CyberFortress

PLATFORM DATASHEET

MA 360°

The core that powers every layer of defence

MA 360° is not one more product in the stack. It is the processing, analysis and orchestration engine at the centre of the platform – where telemetry from every security layer is collected, correlated and turned into a decision.

cyber-fortress.com | info@cyber-fortress.com

THE PLATFORM

One core. One data model. One console.

Whichever vector an attack arrives from, it lands in the same engine and is analysed down to the last detail. That is what separates a platform from a bundle of products: a file seen in an email attachment, the endpoint that opened it and the cloud bucket it reached are not three alerts – they are one incident.

MA 360° — the platform core

Collects telemetry from every security layer, correlates it in real time and orchestrates the response. Detection, classification and containment decisions are produced in milliseconds, and the analysis engine absorbs up to 80% of the manual triage an L1/L2 team would otherwise carry.

THE MODULES THE CORE DRIVES

Malware Analyzer 360

Dynamic sandbox, static analysis, URL verdicts and CDR for unknown and targeted attacks. Every verdict ships with extracted IOCs and an automatic MITRE ATT&CK mapping.

Mail Gateway

Multi-layered protection against phishing, BEC, ransomware and mail-borne APTs, with click-time URL rewrite and inline or BCC deployment.

Threat Hunter

Lightweight agent, automatic triage, YARA sweeps, screen watermarking, tamper protection and air-gap kiosk and bridge support.

Cloud Hunter

Container and image analysis, bucket scanning and real-time cloud file system protection across hybrid and multi-cloud estates.

Data Layer with CyberFortress TI

Multi-source threat intelligence and real-time correlation across terabytes a day – the backbone every module reads from and writes back to.

UI, API, Agent & 3rd Party

Open architecture – 43 ready integrations that extend the platform without replacing what you already own.

WHY THE CORE MATTERS

Six jobs everything else depends on

Every security product produces alerts. Very few produce decisions. The difference is whether anything in the estate is holding the whole picture at the moment a judgement has to be made – and that is the job of the core.

Agents, APIs and third-party connectors feed logs, sandbox verdicts, endpoint telemetry, mail flow and cloud activity into one normalised model, so the tooling you already own keeps its value instead of being replaced. The Data Layer attaches threat intelligence, historical context and behavioural baselines. CyberFortress AI classifies the behaviour and scores the risk.

Then the core acts. One verdict, many actions: isolate the endpoint, quarantine the message, push an IOC to the SIEM and open the ticket — driving both the platform's own modules and your existing SOAR playbooks from the same decision, in milliseconds rather than minutes. Against slow, quiet APT campaigns that difference is the whole game.

WHAT THE CORE ACTUALLY DOES

Unified data collection
Every source normalised into one shared model.

Real-time processing
Decisions in milliseconds rather than minutes.

Deep correlation
Three alerts become one described incident.

Orchestration
One verdict drives every module and your SOAR.

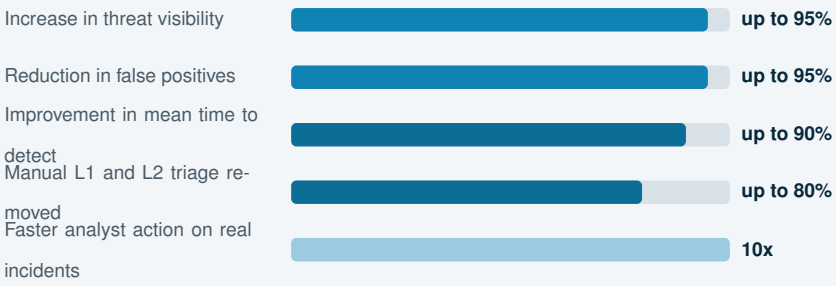
360°
Endpoint, email, cloud and network telemetry in a single pane

< 1 sec
Detection, classification and response decisions

80%
Less manual triage work for your security analysts

Millions
Events and malicious activities processed every second

What correlation and enrichment change



Figures reported by teams running the platform against their previous tooling. The gains come from context, not from a bigger alert list — enriched incidents replace raw events.

HOW IT WORKS

From signal to action

Every event entering the platform follows the same four steps, whatever module produced it. That uniformity is what makes a new module useful on the day it is switched on.

The four steps every event follows

01
Collect
Endpoint agents, mail gateway hooks, cloud connectors and API calls stream raw telemetry in continuously.

02
Enrich
The Data Layer adds threat intelligence, historical context and behavioural baselines.

03
Decide
CyberFortress AI classifies the behaviour, scores the risk and maps it to MITRE ATT&CK.

04
Act
Containment fires across the relevant modules and out to SIEM, SOAR, EDR and ticketing.

Collection is continuous, enrichment is automatic, and the decision carries the actions with it. No step waits for a human unless the policy says it should.

Six responsibilities

Unified data collection
Agents, APIs and third-party connectors feed logs, sandbox verdicts, endpoint telemetry, mail flow and cloud activity into one normalised model.

Real-time processing
Detection, classification and response are produced in milliseconds — the attack is stopped before it has an effect to measure.

Deep correlation
The core joins related events across modules, time and assets, enriches them and presents the whole chain rather than its fragments.

Orchestration
One verdict, many actions: isolate, quarantine, push an IOC, open the ticket – across the platform's modules and your own playbooks.

Analyst leverage
The analysis engine removes up to 80% of the manual work an L1/L2 team would otherwise carry, so analysts spend their hours on the cases that need a human.

Scale that holds
A high-performance architecture built to sustain millions of events per second – the same engine runs a mid-size enterprise and a national-scale environment.

The layers underneath

CyberFortress AI — behavioural intelligence

Four security modules — analysis and enforcement

MA 360° — collection and orchestration

Data Layer with CF TI — correlation and context

What feeds the Data Layer

CyberFortress Threat Intelligence – our own operation, informed by the malware we analyse at scale every day.

Internal platform telemetry – logs, sandbox verdicts, URL results, endpoint telemetry, container behaviour and cloud activity.

Third-party intelligence – external commercial and community feeds, so you are never limited to one vendor's view.

Machine learning baselines – models learn normal behaviour from your own data and mark anomalies automatically.

OPEN ARCHITECTURE

Extend your stack without replacing it

The point is not to become your only security vendor – it is to make the tools you have already paid for work harder. Lightweight agents collect from endpoints with a minimal footprint, and a RESTful API connects the engine to more than 40 security tools with bi-directional data and action flow.

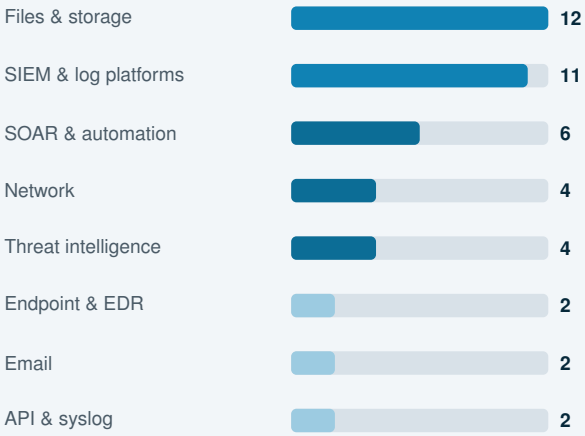
43
Integrations available today across eight categories

16
Built-in connectors requiring no code at all

2-way
Bi-directional data *and* action flow, not just export

REST
Full API for anything that is not on the list

Where the 43 integrations sit



Sixteen ship as built-in connectors; the rest connect over the RESTful API or syslog. Anything not listed can be wired up directly.

Two ways in

Agent-based collection. Lightweight agents gather data automatically from endpoints, giving maximum visibility with a minimal load on the machine. They work naturally alongside the endpoint and email security modules.

RESTful API. The open API connects the engine to more than 40 security tools with bi-directional flow, and is equally available for whatever you have built in-house – submit files and URLs, poll or receive verdicts, pull full reports and IOCs, and drive platform actions.

One alarm, one orchestrated response

01 Alarm
The SIEM raises an alarm on anomalous outbound traffic.

02 Playbook
The SOAR playbook fires automatically, with no analyst in the loop.

03 Contain
MA 360° isolates the endpoint and submits the suspect file.

04 Analyse
The sandbox returns a verdict with IOCs and ATT&CK mapping.

05 Enforce
IOCs push out to the EDR and the firewall automatically.

06 Record
The ticket updates itself and the audit trail closes.

Moving records between systems is the easy half – the value shows up when the connection carries actions as well as data. What used to be a sequence of human handoffs becomes a single flow.

IN PRACTICE

What the core changes day to day

The core is deployed once and every module switched on afterwards gets sharper for it. These are the differences teams report first.

One incident instead of three alerts

A file seen in an email attachment, the endpoint that opened it and the cloud bucket it reached are joined into a single storyline with the whole chain visible, rather than three tickets in three consoles.

A queue that orders itself

Automatic severity ranking puts the cases that need judgement at the top. Known-clean and known-bad drop out immediately.

Existing tooling keeps its value

SIEM, SOAR, EDR and ticketing stay where they are and get better data. The security data lake remains authoritative and the dashboards your team already watches keep working.

Containment without a handoff

Isolating an endpoint, quarantining a message and pushing an IOC are all driven from the same verdict, in the same second, without a human relaying it between systems.

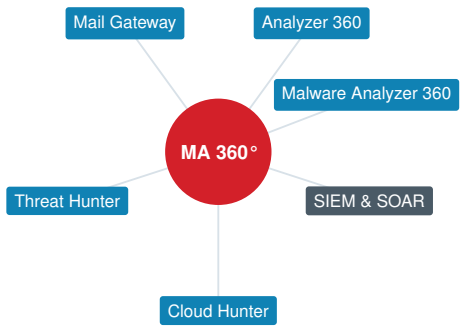
Scale without redesign

The same engine runs a mid-size enterprise and a national-scale environment under heavy threat traffic – millions of events per second on a high-performance architecture.

Analysts on the work that needs them

Up to 80% of L1/L2 triage is absorbed by the engine, and the alerts that do arrive are enriched enough to be worth opening.

What one verdict reaches



Decision	classified and scored
Containment	isolate, quarantine, block
Distribution	IOCs to SIEM, EDR, firewall
Record	ticket and audit trail

See the core running on your own data.

Start a 30-day proof of concept in your own environment, or book a technical architecture session with your security team.

cyber-fortress.com
info@cyber-fortress.com

SPECIFICATION

Features and capabilities

DATA COLLECTION

- Endpoint agents, mail gateway hooks and cloud connectors
- RESTful API submission from any tool you already run
- Third-party connectors for existing security products
- Logs, event records and sandbox verdicts ingested together
- Everything normalised into one shared data model
- Terabytes a day sustained by high-performance engines
- Existing tooling investments keep their value

PROCESSING & CORRELATION

- Detection, classification and response in under a second
- Millions of events per second sustained
- Real-time correlation across modules, time and assets
- Related events joined into a single incident storyline
- Enrichment with CyberFortress Threat Intelligence
- Historical context and behavioural baselines attached
- Up to 95% increase in threat visibility through enrichment
- Up to 95% reduction in false positives

DECISION & CLASSIFICATION

- CyberFortress AI behavioural classification in milliseconds
- LLM and machine-learning threat interpretation
- Risk scoring rather than a bare verdict
- Automatic MITRE ATT&CK tactic and technique mapping
- Adaptive learning from every incident
- Anomaly detection against your own baseline
- Up to 90% improvement in mean time to detect

ORCHESTRATION & RESPONSE

- One verdict drives every module simultaneously
- Endpoint isolation on decision
- Message quarantine and retrospective removal
- IOC push to SIEM, EDR and firewall
- Ticket creation, update and closure
- Existing SOAR playbooks driven from the same decision
- Playbooks can call back into the core for analysis

ANALYST EXPERIENCE

- Single pane across endpoint, email, cloud and network telemetry
- Automatic triage and severity ranking of the queue
- Up to 80% of manual L1/L2 work absorbed
- 10x faster analyst action on real incidents
- Plain-language findings and remediation steps
- AI assistant interprets results for L1 and L2 analysts
- Full incident chain navigable rather than a flat alert list

MODULES DRIVEN

- Malware Analyzer 360 – sandbox, static analysis, URL and CDR
- Mail Gateway – phishing, BEC, ransomware and mail-borne APTs
- Threat Hunter – endpoint agent, YARA sweeps and air-gap modes
- Cloud Hunter – container, bucket and cloud file system
- Each deployable on its own, each sharper with the others on

INTEGRATIONS

- 43 integrations across eight categories – 16 built-in
- RESTful API with bi-directional data and action flow
- SIEM: Splunk, Sentinel, QRadar, Elastic, LogRhythm, ArcSight, Chronicle, Graylog, Wazuh, Sumo Logic, Rapid7 InsightIDR
- SOAR: Cortex XSOAR, Splunk SOAR, FortiSOAR, Tines, Swimlane, Torq
- EDR/EPP: CrowdStrike Falcon and Microsoft Defender
- Threat intelligence: MISP, OpenCTI, ThreatQ, Anomali ThreatStream
- Cloud storage: SharePoint, OneDrive, Drive, Box, Dropbox, S3, Azure Blob, Nextcloud
- Network: ICAP proxy, TAP interface, Broadcom CAS, OPSWAT MetaDefender
- Email: IMAP and Postfix mail flow
- Syslog streaming for everything else

DEPLOYMENT & SCALE

- On-premise, cloud or hybrid deployment
- Air-gapped deployment with kiosk and bridge modes
- Scales from a single node to national-scale estates
- High-performance architecture under heavy threat traffic
- Seamless product update with a single click

ADMINISTRATION

- Role-based user management
- Role restriction on who may read analysis results
- Central policy, quarantine and reporting
- Back up and restore your data
- Health monitor for every engine
- Real-time disk capacity monitoring
- PDF, CSV, JSON and HTML report generation
- Full audit trail of decisions and admin actions

CyberFortress

One core. Every layer feeds it.

MA 360° is the engine the four security modules run on. Start with one module or all of them – the core is what makes the difference between a set of products and a security system.

THE PLATFORM AT A GLANCE

MA 360°
The core — collection, correlation and orchestration.

Malware Analyzer 360
Sandbox, static analysis, URL verdicts and CDR.

CyberFortress TI
Comprehensive Threat intelligence and analytics.

Mail Gateway
Phishing, BEC, ransomware and mail-borne APTs.

Threat Hunter
Lightweight agent, YARA sweeps and air-gap modes.

Cloud Hunter
Container, bucket and cloud file system protection.

CyberFortress AI
Behavioural analytics wrapping every module.

cyber-fortress.com
info@cyber-fortress.com