



Centralized **Log** Management and **SIEM** Platform



100% PCI-DSS Compliant



KVKK (Personal Data Protection Law) Compliance



Fully Compliant with ISO 27001 Standards



Full Compliance with Law No. 5651

Are you ready to discover **Logchase**?

Transforming chaos into actionable insights in sub-second time (<1s). Log management is no longer a burden for your team; it is the unshakable foundation of your operational security and regulatory compliance.

Get in Touch

+90 (850) 305 88 66

info@logchase.com

www.logchase.com

Ataket Mah. Dicle Cd. No:9/A
Ümraniye/İSTANBUL

8 The Green Suite 13105
Dover, DE, 19901, USA

Control Center

NEXT-GENERATION

in Cybersecurity



No more getting lost in millions of data rows. Logchase identifies and deciphers cyber threats within your complex IT infrastructure in seconds, **transforming your organization into a proactive line of defense.**

Why Logchase?

Distinguishing features
in enterprise log
management and SIEM
solutions

⚡ Full Compliance

🚀 High Performance

👥 24/7 Technical Support

Logchase is a comprehensive platform offering centralized collection, intelligent alerting systems, and advanced analytical solutions for enterprise log management and SIEM requirements. Fully compliant with regulatory standards such as KVKK, Law No. 5651, and PCI-DSS; the system caters to businesses of all sizes through flexible deployment options, including cloud and self-hosted. With its robust integration network and tiered packages ranging from "Core" to "Elite," it optimizes data security and traceability from a single point of truth.

1M+

EPS

50+

Pre-built Parsers

99.9%

Uptime SLA

24/7

Technical Support



Powerful Features



Centralized Log Collection

Collect logs from all your systems in a single center. Data from servers, network devices, applications, and security systems are automatically normalized and stored.



Support: Syslog, API, SFTP, Database



Advanced Search & Analytics

Search through millions of logs in seconds. Rapidly detect anomalies with powerful filtering, regex support, and real-time analytics, transforming your organization into a proactive line of defense.



Performance: 1M+ EPS (Events Per Second) processing

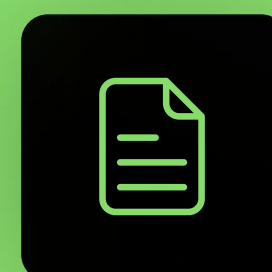


Intelligent Alerting System

Identify suspicious activities instantly with customizable alert rules. Receive 24/7 notifications via E-mail, SMS, and Webhook integrations.



Advanced threat detection with a high-performance correlation engine.



Advanced Reporting

Get a quick start with pre-built report templates or design custom reports tailored to your specific needs. Inform management automatically with scheduled reports.



Export Options: PDF, Excel export & automated scheduling.

info

The visual illustrates that the massive volume of log data generated daily in the modern IT world can no longer be managed with traditional methods, leading to critical security risks and compliance gaps. Logchase's approach transforms this chaos into meaningful insights in less than a second, turning log management from a burden into a fundamental pillar of operational efficiency and security.

Out-of-the-box connectivity for major platforms and services.

Fortinet

Palo Alto

Cisco

Juniper

MikroTik

pfSense

Sophos

SonicWall

Nginx

Apache

IIS

HAProxy

Traefik

Caddy

MySQL

PostgreSQL

MSSQL

MongoDB

Redis

REST API

Webhook

JSON

Batch Import

Real-time

Windows Event

Linux Syslog

macOS

VMware

Kubernetes

Docker

ForcePoint

McAfee

Trend Micro

WatchGuard

Symantec

CrowdStrike

Transform log management from a necessity into your power...

Flexible Deployment Options

Offers flexible deployment models tailored to your requirements—choose between self-hosted environments for complete control, or fast and scalable cloud infrastructure.

Flexible deployment options:
Self-hosted or Cloud



Self Hosted

Complete control and data sovereignty within your own data center. Full compliance with your corporate security policies.

- ✓ Instant Deployment
- ✓ Automatic Updates
- ✓ Flexible Scalability
- ✓ Managed Infrastructure



Cloud

Rapid deployment, automatic updates, and a scalable infrastructure. Minimize your operational overhead.

- ✓ Instant Deployment
- ✓ Automatic Updates
- ✓ Elastic Scalability
- ✓ Managed Infrastructure

On-Premise Package Comparison

Features	Core	Advanced	Enterprise	Elite
Log Sources	5	5 / 15 / 25 / 50	5 / 15 / 25 / 50	25 / 50 / 100 +
EPS	Unlimited	Unlimited	Unlimited	Unlimited
Support Type	Ticket Support	Ticket Support	Ticket & Phone Support	Ticket & Phone Support
SLA	Business Hours	Business Hours	24/7	24/7
System Users	1 User	3 Users	10 Users	Unlimited
Authorization (RBAC)	✗	✓	✓	✓
Dashboard	✓	✓	✓	✓
Search	✓	✓	✓	✓
Reporting	✗	✓	✓	✓
Log Collection Methods	✓	✓	✓	✓
Alert Management Module	✗	✓	✓	✓
Alert Action	✗	✓	✓	✓
Incident Management Module	✗	✓	✓	✓
Risk Scoring	✗	✓	✓	✓
Custom Parsel	✗	✓	✓	✓
FIM	✗	✗	✓	✓
Threat Intelligence	✗	✗	✓	✓
Disaster Replication	✗	✗	✓	✓
Multi Tenant	✗	✗	2 Tenants	5 Tenants
HA Cluster	✗	✗	3 Nodes	5+ Nodes

General Package Overview

On-Premise packages provide a scalable structure from Core to Elite levels, tailored to meet diverse organizational requirements. While all tiers include unlimited EPS and essential log management features, higher-tier packages introduce advanced capabilities such as Role-Based Access Control (RBAC), alert management, and incident management. At the Enterprise and Elite levels, critical security functionalities like FIM (File Integrity Monitoring), Threat Intelligence, and Disaster Replication are activated. Furthermore, these top-tier packages address enterprise-grade demands, including multi-tenancy support and High Availability (HA Cluster). Support levels also scale alongside the packages, reaching up to 24/7 availability. This architecture empowers organizations to undergo a flexible and gradual transition based on their evolving needs.

CENTRALIZED

Log Management

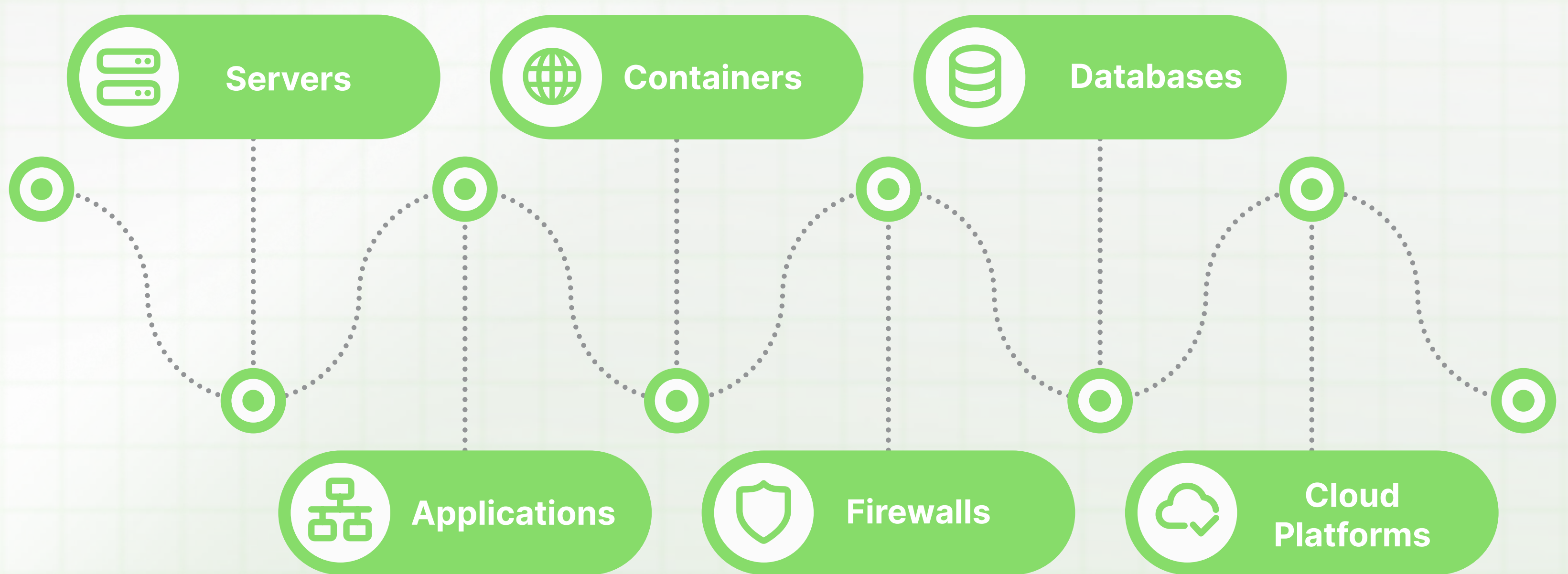
PLATFORM

Collect, normalize, and search logs in real-time across any system. By centralizing data from servers, applications, network devices, and cloud environments, **Logchase** facilitates high-speed search, advanced analytics, and efficient troubleshooting.

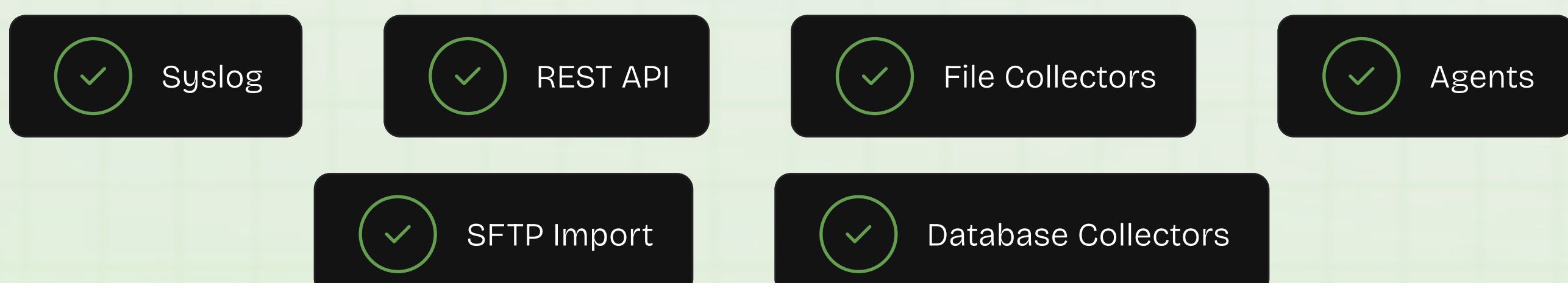


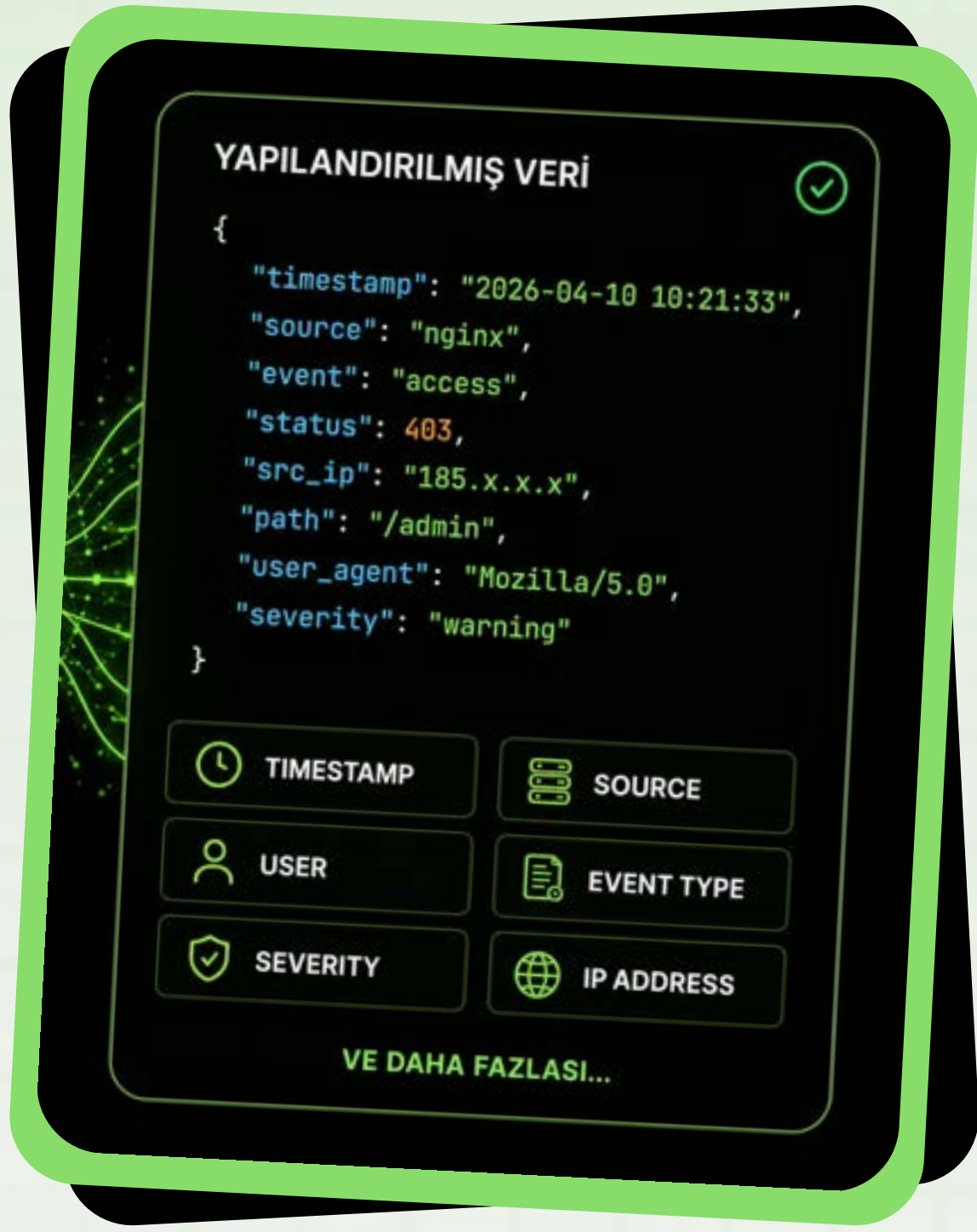
Universal Log Collection

Gather logs seamlessly from servers, applications, containers, firewalls, databases, and cloud platforms.



Supported Methods





Automated Data Normalization

Accelerate your analysis process by automatically transforming raw logs into meaningful and structured data fields. Standardize log formats from diverse sources using our vendor-agnostic parsing engine. With 50+ pre-built parsers, you can achieve integration within minutes and automatically extract critical fields such as timestamp, source, user, event type, severity, and IP address. This eliminates manual workload, minimizes human error, and streamlines your security, monitoring, and reporting workflows.

- ✓ Timestamp
- ✓ Event type
- ✓ Source
- ✓ Severity
- ✓ User
- ✓ IP address

Log Integrity Assurance

Each log record is protected with a unique cryptographic hash, ensuring that its authenticity remains verifiable. Log archives are digitally signed with time-stamps for secure storage.

✓ Cryptographic Hashing

Each log entry is uniquely signed using a SHA-256 hash.

✓ Time-Stamping

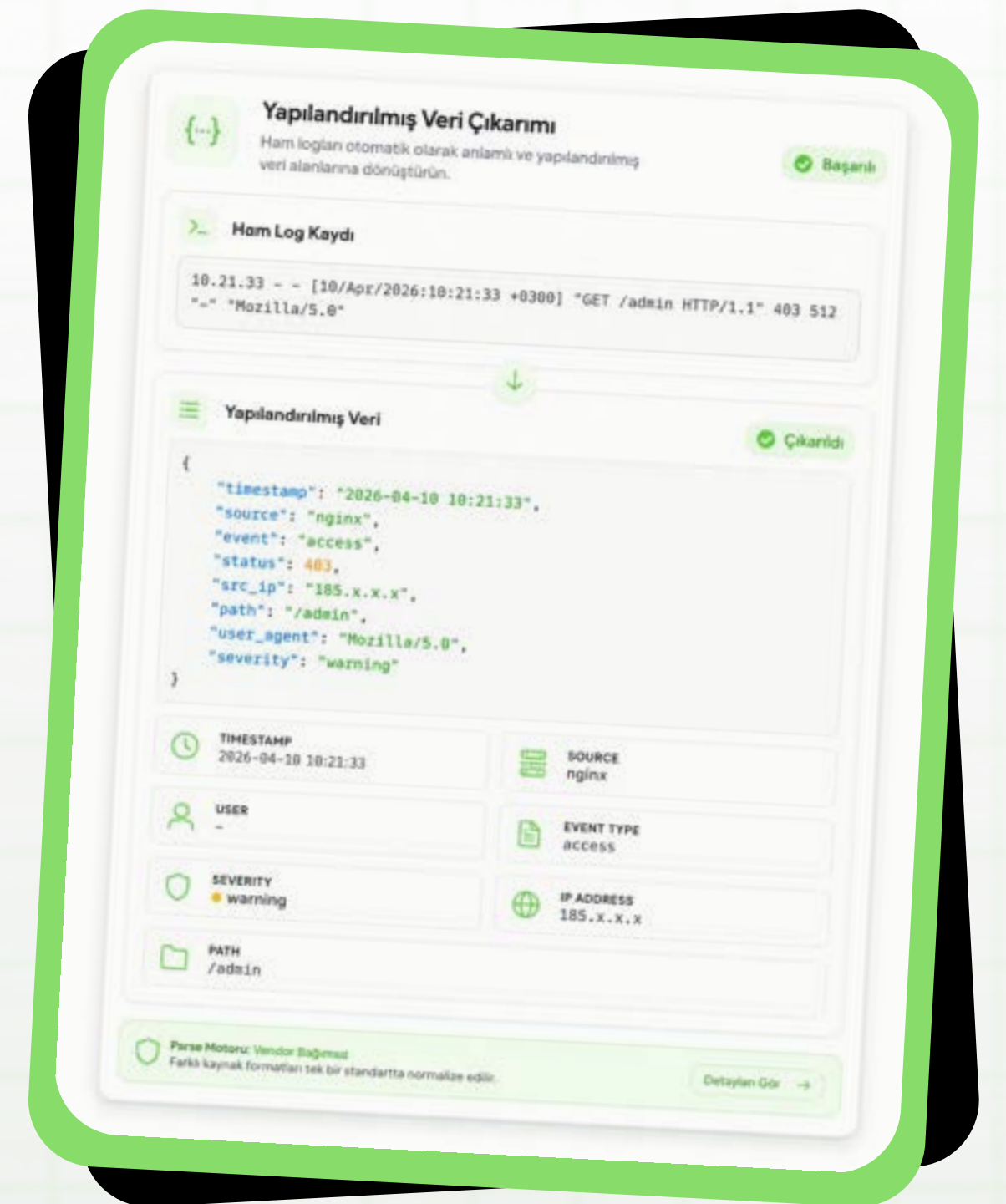
Log archives are signed and stored using FreeSA or Tübitak Zamane protocols.

✓ Integrity Verification

The immutability of logs can be verified at any time to detect any tampering.

✓ Legal Admissibility

Immutable records serve as valid digital evidence in legal proceedings.



Powerful Search Engine

Access the data you need instantly with a robust search engine capable of querying billions of log records in seconds. Perform deep-dive queries across all content with full-text search, and narrow down results effortlessly using field-based filtering. Solve complex search scenarios with Regex support and focus on specific periods with time-range filtering. Optimize your analysis workflows by storing frequently used searches with the "Saved Queries" feature.

- ✓ Full-text search
- ✓ Time-range filtering
- ✓ Field-based filtering
- ✓ Saved queries
- ✓ Regex search
- ✓ High-performance search engine

Disaster Recovery Replication



How is disaster recovery performed?

All your log data is automatically replicated in real-time to geographically isolated disaster recovery sites. By eliminating the risk of data loss, we guarantee seamless business continuity.

Real-Time Replication

Logs are instantly synchronized with the disaster recovery site. RPO $\approx$ 0.

Geographic Redundancy

Full protection provided by data centers located in distinct geographic regions.

Seamless Business Continuity

Log collection and analysis operations continue without interruption, even in disaster scenarios.

Real-Time Log Analytics

Detect anomalies and patterns through statistical analysis and behavioral modeling.

⚡ Statistical Analysis

🚀 Behavioral Patterns

👥 Baseline Comparison

👥 Log Frequency Analysis

Use Cases

FAST AND INTELLIGENT LOG ANALYSIS

Rapid Troubleshooting
Identify root causes instantly through log centralization.

Audit and Compliance
Maintain long-term log retention to meet regulatory compliance requirements.

DevOps Observability
Analyze application logs to detect errors and identify performance bottlenecks.





Detect threats before they escalate and respond instantly.

The SIEM Platform for Modern Security Teams

Correlation Engine

Go beyond individual events by correlating data from multiple log sources. Detect attack chains and anomaly patterns by aggregating activities occurring across disparate systems. For instance, automatically uncover critical scenarios such as a successful login or privilege escalation following multiple failed login attempts from the same IP.

Centralized Security Visibility

Achieve end-to-end visibility by centralizing logs from your entire infrastructure. Centrally monitor data from servers, endpoints, applications, and firewalls. This allows you to visualize inter-system connections more clearly, identify threats faster, and accelerate your response processes.

Alert Rules and Detection Logic

Create customizable alert rules based on log frequency, specific patterns, and field-based values. Automatically detect critical incidents through anomaly detection and threat intelligence matching. Receive instant notifications for scenarios such as rapid brute force attempts, unexpected user activities, or unauthorized access to sensitive data.

1M+

EPS INGESTION

<1S

SEARCH PERFORMANCE

REAL-TIME

ALERT PROCESSING

SOC Workflow Support

Logchase empowers security teams to detect, investigate, and respond to incidents with agility.

Detect
Incidents

STEP 1

Investigate
Incidents

STEP 2

Prioritize
Alerts

STEP 3

Rapid
Response

STEP 4

A modern SIEM platform empowers security teams to centralize, analyze, and transform log data into actionable insights. By correlating data from disparate sources through its correlation engine, it uncovers complex attack chains, ensures full infrastructure observability via centralized visibility, and identifies threats instantly with advanced alerting mechanisms. Consequently, security teams can respond to incidents more rapidly, manage risks proactively, and significantly enhance operational efficiency.

What is SIEM?

SIEM (Security Information and Event Management) is a comprehensive security solution that centrally collects, correlates, and analyzes log data from disparate systems. It uncovers hidden links between events through log correlation, provides instant threat notifications via sophisticated alerting mechanisms, and empowers security teams to rapidly analyze and respond to incidents through streamlined investigation workflows.

Centralized Security Visibility

Gain full visibility across your entire infrastructure.

✓ Servers

✓ Endpoints

✓ Applications

✓ Cloud Environments

✓ Firewalls

Correlation Engine

Detect complex attack patterns across multiple log sources.

✓ Successful login following multiple failed attempts

✓ Privilege escalation following suspicious activity

✓ Unusual geographic login patterns (Anomalous Geo-location)

Alert Rules And Detection Logic

Create detection rules based on event frequency, log patterns, field values, and anomaly detection.

✓ Field Values

✓ Log Patterns

✓ Threat Intelligence Matching

✓ Anomaly Detection

✓ Event Frequency

Don't just archive your logs. Empower your security with **LOGCHASE**.

Traditional Log Storage vs Logchase SIEM



Traditional Log Storage

Logs are stored but not analyzed.

✓ Passive Storage

✓ Manual Searching

✓ Lack of Correlation

✓ Delayed Alerting



Logchase SIEM

Logs are analyzed, correlated, and enriched.

✓ Active Analysis

✓ Instant Search

✓ Powerful Correlation Engine

✓ Real-time Alerting

Proactive

Threat Detection

Threat Monitoring

Identify suspicious activities instantly with real-time threat detection and intervene before incidents escalate. Proactively manage security risks through advanced analytics and alerting mechanisms.



Behavioral Anomaly Detection

Detect unusual activity patterns.

Abnormal Login Frequency

Anomalous Geo-locations

Unexpected File Access

Privilege Abuse

Transform your security posture into a proactive model by detecting threats in real-time with Logchase. By analyzing log data from diverse sources instantly, the system uncovers suspicious activities before they escalate, enabling rapid response and decisive action. This ensures that potential attacks are identified at their inception and neutralized before they can impact your critical systems. With advanced correlation, alerting, and analytical capabilities, you can move beyond isolated incidents to focus on the interconnected relationships between events. This translates into deeper visibility and higher accuracy in threat detection. Logchase not only reduces the manual workload on security teams but also enhances operational efficiency through rapid response capabilities, ultimately strengthening your organization's cybersecurity resilience.

Threat Intelligence Integration

Enriched threat data powered by Threat.live and AbuseIPDB integrations. Match your logs against known malicious indicators in real-time.

Malicious IP Addresses

Botnet Activity

TOR Exit Nodes

Brute Force Sources

Suspicious Activity Detection

Suspicious Activity Detection provides rapid response capabilities by identifying risky behaviors—such as brute force attacks, privilege escalation attempts, and lateral movement—at an early stage.



BRUTE FORCE ATTACKS

Detect brute force attacks early by analyzing high volumes of failed login attempts. Take swift action with automated alerts to safeguard account security.



WEBSHELL UPLOADS

Block potential backdoors by detecting suspicious scripts and files uploaded to servers. Maintain system integrity by identifying unauthorized access attempts in their infancy.



PRIVILEGE ESCALATION

Identify elevation-of-privilege attempts by monitoring activities that exceed a user's standard permission levels. Intervene immediately to prevent unauthorized access to critical systems.



SUSPICIOUS PROCESS EXECUTION

Uncover anomalous behaviors by analyzing unexpected or potentially malicious processes. Continuously monitor active system operations to detect threats at the earliest possible stage.



LATERAL MOVEMENT ATTEMPTS

Prevent threat propagation by detecting adversary activities moving horizontally across your network. Break the attack chain by analyzing suspicious connections between disparate systems.

Risk Scoring

Each event can be assigned a risk score to streamline investigation prioritization.

100-85
CRITICAL

Active Attack Indicators

84-50
HIGH

Suspicious Activity Patterns

49-25
MEDIUM

Significant Security Events

24-0
LOW

Informational Events

Logchase delivers real-time threat detection capabilities, including behavioral anomaly detection, threat intelligence integration, suspicious activity monitoring, and risk scoring.

Security teams can identify brute force attacks, webshell deployments, privilege escalation attempts, and lateral movement across their entire infrastructure. By automating the identification of these threats, Logchase ensures that critical risks are prioritized, allowing for faster response and enhanced cyber resilience.

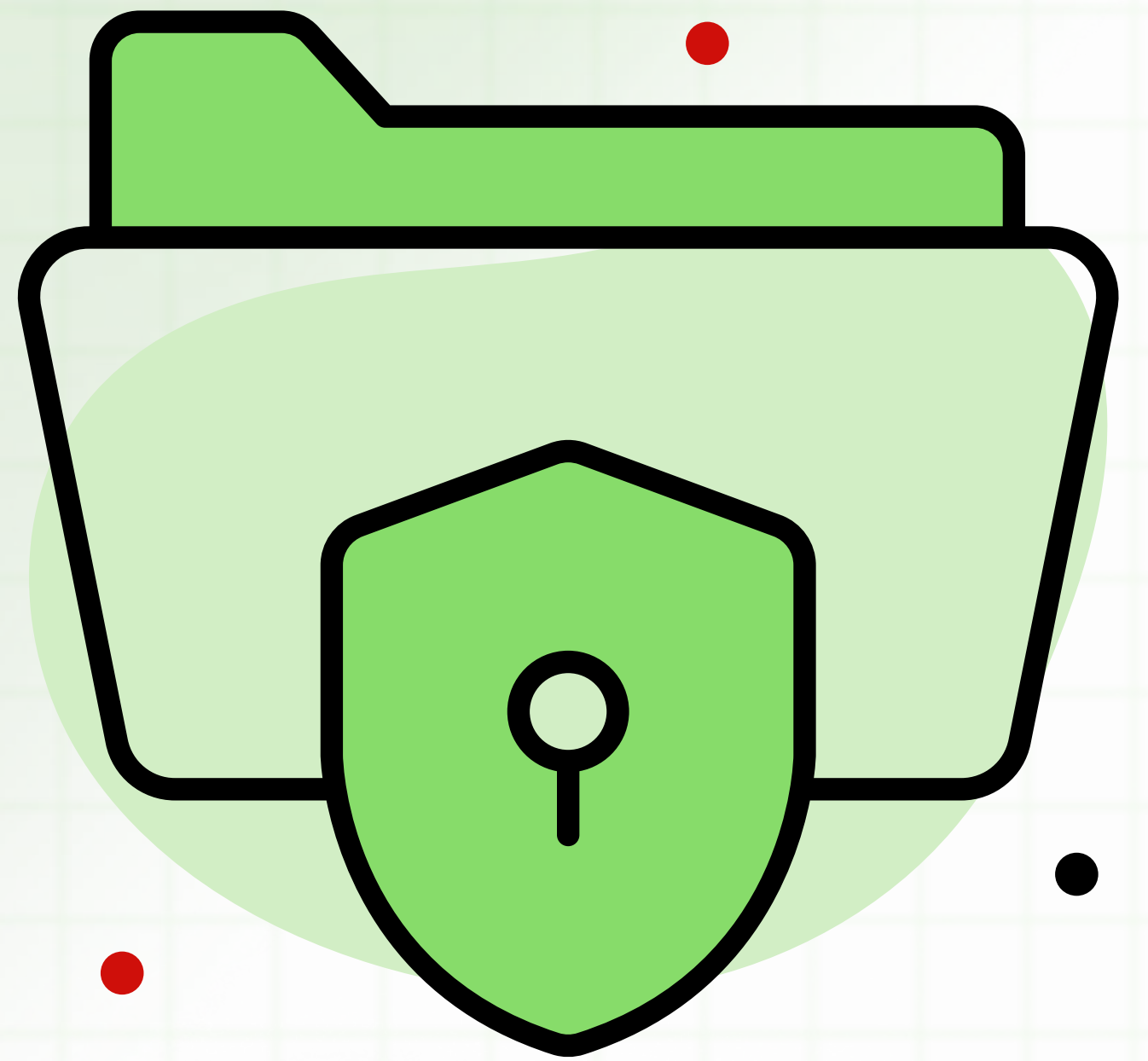
File Integrity

FIM

Monitoring

Detect unauthorized file changes on your Linux and Windows servers in real-time.

Logchase FIM continuously monitors critical files and directories, identifies unauthorized modifications, and alerts security teams before incidents escalate.



File Integrity Monitoring (FIM) is a security-enhancing solution that monitors file and directory changes across systems in real-time. It detects and provides detailed reporting on critical operations such as file creation, deletion, or modification. By generating instant alerts for suspicious changes, it enables rapid response. Furthermore, it helps meet compliance requirements and maintains constant control over system integrity, ensuring more effective management of both security and audit processes.

File Integrity Monitoring

What is?



Unauthorized File Modifications



Malware / Webshell Deployment



Ransomware Activity



Configuration Changes



Privilege Escalation Attempts



Insider Threats

File Integrity Monitoring (FIM) is a critical security control that detects changes in files, directories, and system configurations. Logchase FIM provides real-time visibility into file-level activities across Linux and Windows environments using lightweight agents, ensuring minimal impact on system performance while maintaining maximum security.



logchase

FIM CORE FEATURES

About Core Features

Logchase FIM provides real-time monitoring of all modifications across files and directories, delivering comprehensive visibility into what was changed, when, and by whom. With flexible monitoring policies and an intelligent alerting system, it ensures critical changes are detected instantly for rapid response. Its lightweight, cross-platform agents deliver high performance across both Linux and Windows environments.

FIM CORE FEATURES

Real-Time File Change Detection

Monitor critical files and directories across your Linux and Windows servers.

- File Creation
- File Deletion
- Permission Changes
- File Renaming
- Content Modification
- Hash Modification



FIM CORE FEATURES

Intelligent Alerting System

Define alert levels based on the sensitivity of modifications.

- By File Path
- By File Type
- By Modification Type
- By Hash Modification
- By File Extension Rules
- By User Identity

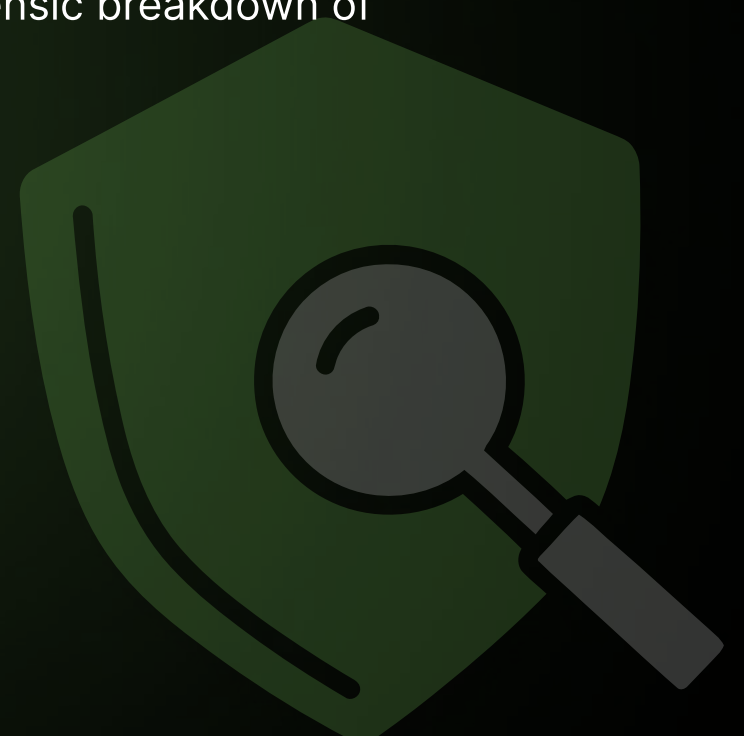


FIM CORE FEATURES

Detailed Change Visibility

Logchase FIM goes beyond simple detection—it provides a comprehensive forensic breakdown of exactly what was modified.

- Inserted Lines
- Deleted Lines
- Previous vs. New Hash
- Affected User
- Associated Process
- Change Timestamp

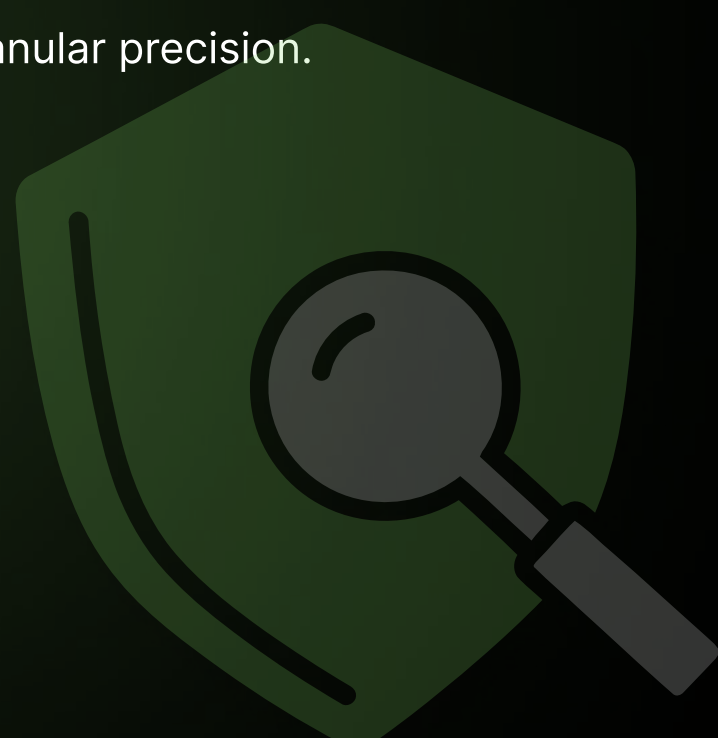


FIM CORE FEATURES

Flexible Monitoring Policies

Monitor specific files, directories, extensions, or application codebases with granular precision.

- /etc
- /var/www
- C:\inetpub
- config files
- scripts
- binaries

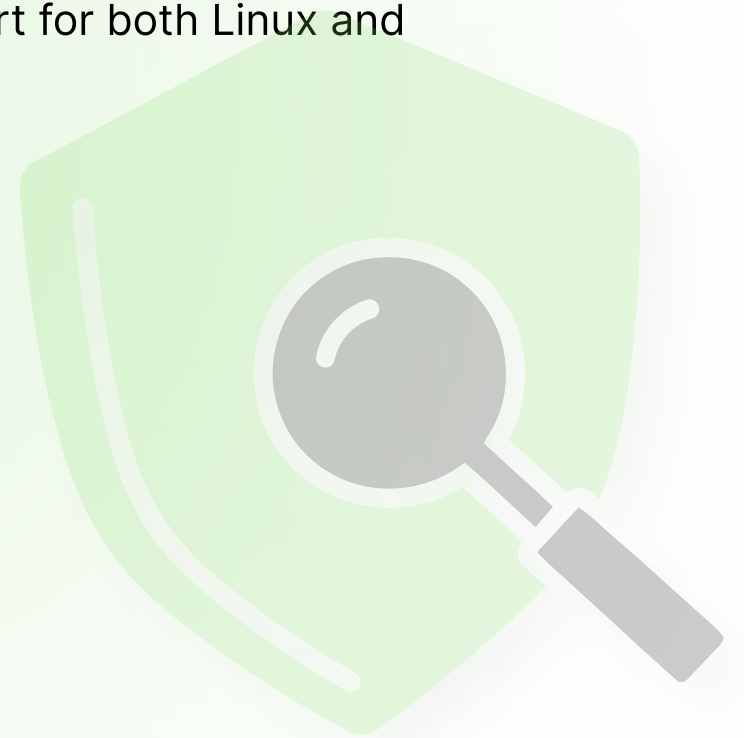


FIM CORE FEATURES

Cross-Platform Agents

Lightweight architecture with minimal performance impact. Comprehensive support for both Linux and Windows environments.

- Linux Servers
- Windows Servers
- Ubuntu Servers
- Centos Servers



USE CASES

Logchase FIM supports a wide range of security scenarios where file integrity is mission-critical.



WEBSHELL DETECTION

Detect unexpected PHP, ASPX, or script files uploaded to web directories. Identify potential backdoors before they are executed. `/var/www/html/uploads/shell.php`



CONFIGURATION CHANGE MONITORING

Track modifications in system configuration files across all extensions. *Ensure your infrastructure remains in its "known-good" state.*



RANSOMWARE ACTIVITY DETECTION

Detect anomalous mass-scale file modifications or encryption patterns.



INSIDER THREAT DETECTION

Monitor unauthorized modifications made by privileged accounts. Gain visibility into internal activities that bypass traditional security layers.



COMPLIANCE MONITORING

Seamlessly support regulatory frameworks that mandate file integrity monitoring: *PCI DSS ISO 27001 SOC 2 HIPAA*

Protect system integrity by monitoring all critical activities, including file creation, deletion, modification, and permission changes. Leverage cryptographic hash verification and rule-based monitoring for reliable analysis and flexible, policy-driven control.

Supported Change Types

- File created
- File deleted
- File modified

- File renamed
- Permission changed
- Hash changed
- Ownership changed

FIM TECHNICAL SPECIFICATIONS

Hash Verification

Verify file integrity using cryptographic hash algorithms to rapidly detect unauthorized changes. Leverage SHA-256 for secure analysis while maintaining compliance through support for legacy methods.

- SHA-256
- SHA-1
- MD5



FIM TECHNICAL SPECIFICATIONS

Rule-Based Monitoring

Define your monitoring scope by creating customizable rules based on directory, file extension, and sensitivity levels. Monitor critical files with environment-specific policies to keep all modifications under control.

- Directory-Based
- Extension-Based
- Sensitivity Level
- Environment-Based

Logchase FIM continuously monitors critical system files to make unauthorized modifications visible, providing security teams with immediate control. Its flexible rule structure and detailed change analysis enable the management of both security and compliance processes from a single platform. Furthermore, its lightweight agent architecture ensures operation across diverse environments with minimal performance impact.

Intelligent Alarm Levels

Automatically define alert levels based on the sensitivity of the modification.

Critical System File Modification CRITICAL /etc/passwd, /etc/shadow	System Configuration Change HIGH /etc/passwd, /etc/shadow	Application Config Modification MEDIUM nginx.conf, web.config	Log File Rotation/Change LOW /var/log/*, application logs
--	--	--	--

Intelligent alarm levels automatically classify file changes by sensitivity, prioritizing critical events. This allows security teams to focus rapidly on significant threats while easily distinguishing low-priority modifications.



Why?

Logchase Partner

Attractive Profit Margins

Grow your business with competitive partner discounts and high-profit margins designed to maximize your ROI.

Comprehensive Training

Empower your team with specialized sales and technical training programs to turn them into certified Logchase experts.

Dedicated Technical Support

Access full technical assistance and expert guidance throughout both pre-sales and post-sales processes.

Marketing Support

Boost your visibility through joint marketing initiatives, co-branded campaigns, and verified customer success stories.

Lead Generation & Distribution

We fuel your growth by sharing qualified sales leads and potential customer opportunities within your region.

Official Certification

Gain industry recognition with the official Logchase Partner certificate and authorized brand usage rights.

Step 3

Following the evaluation, the Logchase team will contact you to complete the final steps of your application.

Step 4

Upon admission to the program, you will undergo a comprehensive training and certification process to ensure technical and sales excellence.

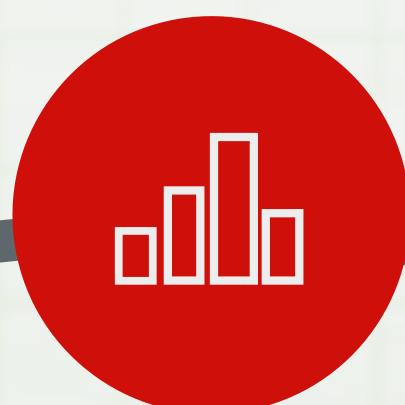
Step 2

Once your preliminary application is approved, our sales team will reach out to schedule an introductory meeting.



Step 1

Fill out the preliminary application form on our official website to start your journey.



Step 5

Congratulations! After successfully completing the certification, you are now an official Logchase Partner.



Scan The QR Code To Access
The Application Page And
Join Our Network Today.



Centralized **Log** Management and **SIEM** Platform

We have briefly summarized what you can achieve with **Logchase.
Contact us today to discover how we can secure your digital future.**

Logchase provides end-to-end visibility by unifying critical security needs—including Log Management, SIEM, Threat Detection, and FIM—into a single, powerful platform. With real-time analysis, robust correlation, and advanced search capabilities, security teams can detect and respond to incidents with unprecedented speed.

Our flexible architecture, extensive integration support, and versatile deployment options ensure seamless adaptation for organizations of any scale. By streamlining compliance requirements and simplifying audit processes, Logchase makes security operations faster, more efficient, and significantly more effective.



Guardian of Your Critical Data



Active Correlation Engine



Out-of-the-Box Detection Logic



Real-Time SOC Workflow

Contact Us



+90 (850) 305 88 66



info@logchase.com



www.logchase.com



Ataket Mah. Dicle Cd. No:9/A
Ümraniye/İSTANBUL



8 The Green Suite 13105
Dover, DE, 19901, USA