always Aware. Always Secure. Adaptive Zero Trust