FrontierZero

FrontierZero vs Microsoft Defender

Quick-Glance Comparison

Executive Summary

The enterprise software landscape has expanded rapidly, with organizations now managing an average of over 300 applications across their ecosystem. As business units independently adopt specialized software, identity security has become the primary battleground for corporate defense. Today, malicious actors rarely "hack" their way into networks through traditional technical exploits; instead, they leverage leaked dark web credentials to simply log directly into unprotected applications.

While Microsoft Defender offers stellar security posture management within its native environment, it is inherently designed to protect the Microsoft suite alone. This leaves a dangerous visibility gap regarding standalone custom software, shadow AI platforms, and decentralized applications bought via credit cards outside of IT control. FrontierZero acts as a complementary, agentless "identity X-ray" layer that bridges this gap, unifying your security architecture across all platforms while simultaneously identifying major software licensing waste.

Key Strategic Insights & Data Points

- **The Vulnerability of External Access:** Approximately 60% of data breaches involve third-party vendors or contractors, and 71% of organizations experience at least one identity-related incident annually. Despite this risk, 96% of companies do not actively monitor suppliers who have direct access to their data. This specific blind spot has historically led to massive operational disruptions, such as Jaguar Land Rover's £1.9B economic impact and subsequent 6-week global production shutdown.
- **Severe Lifecycle Gaps:** Standard IT off-boarding checklists are highly effective at disabling core directories like Microsoft 365, but 92% of surveyed companies fail to track departing employees or contractors who retain active, persistent logins on decentralized line-of-business applications.
- **The Cost of Exposure vs. ROI:** With the global average cost of a data breach soaring to $4.4M ($183 per individual compromised record), corporate security is a critical financial priority. FrontierZero addresses this with a dual-value proposition: it hardens identity tracking while actively locating underutilized software licenses, routinely saving organizations up to 40% on their existing SaaS budget.
- **Rapid Shadow AI Control:** As teams rapidly adopt unauthorized AI extensions and tools (such as DeepSeek or free versions of ChatGPT), sensitive corporate data faces immediate exposure risks. FrontierZero establishes an anomaly-detecting "Pattern of Life" for every internal and external user identity, deploying completely agentless connectivity within 15 minutes to flag abnormal data movements without requiring local device installations.

Feature Comparison Matrix

Capability / Feature	FrontierZero (FZ)	Microsoft Defender / M365 Security	Critical Business Gap Addressed
Primary Core Focus	Identity-centric visibility across the entire internal, external, and multi-SaaS landscape.	Endpoint and configuration posture management strictly within the Microsoft environment.	**The Non-Microsoft Blind Spot:** Protects the "Microsoft world," but leaves external business apps unmonitored.
Identity Enrichment & Context	Pulls and cross-correlates log files from Salesforce, AWS, SAP, etc., to map a "Pattern of Life".	Provides standard, siloed sign-in logs restricted exclusively to Microsoft applications.	**Siloed Logs:** Failing to see that a compromised password on Microsoft is still active on an unlinked app.
Third-Party Access Tracking	Segments external users, groups them by vendor/contractor company, and audits vendor domains.	Automatically creates un-audited guest accounts in the active directory during file/Teams sharing.	**Supply Chain Breaches:** Overlooking third-party supplier access, which led to the JLR and Qantas breaches.
Shadow AI & SaaS Discovery	Agentless tracking of decentralized, line-of-business apps bought via credit cards (e.g., DeepSeek, Canva).	Captures native enterprise app registrations but misses independent, user-password logins.	**Shadow AI Sprawl:** Outbound corporate data leaks originating from unauthorized AI tool adoption by teams.
In-House App Integration	Ingests standalone application logs to run behavior analytics and enriches SIEM/SOC platforms.	Relies heavily on SSO, Entra ID, or Active Directory integrations to track user sessions.	**Fragmented Alerts:** Relying on manual application logs and disconnected email alerts sent directly to the SOC.
Time to Value & ROI	**15-minute setup** with zero agents, offering localized compliance (NCA) and up to **40% cost savings**.	Extended enterprise deployment timelines; focuses on posture metrics rather than cost optimization.	**CFO Alignment:** Security tools typically represent a pure cost, whereas FZ offsets its cost by cutting licensing waste.

Detailed Capability Breakdown

Non-Microsoft Product Visibility & Identity Enrichment

- **FrontierZero Unique Approach:** Agentless connectivity pulls and enriches identity logs across your entire multi-SaaS ecosystem, including Salesforce, AWS, and SAP. By cross-correlating these disjointed log files, it builds a cohesive "Pattern of Life" to catch critical security blind spots—such as an employee updating their primary Microsoft password after a breach but leaving a leaked, unconfigured password active on a peripheral app like HubSpot.
- **Microsoft Defender Limitations:** Monitors the native Microsoft environment exceptionally well but is inherently limited to that ecosystem. Its standard sign-in logs lack cross-application context, leaving it blind to identity risks occurring inside non-Microsoft environments that aren't natively connected via SSO.
- **The Reality:** Many organizations fall into a false sense of security believing Microsoft covers their entire footprint. This leaves massive blind spots in independent, department-bought business applications where hackers can use dark web credentials to simply log in undetected.

Standalone & In-House Application Integration

- **FrontierZero Unique Approach:** Ingests standalone and in-house application logs—such as custom-built internal corporate platforms—directly into its threat detection engine. It normalizes this standalone data to run user behavior analytics and seamlessly feeds these enriched alerts directly into your central SIEM or SOC (like Microsoft Sentinel or Splunk) to maximize threat detection accuracy.
- **Microsoft Defender Limitations:** Relies heavily on Entra ID, Active Directory, or standard single sign-on (SSO) configurations. For standalone or custom in-house applications that do not support these modern integration protocols, Microsoft tools cannot natively track or monitor individual user sessions.
- **The Reality:** Custom in-house systems routinely handle proprietary data but slip under the radar of enterprise security perimeters. This forces security teams to rely on local application logs, manual audits, and fragmented email alerts sent to the SOC.

Off-boarding and Lifecycle Management

- **FrontierZero Unique Approach:** Agentless discovery scans beyond the standard IT directory to automatically find decentralized, line-of-business (LoB) software bought via credit cards (e.g., Canva, DeepSeek, Notion, or project management platforms). It continuously flags ex-employees and third-party contractors who retain active sessions across these peripheral systems long after their primary corporate accounts are closed.
- **Microsoft Defender Limitations:** Successfully cuts off access to the core M365 suite and SSO-connected corporate infrastructure during off-boarding, but has no mechanism to trace or clean up standalone accounts created on business-owned SaaS platforms outside IT control.
- **The Reality:** Standard IT off-boarding checklists successfully disable Microsoft 365, but miss dozens of business-owned SaaS applications where departing employees or un-audited vendor guest accounts maintain persistent, live access to corporate data.