OpenText Behavioral Signals with Microsoft Defender for Endpoint

Swiftly reveal hidden and unknown threats, including insiders and advanced persistent threats (APTs)



At a glance

- Advanced insider threat, novel attack, and APT detection
- Continuous attack surface visibility and detection
- Actionable leads distilled from billions of events
- Risk aggregation for low-and-slow attack detection
- Enhanced value from your Microsoft Defender for Endpoint data

Defending an organization from attacks is expensive, time consuming, and exhausting. While the attacker needs to only be right once, defenders need to be right 24/7. Because of this, defenders must have the right tools to catch threats before damage can be done. User Entity Behavior Analytics (UEBA) is one of these tools.

OpenText™ Behavioral Signals, a UEBA solution, uses machine learning to identify “normal” behavior for entities (users, servers, endpoints, etc.) in an organization, finding and alerting threat hunters when anomalies are detected. Where traditional rules, thresholds, and pattern matching techniques are adept at catching known threats, Intelligence is adept at catching unknown threats.

Behavioral Signals provides context-rich leads, allowing threat hunters to focus less on hypotheses-based hunting and more on detecting and preventing attacks. Behavioral Signals also improves your overall SOC efficiency.

Unlike other tools, which require frequent updating of rules and thresholds to remain relevant and reduce false positives, Behavioral Signals automatically adapts and evolves with your changing organization.

Case study: Preventing layoff data exfiltration

During a round of layoffs a Behavioral Signals customer wanted to ensure outgoing employees were not walking off with company secrets. Using Behavioral Signals with EDR data, the customer detected an employee logging in outside of their normal working hours and attempting to transfer 4,000-plus files to a removable device.

When confronted about the files, the employee assured the security team that his actions were not malicious and promised not to transfer files again. Less than a week later, the employee increased their risk score by running an application that had never been run and then attempting to move more than 800 GB of data to a removable drive. This prompted the security team to take further action.

Despite a change in attack vectors and an attempt to hide their real intent, Behavioral Signals was able to detect the employee's anomalous behavior, raise their risk score, and provide the contextual evidence needed to prevent further damage.

Essential to advancing Defender's security

Behavioral Signals effectively detects insider threats, novel attacks, and APTs by repurposing the rich telemetry that is already being produced by the Microsoft Defender endpoints in your enterprise.

Microsoft Defender for Endpoint telemetry is especially powerful when used for behavioral analytics since it records events that take place on individual endpoints and across all endpoints in an organization. With Microsoft Defender telemetry, Behavioral Signals can detect attack scenarios such as:

- Data staging/exfiltration
- Unusual uploads/downloads
- Account compromise and misuse
- High risk IP/data access
- Unusual traffic and connections

With just the Microsoft Defender data, Behavioral Signals detects these attack scenarios and provides contextual and relevant insights to threat hunters to help them quickly determine the best way to stop a threat from becoming a major security incident.

With EDR solutions like Microsoft Defender, Behavioral Signals has detected and helped stop attacks including, third-party attacks, nation state attacks, advanced reconnaissance, sensitive file accesses/exfiltration, and password guessing on C-suite accounts.

Microsoft Defender + Microsoft Entra ID with Behavioral Signals

While Behavioral Signals is effective at using Microsoft Defender for Endpoint data to detect threats originating from company-controlled endpoints, an organization's digital footprint and attack surface extends beyond physical hardware and devices. Microsoft Entra ID (Formerly Azure Active Directory) data is an excellent source of telemetry for Behavioral Signals that gives security teams powerful insights into unusual user authentication attempts, cloud, or web application access, and more, which gives security teams powerful insights into unusual user authentication attempts, cloud, or web application access.

When paired together, Microsoft Defender telemetry and Microsoft Entra data complement each other and expand your visibility of relationships between endpoint and cloud entities. Combining endpoint, active directory, and cloud application (Microsoft 365 and SharePoint) data, Behavioral Signals can follow threats as they move between endpoint and cloud, highlighting potentially risky entities faster than with endpoint data alone.

Learn more >

Copyright © 2026 Open Text • 09.26 | 242-000156-001

opentext™