PONDURANCE

SOLUTION GUIDE

Pondurance MDR for Microsoft for Mid-Market Organizations

A Solutions Overview for Hybrid Environments, Regulated Industries, and High-Risk Microsoft Ecosystems

Attackers go where payoff is high and defenses are thin—and mid-market organizations running Microsoft-centric environments are prime targets. These organizations handle large volumes of regulated data (PII/PHI) — yet must defend complex Microsoft 365, Entra ID/Azure AD, Active Directory, and hybrid cloud systems with limited budgets, lean IT teams, and little to no dedicated SOC support.

This imbalance fuels identity compromises, ransomware precursors, BEC attacks, and collaboration-tool exploits. Legacy on-prem systems, hybrid Active Directory, and insufficient Microsoft 365 configuration hardening create pathways for attacker persistence and lateral movement.

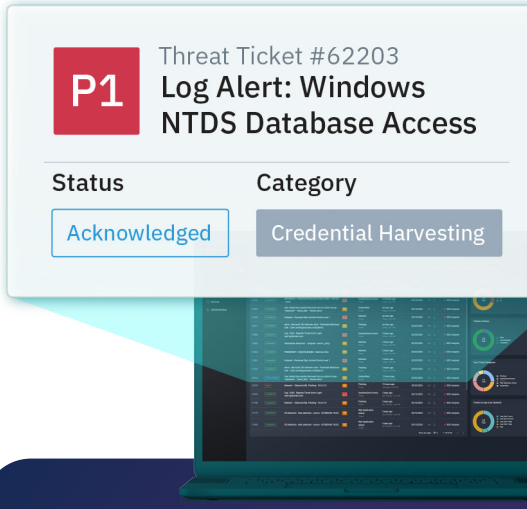
Pondurance delivers MDR designed for these realities. We provide deep Microsoft-native detection, hands-on response actions, hybrid visibility across cloud and on-prem workloads, and proactive reduction of attack surface through Microsoft 365 configuration hardening.

Unlike MDR providers who only pass back alerts and leave the burden on internal teams, Pondurance combines telemetry-agnostic data collection, Microsoft Graph integrations, STIG-based configuration auditing, on-prem log collection, and 24/7 U.S.-based analysts who can take direct action to reduce breach impact in real time.

The Modern Microsoft-Centric Threat Landscape

Microsoft-based environments are now the dominant target for attackers due to their ubiquity in mid-market organizations and the interconnectivity of their solutions. Microsoft 365, Entra ID, and hybrid AD environments provide identity and collaboration capabilities that, when misconfigured or overlooked, become high-value opportunities for attackers. Threat actors exploit:

- Business email compromise via mailbox takeover or manipulation, MFA bypass, token theft, etc.
- Teams and SharePoint attacks including message injection, impersonation, and malicious file delivery. Recent threat operations have begun to leverage Teams to trick other users into becoming part of the attack.
- Hybrid Active Directory weaknesses such as old protocols, weak legacy policies, outdated forms of Active Directory, etc.



PONDURANCE MDR DELIVERS

- ✓ Deep Microsoft-native detection
- ✓ Hands-on response actions
- ✓ Hybrid visibility across cloud and on-prem workloads
- ✓ Proactive reduction of attack surface through Microsoft 365 configuration hardening

PROACTIVE MANAGED RESPONSE CAPABILITIES

When an attack occurs, we can jump into action to immediately:

- Reset sessions
- Lock compromised accounts
- Contain endpoints
- Identify and eliminate malicious mailbox rules before they can be exploited

©2025 Copyright Pondurance, Inc. All Rights Reserved

- OAuth grant abuse through malicious “add-ons” and extensions.
- Endpoint (and server) compromises that expand into cloud sessions, mailbox manipulation, and data exfiltration.

Microsoft & the Mid-Market

Microsoft tools generate rich telemetry—but require expertise, tuning, and constant monitoring to be effective. They assume the presence of a skilled, well-staffed security team capable of triage, correlation, and active response — without which it is difficult to operationalize Microsoft’s security capabilities. Mid-market organizations rarely have this capacity internally — making MDR a necessity rather than a luxury for the mid-market.

> *“Microsoft tools generate rich telemetry—but require expertise, tuning, and constant monitoring to be effective.*

Unique Challenges to Mid-Market Microsoft Environments

Limited budgets
for SIEM, SOAR, or Microsoft E5 licensing

Lack Specialized Staff
IT staff must juggle too much without expertise

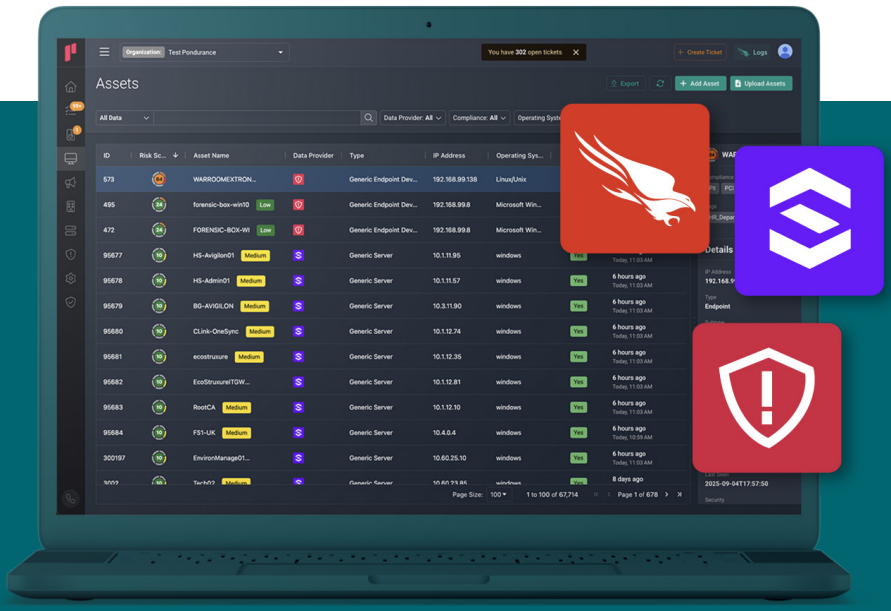
No Dedicated SOC
Lack active threat hunting & incident response

Hybrid Architecture
Complex combo of cloud, on-prem, and legacy systems

Regulatory Pressure
Crushing state, federal, & cyber insurer demands

POTENTIAL GAPS IN MICROSOFT-FIRST SECURITY ARCHITECTURES

- Misconfigured tenants, including risky mailflow and authentication settings — often to accommodate legacy applications
- Lack of 24/7 monitoring for identity anomalies, session hijacking, or MFA fatigue attacks
- Limited visibility into Teams and SharePoint threats due to complex event patterns
- No centralized correlation between endpoint, identity, network, and cloud logs
- Relevant alerts marked as ‘informational’ by Microsoft, leading to missed red flags



Why Pondurance is Different

Competitors often provide only cloud log monitoring or rely solely on Microsoft Graph API signals. Without hybrid visibility—including for on-premises infrastructure, AD, VPN, and legacy systems—attackers often lurk undetected long before pivoting to Microsoft 365. Pondurance fills this gap by monitoring the entire attack chain from on-premises, to cloud, to identity across AD and Entra ID.

 ©2025 Copyright Pondurance, Inc. All Rights Reseved

Pondurance MDR for Microsoft-Centric Environments

Pondurance MDR includes solutions engineered specifically to provide an elevated security posture for hybrid Microsoft environments, providing Microsoft-native detection, proactive hardening, and hands-on response that aligns with attacker behavior.

Proactive Hardening of Microsoft 365

Pondurance's Microsoft 365 Configuration Audit reduces attack surfaces before adversaries exploit it. Using DHS ScubaGear and other tools and methodologies, Pondurance benchmarks your M365 tenancy against security best practices and identifies misconfigurations that commonly lead to BEC and credential compromise.

CAPABILITIES

- Assessing authentication, conditional access, mailflow, and privilege configurations.
- Detecting suspicious inbox rules, forwarding policies, or permission anomalies.
- Identifying foreign logins, risky ISPs, TOR nodes, and anomalous user-agents.
- Tailored remediation roadmap with prioritized fixes.
- Optional validation to confirm changes have been implemented.

CORE CAPABILITIES

- ✓ Native Microsoft Graph API integration for M365, Entra ID, Defender XDR.
- ✓ Automated log ingestion from cloud + on-prem systems via collectors and agents.
- ✓ SIEM-grade normalization and enrichment for identity, endpoint, and collaboration activity.
- ✓ 24/7 SOC with analysts trained in Microsoft attack chains.
- ✓ Direct response actions including session resets, password resets, and device containment through Defender XDR and 3rd-party tools.
- ✓ Integrated digital forensics and incident response (DFIR) support for validated incidents.

Microsoft 365 + Entra ID Threat Detection & Response

Pondurance's cloud-native log collector integrates directly with the Microsoft Graph API to ingest M365 and Entra ID signals without requiring hardware or VPN connections. Once collected, logs enter the Pondurance MDR platform for advanced analytics, correlation, and threat scoring.

KEY RESPONSE CAPABILITIES

- Terminating suspicious active sessions in Entra ID.
- Resetting user passwords and requiring re-authentication.
- Removing malicious mailbox rules or OAuth grants.
- Quarantining or containing endpoints through Defender XDR and 3rd-party tools.
- Automatic enforcement of response playbooks with pre-approved customer authorization.

Hybrid Visibility and Threat Correlation

Not cloud-only? If you rely on on-prem Windows systems, legacy applications, medical/OT devices, and/or secure network infrastructure, Pondurance provides full-stack visibility by collecting:

- Windows event logs, domain controller logs, Linux and other logs.
- Firewall, VPN, and proxy logs for ingress/egress correlation.
- Logs from legacy systems and critical operational technologies.

This enables Pondurance analysts to detect attack paths that move from on-prem to the cloud—something cloud-only MDR providers cannot recognize as quickly when time to respond is a key metric.

 ©2025 Copyright Pondurance, Inc. All Rights Reserved

INCIDENT RESPONSE ASSURANCE

With our DFIR Assurance Guarantee you'll get immediate access to the world-class Pondurance DFIR team — with up to $2M of uninsured breach investigation costs covered in the event of a qualifying compromise.

Why Pondurance

Pondurance provides a unique combination of affordability, hybrid visibility, Microsoft expertise, hands-on response, and regulated-industry knowledge. For mid-market organizations with limited budgets and limited security staff, Pondurance MDR is unparalleled as a practical and effective path to reducing breach risk.

BUSINESS VALUE FOR MID-MARKET MICROSOFT ORGANIZATIONS

- 24/7 SOC coverage without hiring internal staff.
- Faster containment of on-prem and cloud-based threats.
- Proactive reduction of Microsoft 365 attack surface.
- SIEM-level visibility across cloud + on-prem without SIEM management overhead.
- Audit readiness for HIPAA, PCI, FERPA, SEC, and cyber insurance.
- Reduced probability and impact of breaches, ransomware, and BEC.

Up to 80%
Lower Breach Risks

4.8/5
Gartner Peer Reviews

3x
More cyberattacks disrupted

See Pondurance in action

Get a free, personalized demo to see how Pondurance can help you eliminate breach risks

Request a demo at:
pondurance.com/get-a-demo



PONDURANCE

ELIMINATE BREACH RISK

Pondurance was founded to give mid-market organizations the same level of protection as large enterprises. From day one, our mission has been to eliminate breach risks by making world-class cybersecurity and managed security services accessible.

 ©2025 Copyright Pondurance, Inc. All Rights Reserved