Microsoft Sentinel & Druva: Strengthening Data Security with Seamless SIEM Integration

This partnership takes enterprise security to the next level by enabling organizations to better protect their backup data from emerging cyber threats. Here's how this powerful integration enhances security operations and streamlines workflows.

The challenge

Managing security across complex environments is a growing challenge, especially for organizations working with multiple SIEM platforms, dispersed teams, and critical backup systems. Gaps in synchronization often lead to misaligned workflows, delayed responses, and increased vulnerability to cyber threats like ransomware and data corruption. Consolidating management and maintaining real-time updates are critical for effective security operations.

The solution

Druva's integration with Microsoft Sentinel bridges the gap between backup systems and advanced security workflows, delivering bidirectional synchronization that ensures seamless alignment across platforms. This integration allows businesses to unify management, enhance visibility, and streamline threat detection and response while maintaining existing tools and processes.

Benefits of the integration

- **Centralized Management:** Consolidates multiple Microsoft Sentinel tenants into a single Druva Cloud instance for streamlined operations.
- **Improved Threat Response:** Enables faster detection and automated responses, reducing the impact of potential threats.
- **Regulatory Compliance:** Enhances visibility into backup activities, making it easier to meet audit requirements.
- **Operational Resilience:** Strengthens security without disrupting existing workflows or tools.

The integration

Druva integrates with Microsoft Sentinel to provide seamless bi-directional synchronization, allowing SecOps teams to quarantine compromised snapshots directly from Sentinel. This streamlines threat response, automates workflows, and accelerates recovery, benefiting MSSPs with simplified co-managed SIEM services. Additionally, Druva offers the first Microsoft Security Copilot plugin for data security, leveraging AI to enhance threat detection, reduce investigation time, and improve compliance efforts.

Key features

- **Unified Visibility:** Integrates Druva's backup telemetry with Microsoft Sentinel's workflows, providing a holistic view of security events.
- **Real-Time Updates:** Synchronization ensures incident updates are instantly reflected across platforms, reducing communication gaps.
- **Enhanced Data Monitoring:** Tracks authentication events, password changes, and backup policy modifications directly within Sentinel.
- **Compliance Support:** Simplifies audits with better visibility into backup activities.

Microsoft Sentinel and Druva

Microsoft Sentinel is a cloud-native security information and event management (SIEM) platform that uses built-in AI to analyze large volumes of security log data across an enterprise. Druva's integration with Microsoft Sentinel enables security teams to gain new insights into their backup security and respond to threats faster—all without the need for additional security solutions.This integration empowers businesses to align their backup protection with modern cybersecurity strategies, creating a stronger, more resilient security posture to fend off cyber threats.

Use Case: Faster Threat Detection

- **Challenge:** Threats targeting backup systems can go unnoticed, delaying response times and increasing risk.
- **Solution:** Correlate Druva data with other sources to quickly identify and address threats before they escalate.

Use Case: Streamlined Incident Response

- **Challenge:** Manual incident response processes are time-consuming and prone to errors, slowing down recovery efforts.
- **Solution:** Leverage automated playbooks to respond efficiently to incidents, reducing downtime and human error.

Use Case: Improved Ransomware Defense

- **Challenge:** Ransomware can spread rapidly, compromising critical data before detection.
- **Solution:** Real-time monitoring of data activity enables early detection and neutralization of ransomware attempts.

Use Case: Enhanced SecOps Performance

- **Challenge:** Delays in system isolation tools increase the risk of spreading threats like ransomware.
- **Solution:** SecOps teams quickly quarantine threats, reduce exposure risks, and streamline responses on a unified platform.

druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva, the autonomous data security company, puts data security on autopilot with a 100% SaaS, fully managed platform to secure and recover data from all threats. The Druva Data Security Cloud ensures the availability, confidentiality, and fidelity of data, and provides customers with autonomous protection, rapid incident response, and guaranteed data recovery. The company is trusted by its more than 6,000 customers, including 65 of the Fortune 500, to defend business data in today's ever-connected world. Amidst a rapidly evolving security landscape, Druva offers a $10 million Data Resiliency Guarantee ensuring customer data is protected and secure against every cyber threat. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.