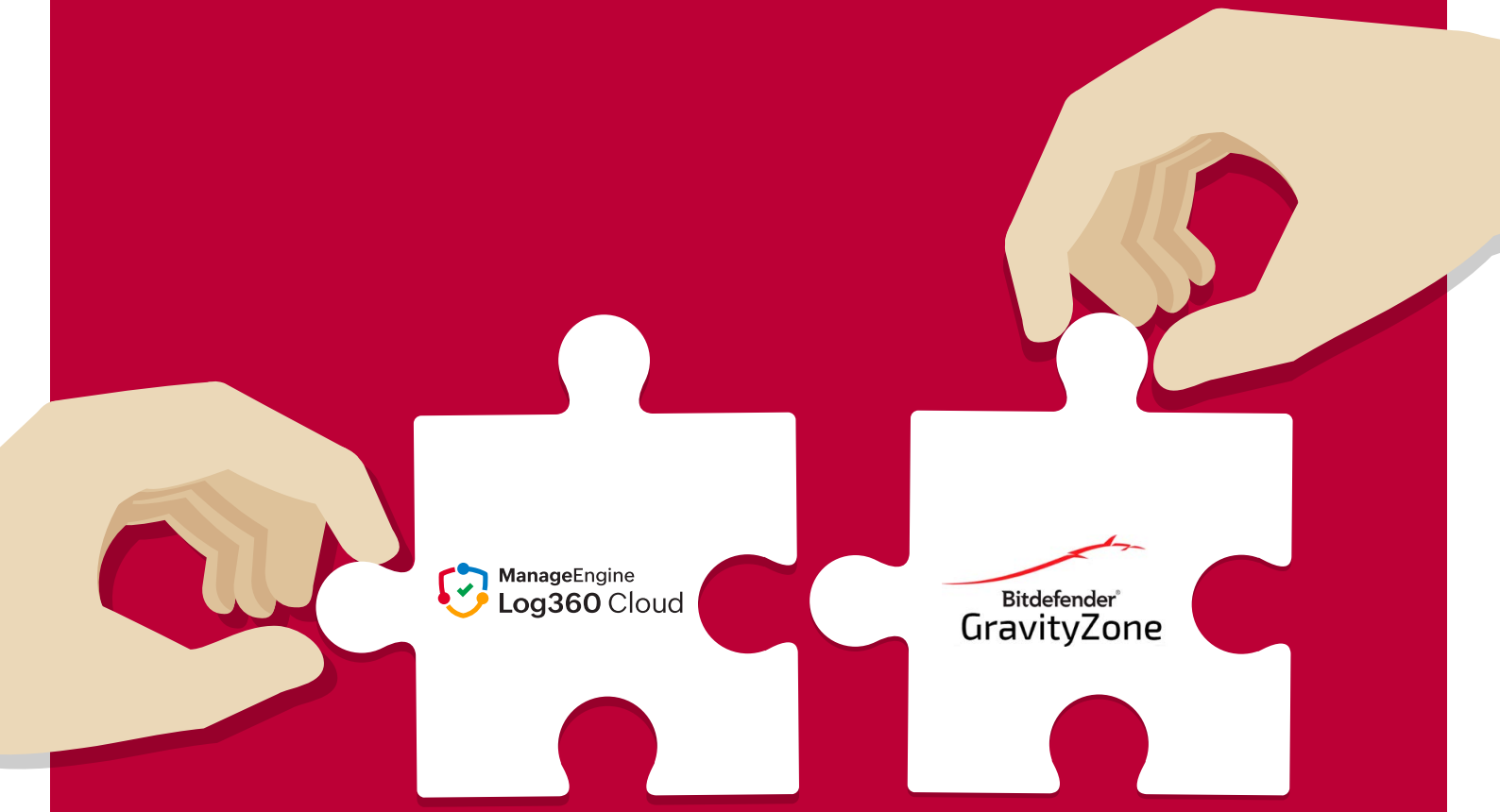
ManageEngine
Log360 Cloud

DATASHEET

Bitdefender GravityZone integration with Log360 Cloud



Overview

Bitdefender GravityZone is an endpoint detection and response (EDR) platform that generates detailed security telemetry across malware, ransomware, network protection, and device control.

The Bitdefender GravityZone integration enables Log360 Cloud to collect EDR logs via syslog and use them for centralized monitoring, correlation, and investigation.

What data is collected

The integration ingests GravityZone EDR logs, including:

Malware and ransomware detections

Network protection and anti-phishing events

Device control and data protection activity

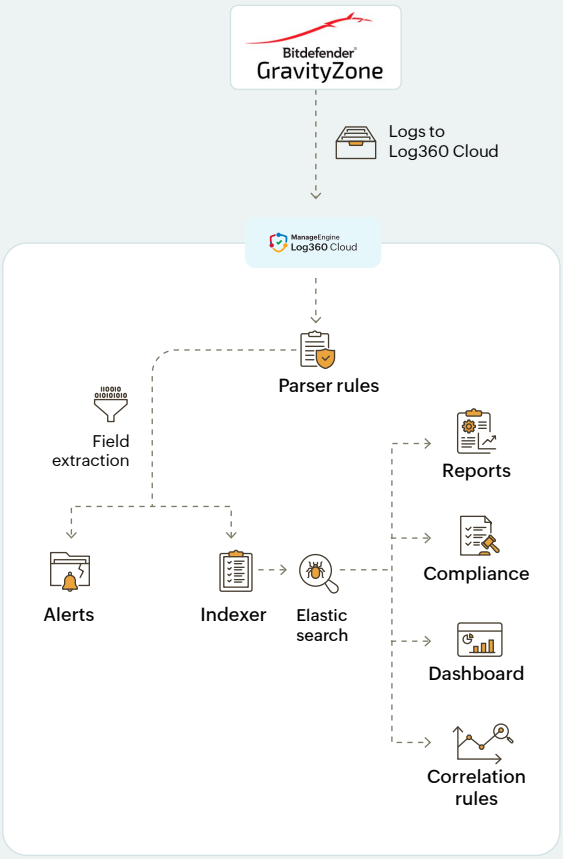
Firewall and authentication events

System and agent status events

These logs are parsed and normalized for SIEM analytics.

How it works

1. Bitdefender GravityZone forwards logs via syslog (on-prem or cloud).
2. Log360 Cloud receives and parses EDR events.
3. Events are indexed and stored for analysis.
4. Data is used across:
   - Reports and dashboards
   - Alert profiles
   - Detection rules
   - Incident Workbench investigations



Use cases and challenges | How Log360 Cloud helps

Use case / challenge	How the integration helps
EDR data siloed from SIEM	Centralizes Bitdefender detections with other security logs.
False positives in endpoint alerts	Correlates EDR events with SIEM data for context.
Limited historical visibility	Retains Bitdefender logs long term for audits and reviews.
Manual threat investigation	Enables investigation using correlated endpoint, user, and network data.
Compliance reporting gaps	Provides out-of-the-box compliance-ready reports.

Analytics available

Once integrated, Log360 Cloud transforms Bitdefender telemetry into actionable detection visibility, correlated threat identification, contextual investigations, and automated response workflows.

Detection Visibility and Trend Analysis

Bitdefender GravityZone events are converted into structured summaries and trend views that provide insight into threat posture across endpoints and users.

This includes:

- Malware and ransomware detection trends over time
- Severity-based threat distribution
- Mitigation status visibility (mitigated vs unmitigated threats)
- Authentication and system activity tracking

Examples:

Ransomware Detection Trend View

Displays ransomware activity spikes across endpoints.

Endpoint Threat Activity Summary

Highlights systems generating repeated or high-severity detections.

Security Posture and Protection Monitoring

The integration continuously monitors endpoint protection health and risk conditions that may expose systems.

This includes monitoring:

- Unmitigated threats
- Agent uninstall events
- Overloaded security servers
- Outdated update servers

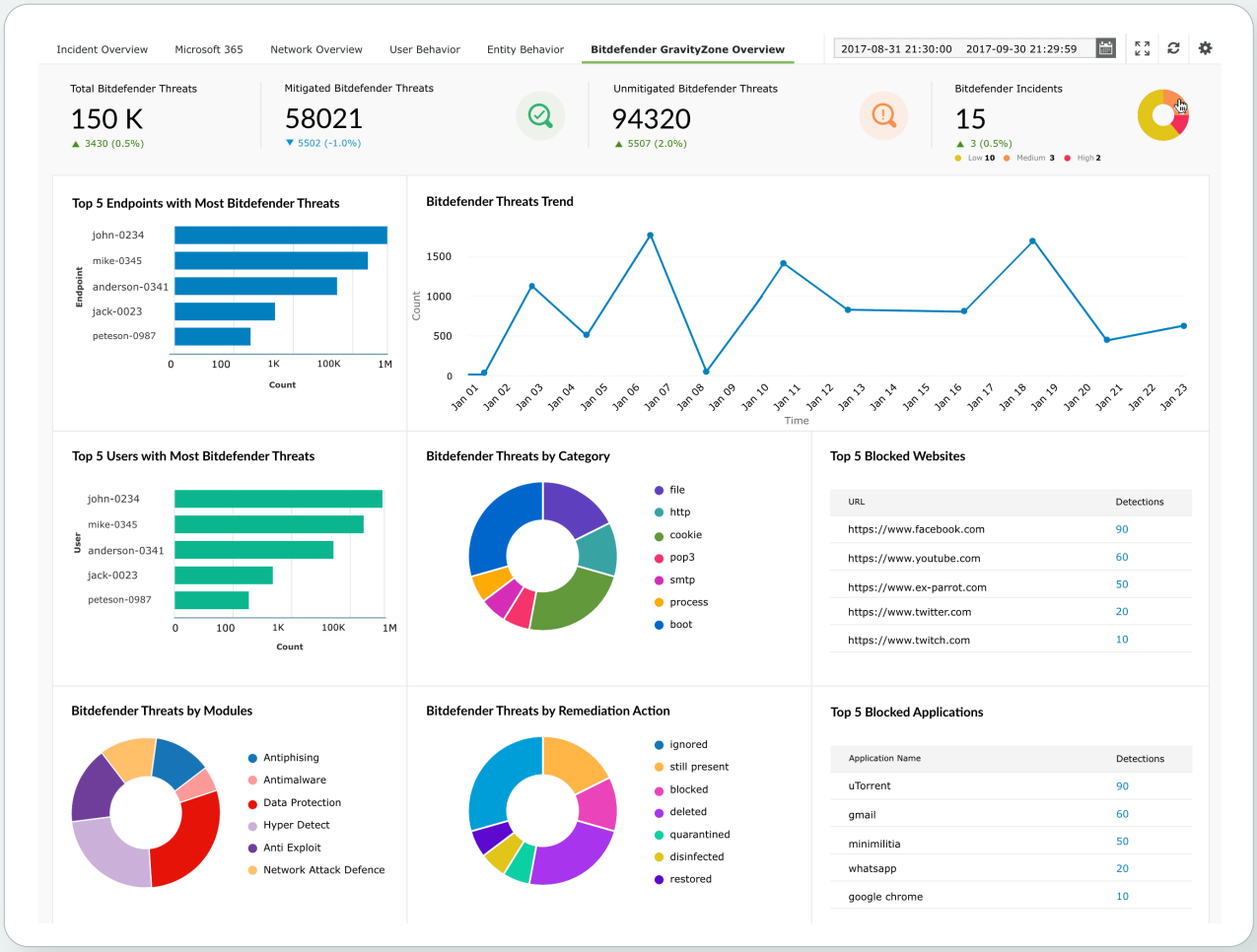
These alerts help detect protection gaps and operational risks early.

Real-Time Operational Visibility

Log360 Cloud offers a prebuilt visual dashboard that provides real-time insights into:

- Top affected endpoints and users
- Total, mitigated, and unmitigated threats
- Threat distribution by protection module
- Category-based detection trends

Gain instant visibility into endpoint threat posture and mitigation status without relying on manual searches.



Correlated Threat Detection

Bitdefender GravityZone detections are correlated with SIEM data to uncover multi-stage or coordinated attack patterns that endpoint telemetry alone may not expose.

This enables detections of:

- Coordinated reconnaissance across multiple systems
- Ransomware-like destructive behavior
- Lateral movement combined with credential harvesting
- Suspicious script-based execution chains

Examples:

Rule Name	Description	Objective
StormScan Coordinated Recon Detection	Detects coordinated port scanningacross multiple endpoints.	Identify distributed or repeated port scans to reduce noise and highlight potential lateral movement.
Obfuscated PowerShell with Shadow Copy Wipe	Detects encoded PowerShell followed by volume shadow copy deletion.	Identify ransomware-like destructive activity.

Investigation Workbench Context

Bitdefender-specific investigation components embed endpoint context directly within the Incident Workbench.

This provides:

- Threat breakdown by protection module
- Recent endpoint detections timeline
- Files most frequently involved in incidents
- Historical correlation with related alerts

Analysts can assess attack scope and root cause without switching tools.

Outcomes

By integrating Bitdefender GravityZone with Log360 Cloud, organizations achieve:

- Centralized EDR visibility
- Improved detection accuracy through correlation
- Faster investigations with contextual data
- Stronger audit and compliance support

About Log360 Cloud

ManageEngine Log360 Cloud, a unified cloud SIEM solution with integrated CASB capabilities, helps enterprises secure their network from cyberattacks. With its security analytics, threat intelligence and incident management capabilities, Log360 Cloud helps security analysts spot, prioritize and resolve threats in both on-premises and cloud environments. The solution is highly scalable and helps drive down infrastructure and storage costs.

For more information about Log360 Cloud, visit www.manageengine.com/cloud-siem/.

Sign-up for free

Get a personalized walk-through