ManageEngine
Log360

The unified security platform

Today's agenda

Threat reality: Faster attacks, slower response chains

Where SIEM-only workflow breaks

Use cases: Incident containment, alert triaging

France fit: GDPR, NIS2 operational constrains

Why this matters right now

- Identity-led attacks and lateral movement dominate incidents
- Tool fragmentation slows triage and containment
- Analyst fatigue and queue overload are now structural
- Regulators expect evidence of controls, not tool checklists

Where SOC workflows break

- Alert generated -> manual enrichment -> ownership assignment
- Escalation loops delay containment decisions
- Response execution disconnected from investigation context
- Detection in minutes, response in hours

OPERATING MODEL SHIFT

Visibility Without Orchestration Creates Backlog

SIEM-only

- Collect
- Correlate
- Alert
- Manual triage dominates

SIEM + SOAR + AI

- Prioritize
- Enrich
- Orchestrate
- Respond + document continuously

ManageEngine Log360

SECURITY CONTROL CENTER

Entire security stack. One control center

Your IT stack | Telemetry in

Endpoint security
Crowdstrike.Bitdefender. MS Defender. SentinelOne
EDR/XDR alerts | Process telemetry

Network security
PaloAlto . Fortinet . Cisco . Check Point
NGFW logs | IDS/IPS alerts | VPN Sessions

Identity & Access
Okta . Cisco Duo . Azure
Auth events · MFA challenges · privilege escalation

Cloud platforms
AWS . Azure . M365
CloudTrail · Activity logs · sign-in logs · API calls

Vulnerability & scanning
Qualys . Tenable . Rapid7 . Nessus
CVE data · asset risk scores · scan results

Infrastructure & Database
Windows · Linux · SQL · Oracle · Syslog
OS events · DB audit · SNMP · custom regex

Log360 - Security control center

AI Intelligence
Zoho MCP | Zia Agent Studio | Zia Assistant

Govern & comply
100+ frameworks · Audit evidence · Breach Notification. Incident Report

Respond & orchestrate
SOAR

Data & cloud security
FIM | DLP | CASB

Detect & Analyze
Correlate | UEBA | Threat intel | ITDR

Collect & Normalize
Universal log parsing · schema normalization · 750+ sources

Response Out | SOAR actions

Endpoint
Isolate host · Killl process · Deploy patch · Disable USB
via Endpoint Central, CrowdStrike API, Defender

Network
Block IP at firewall · quarantine VLAN · revoke VPN
via Palo Alto, Fortinet, Cisco API

Identity
Disable account · force MFA · revoke sessions
via AD360, Okta, PAM360, Entra ID

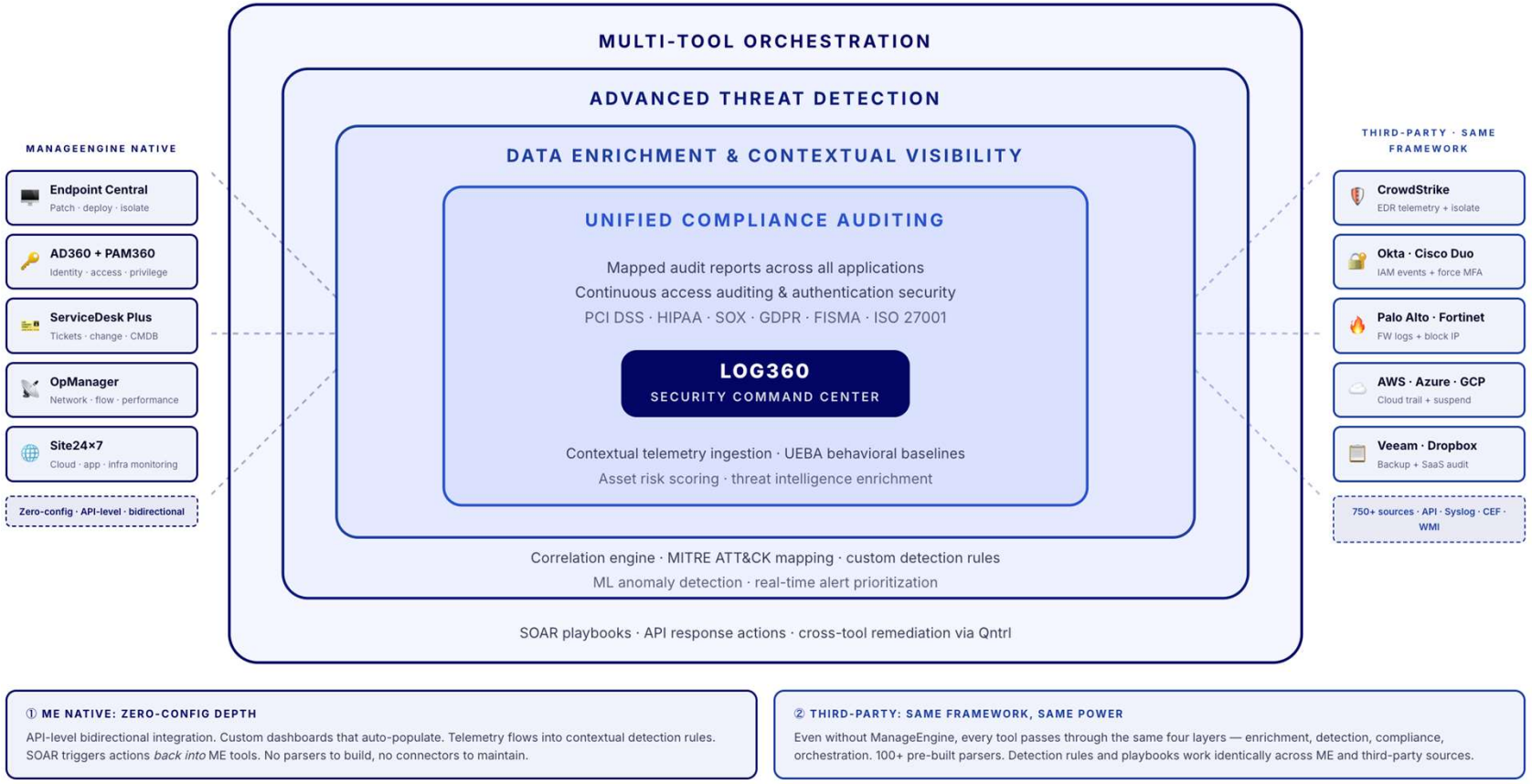
ITSM tools
Auto-create incident · Assign · Escalate · SLA track
via ServiceDesk Plus, ServiceNow, Jira

Compliance
Auto-generate evidence · map to controls · audit report
100+ frameworks auto-mapped

Custom actions
Python / Deluge scripts · webhook · REST API calls
Extensible to any tool with an API

INTEGRATION

One framework. Native first, then everything else



① ME NATIVE: ZERO-CONFIG DEPTH

API-level bidirectional integration. Custom dashboards that auto-populate. Telemetry flows into contextual detection rules. SOAR triggers actions *back into* ME tools. No parsers to build, no connectors to maintain.

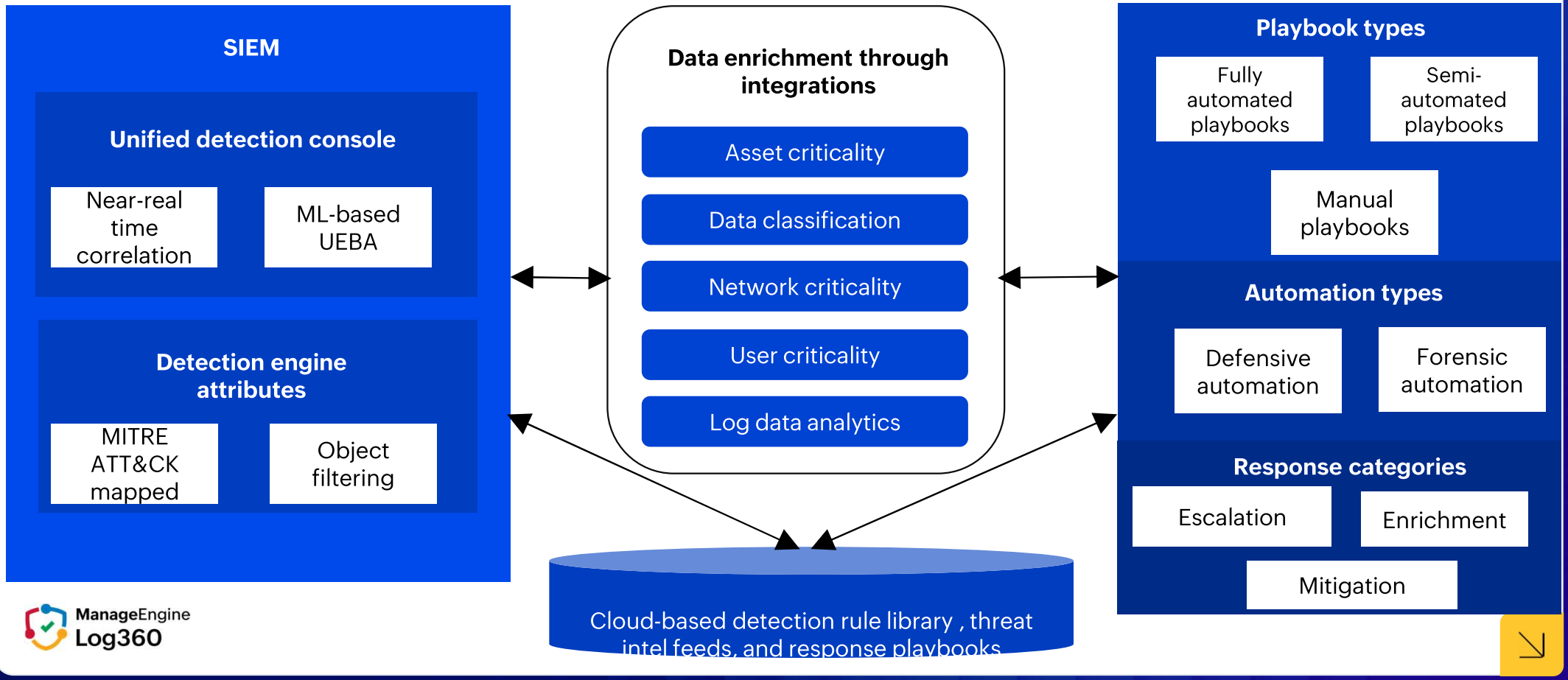
② THIRD-PARTY: SAME FRAMEWORK, SAME POWER

Even without ManageEngine, every tool passes through the same four layers — enrichment, detection, compliance, orchestration. 100+ pre-built parsers. Detection rules and playbooks work identically across ME and third-party sources.

ManageEngine Log360

INTEGRATION

How it all comes together



Total Bitdefender Threats

150 K

▲ 3430 (0.5%)

Mitigated Bitdefender Threats

58021

▼ 5502 (-1.0%)

Unmitigated Bitdefender Threats

94320

▲ 5507 (2.0%)

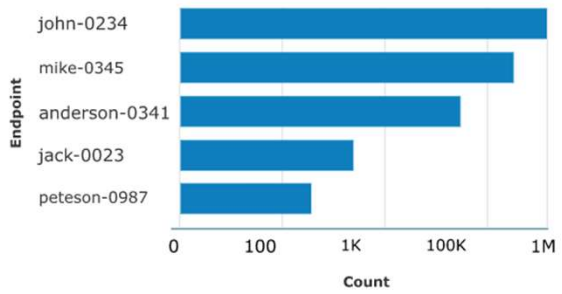
Bitdefender Incidents

15

▲ 3 (0.5%)

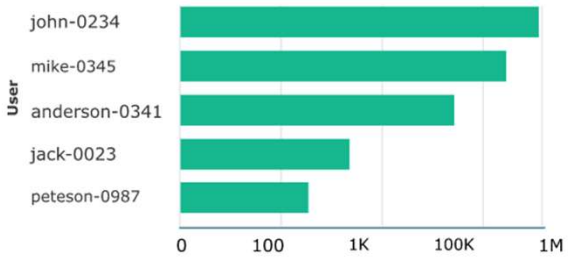
Low 10 Medium 3 High 2

Top 5 Endpoints with Most Bitdefender Threats



Bitdefender Threats Trend

Top 5 Users with Most Bitdefender Threats

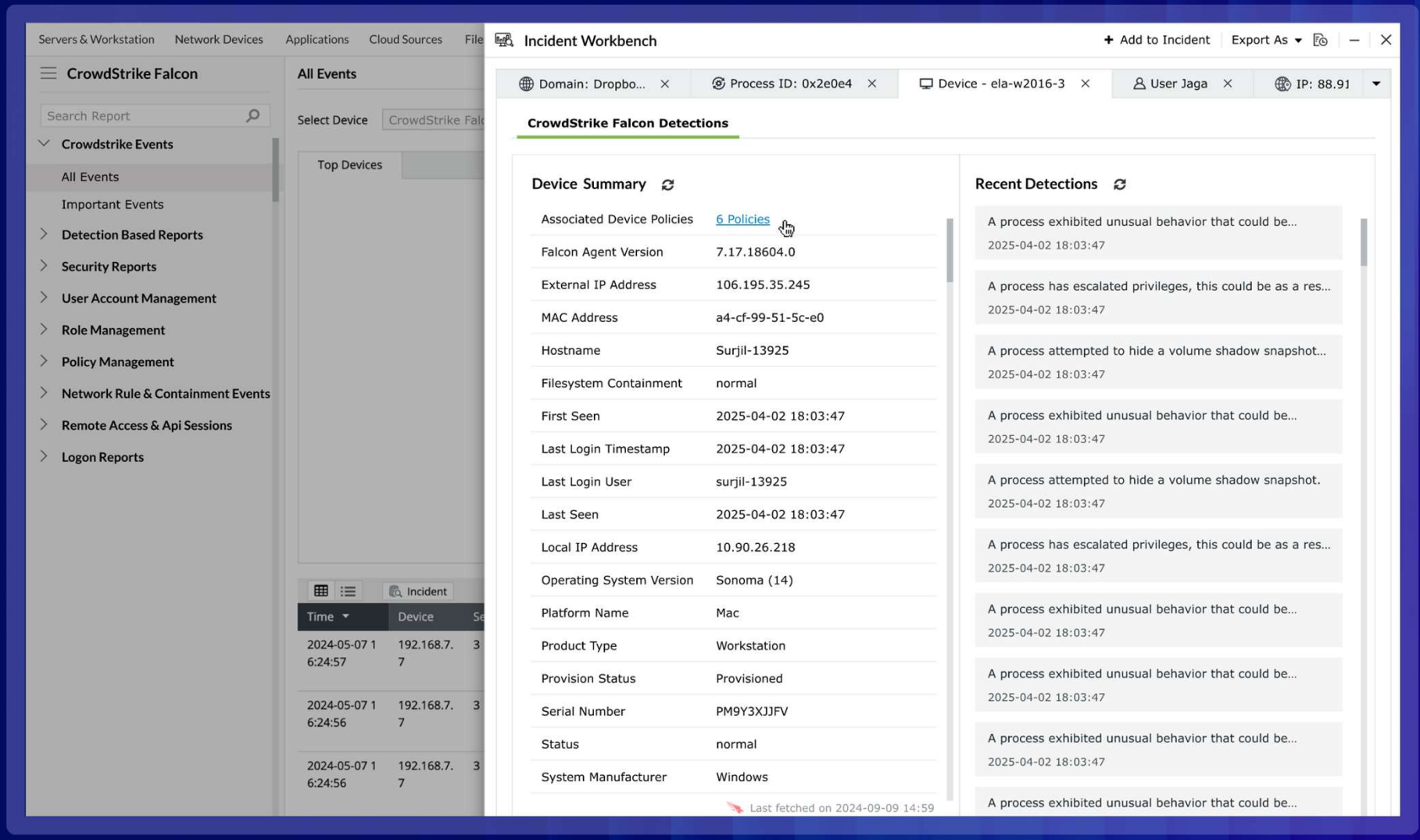


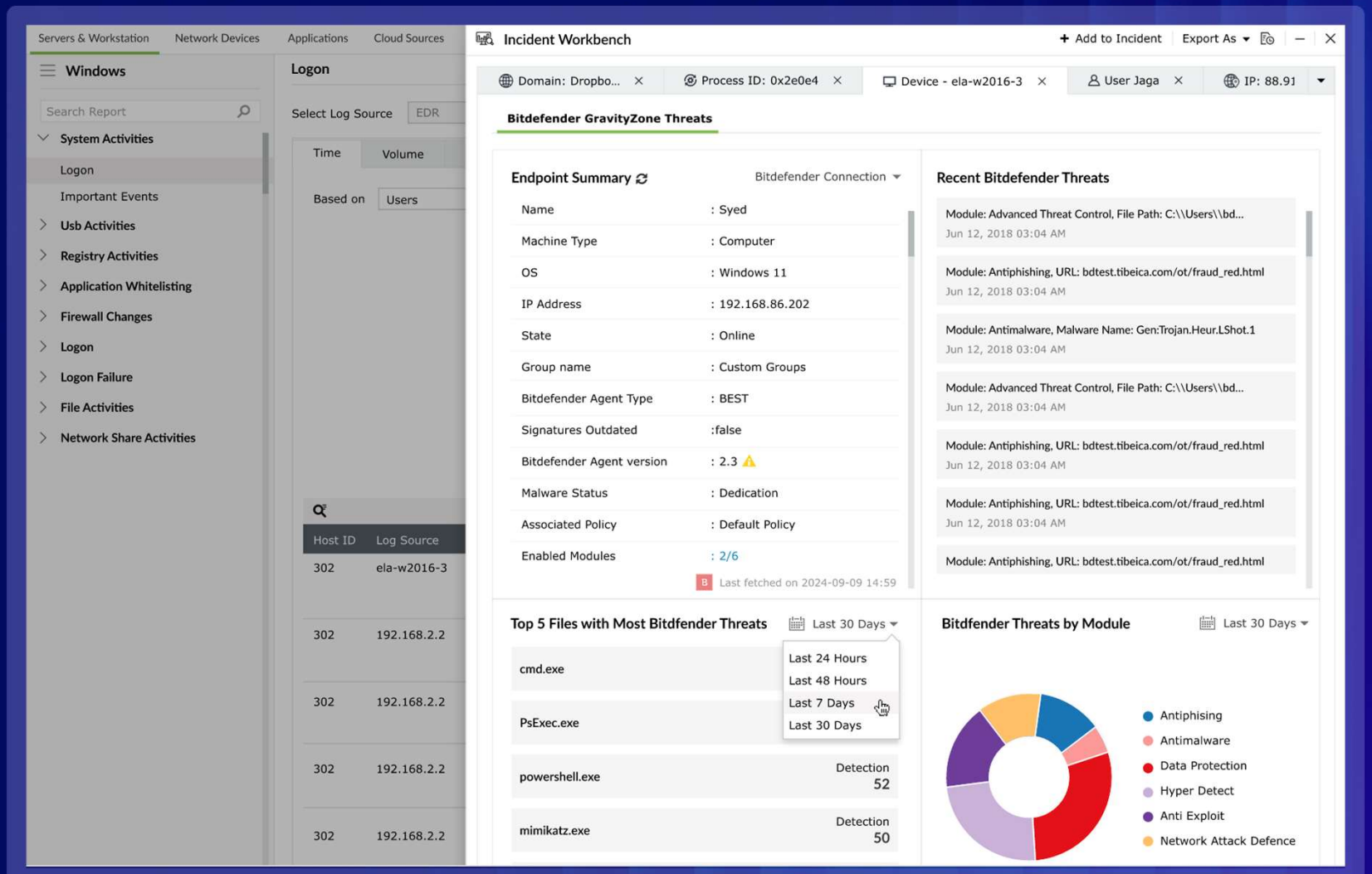
Bitdefender Threats by Category

Top 5 Blocked Websites

URL	Detections
https://www.facebook.com	90
https://www.youtube.com	60
https://www.ex-parrot.com	50
https://www.twitter.com	20

ManageEngine Log360


Servers & Workstation
Network Devices
Applications
Cloud Sources
CrowdStrike Falcon
Search Report
Crowdstrike Events
All Events
Important Events
Detection Based Reports
Security Reports
User Account Management
Role Management
Policy Management
Network Rule & Containment Events
Remote Access & Api Sessions
Logon Reports
All Events
Select Device
Top Devices
Incident
Time
Device
2024-05-07 16:24:57
192.168.7.7
2024-05-07 16:24:56
192.168.7.7
2024-05-07 16:24:56
192.168.7.7
Incident Workbench
+ Add to Incident
Export As
Domain: Dropbo...
Process ID: 0x2e0e4
Device - ela-w2016-3
User Jaga
IP: 88.91
CrowdStrike Falcon Detections
Device Summary
Associated Device Policies
6 Policies
Falcon Agent Version
7.17.18604.0
External IP Address
106.195.35.245
MAC Address
a4-cf-99-51-5c-e0
Hostname
Surjil-13925
Filesystem Containment
normal
First Seen
2025-04-02 18:03:47
Last Login Timestamp
2025-04-02 18:03:47
Last Login User
surjil-13925
Last Seen
2025-04-02 18:03:47
Local IP Address
10.90.26.218
Operating System Version
Sonoma (14)
Platform Name
Mac
Product Type
Workstation
Provision Status
Provisioned
Serial Number
PM9Y3XJJFV
Status
normal
System Manufacturer
Windows
Last fetched on 2024-09-09 14:59
Recent Detections
A process exhibited unusual behavior that could be...
2025-04-02 18:03:47
A process has escalated privileges, this could be as a res...
2025-04-02 18:03:47
A process attempted to hide a volume shadow snapshot...
2025-04-02 18:03:47
A process exhibited unusual behavior that could be...
2025-04-02 18:03:47
A process attempted to hide a volume shadow snapshot.
2025-04-02 18:03:47
A process has escalated privileges, this could be as a res...
2025-04-02 18:03:47
A process exhibited unusual behavior that could be...
2025-04-02 18:03:47
A process exhibited unusual behavior that could be...
2025-04-02 18:03:47
A process exhibited unusual behavior that could be...
2025-04-02 18:03:47
A process exhibited unusual behavior that could be...



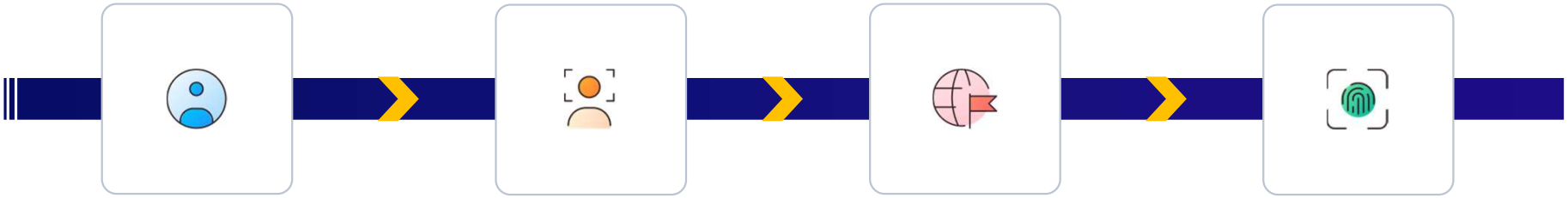
ManageEngine Log360

Use cases

USE CASE: 1

Impossible Travel

Detect suspicious logins occurring from geographically impossible locations within a short time window.



USE CASE: 1

Impossible Travel

Impact

- Unauthorized account access
- Credential compromise
- Potential session hijacking
- Risk of lateral movement within the environment

Traces (Logs & Evidence)

M365 / Azure AD

- Sign-in logs
- Geo-location and IP address changes
- MFA success or failure events

VPN

- Connection logs with public IP and geo-location

Active Directory

- Event ID 4624 (successful logon)

Windows Endpoints (optional)

- Session and logon activity

USE CASE: 1

Impossible Travel

Detection

- Correlate M365 sign-in events from geographically distant locations
- Geo-distance threshold greater than 1000 km
- Correlation window of 15 minutes
- Trigger when 2 or more logins from new IPs occur within the window
- Enrich with AD logon events and MFA patterns

Investigation

- Review sign-in timelines across M365 and AD
- Validate IP reputation and geo-location changes
- Analyze MFA challenge outcomes
- Confirm whether logins originated from known devices or networks

Responses

- Trigger adaptive or step-up MFA
- Alert SOC analysts with contextual evidence
- Flag the user account for further review
- Initiate incident response workflow if required

USE CASE: 2

Privileged Admin 360 Profile
(Cross-Platform Account Investigation)

Analyst prompt examples

- Give me a 360 profile for jsmith_admin
- Why did jsmith_admin log in from Frankfurt 27 minutes after Coimbatore?
- Show all recent privilege changes and tickets for jsmith_admin

Integrating

- Log360
- Okta
- Crowdstrike / Bitdefender
- ServiceNow

Investigation workflow

1. **Identity + Access Profile Log360 + Okta**
2. **Endpoint Investigation CrowdStrike**
3. **Authentication Timeline (48h) Log360 + Okta**
4. **Network + Privilege Audit Log360**
5) **Ticket Correlation ServiceNow**
Investigation - MCP Orchestrator

Why Log360 wins

SECURITY CONTROL CENTER

Five domains. Three pillars. One platform

Threat detection, investigation and response

Core SIEM engine
Log collection | Real-time correlation | Threat hunting | Investigation Workbench | Forensic Analysis | MITRE ATT&CK mapping

UEBA
ML baselines | Risk scoring | Insider threats | Anomaly detection | Peer grouping | User identity mapping

Security operations & ITDR

Orchestration and response
Visual playbooks | Auto-containment | Zoho Qntrl engine | Endpoint response | Identity response | Network response

ITDR
Complete and granular visibility into hybrid AD environments and risk identification

Risk and compliance

Compliance audit readiness
100+ frameworks | Evidence generation | Breach Notification | Incident Report through AI investigation

SHARED DATA FABRIC | Every domain reads from and writes to the same correlated data store — no integration middleware, no data silos, no swivel-chair.

ManageEngine Log360

STRUCTURAL DIFFERENTIATOR

SOAR - Built on Qntrl by Zoho

Every major SIEM vendor *acquired* their SOAR. Zoho *built* Qntrl — the same workflow engine that powers operations across 100M+ Zoho users. That's why Log360 can include SOAR at zero execution cost.

Privately held	**Profitable**	**Zero M&A debt**
$0 per execution cost	**$0 separate SOAR license**	**∞ playbook run**

Automate more → pay the same. Maturity is *rewarded*, not penalized
Bi-directional response: EC, PAM360, AD360, SDP, firewalls, custom APIs
No acquisition risk — Zoho builds, not buys. Roadmap continuity guaranteed

Enterprise workflow engine, repurposed for SOAR

- → Battle-tested at enterprise scale before it ever reached security — not a v1 SOAR built to check a box
- → Visual drag-and-drop builder, conditional branching, approval gates, SLA timers — all inherited from Qntrl
- → Native to Log360 — SIEM alert fires, SOAR playbook executes in the same process, same data context, zero latency

The structural moat: Un-acquiring a $500M SOAR bolt-on and rebuild natively. Zoho never had to — Qntrl was built as an enterprise workflow engine first, then applied to security. The result: zero execution cost automation that scales with your SOC maturity, not against it.

ManageEngine Log360

COMPLIANCE

Audit-ready by default — not as an afterthought

Every detection rule, UEBA anomaly, and SOAR response automatically generates audit evidence. When security operations produce compliance as a natural output, your CISO stops firefighting audits and starts owning posture.

100+
Frameworks

26K+
Mapped Controls

Decoupled marketplace

Region / Sector	Frameworks
Global	ISO 27001, SOC 2, CSA CCM, CIS, NIST CSF, NIST 800-53
Europe	GDPR, NIS2, DORA, eIDAS, UK Cyber Essentials
Americas	HIPAA, SOX, PCI DSS 4.0, CMMC v2, NYDFS, CCPA
APAC/MEA	PDPA, NCA SIEM (KSA), IRAP, SEBI, PDPL
Sector	SWIFT CSCF, NERC CIP, FFIEC, MAS TRM, TISAX

Closed-loop compliance workflow

1 · AUTO-MAP
Security events automatically mapped to framework controls. Detection = evidence.

2 · CONTINUOUS MONITORING
Real-time compliance posture. Control violations trigger alerts — not quarterly audit findings.

3 · EVIDENCE GENERATION
Audit workpapers, evidence queries, control attestation reports — generated, not assembled.

4 · AUDITOR HANDOFF
Export-ready PDF/CSV reports. Auditor gets the package, not a platform login.

ManageEngine Log360

Intelligence

AI-native from the ground up

Not a chatbot bolted on. AI is woven into the architecture — through Zoho's MCP server, pre-built agents, and the Zia Agent Studio for full customization.

LAYER 03: Zia Agent Studio
Build custom AI agents — no code, no hard coded prompts

LAYER 02: Pre-built Security Agents
Threat hunter · Investigator · Compliance reviewer · Report writer

LAYER 01: Zoho MCP Server
Model Context Protocol — secure model-to-data brokerage

// WHY IT MATTERS

AI you OWN
Not AI you RENT.

- → No prompt lock-in — agents are fully customizable
- → Data stays inside your boundary via MCP
- → BYO LLM — Zia, OpenAI,
- → Agent-to-agent collaboration for complex investigations

Our recent customers across Europe and the UK

ManageEngine

ManageEngine
Log360

Thank you