CyberFortress

PRODUCT DATASHEET

Malware Analyzer 360

Advanced Malware and URL Analysis

Signature-based tools only catch what someone has already named. Malware Analyzer 360 judges files, links and behaviour by what they actually do – so zero-day and APT activity surfaces before it takes hold.

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

THE PLATFORM

One core. Every layer feeds it.

CyberFortress is not a catalogue of separate tools. Every module streams its telemetry into a single core, is enriched by shared threat intelligence, and is read by one intelligence layer – so a malicious file caught in the mail flow and the endpoint that already received a copy are one incident, not two.

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 seconds, and the analysis engine absorbs up to 80% of the manual triage an L1/L2 team would otherwise carry.

THE FOUR SECURITY MODULES

Malware Analyzer 360

Dynamic sandbox detonation, static code inspection, live URL verdicts and Content Disarm & Reconstruction. Every verdict ships with extracted IOCs and an automatic MITRE ATT&CK mapping.

Mail Gateway

Multi-layered defence against phishing, BEC, ransomware and mail-borne APTs. AI anti-phishing, attachment sandboxing, click-time URL rewrite, inline and BCC deployment, plus an Outlook add-in.

Threat Hunter

A lightweight endpoint agent backed by central analysis – USB, share and download control, automatic triage, YARA sweeps, screen watermarking, tamper protection and air-gap kiosk and bridge modes.

Cloud Hunter

Container and image analysis with CVE-based scanning, bucket exposure checks, cloud file system protection and real-time monitoring 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.

CyberFortress AI

Behavioural analytics and millisecond classification wrapping the whole platform, learning from every event and cutting false positives as it goes.

WHY MALWARE ANALYZER 360

Judged on behaviour, not on a name

An advanced attack is built to evade the controls you already own. It arrives unnamed, hides its payload, checks whether it is running in a virtual machine, and waits. Signature matching cannot describe something nobody has published yet.

Malware Analyzer 360 answers a different question: not *have we seen this file before*, but *is this process doing something a legitimate process would never do*. The sample is detonated inside a hardened, isolated environment where every system call, registry change, memory movement, network connection and spawned process is recorded as it happens – while a static pass reads the file at code level without ever running it, extracting signatures, suspicious API calls, packing and obfuscation.

The two methods together close the gap either leaves alone: strong coverage of known families *and* of zero-day samples. Evasion does not help. Malware that sleeps, hides or fingerprints the sandbox still has to act eventually, and when it does the behavioural trace gives it away.

QUARANTINE IN VIRTUAL MACHINES

Detonate
Executed in a customised, fully isolated VM.

Watch
Thousands of pattern checks and placed sensors record every action.

Analyse
AI-powered multi-flow analysis establishes the full context of the attack.

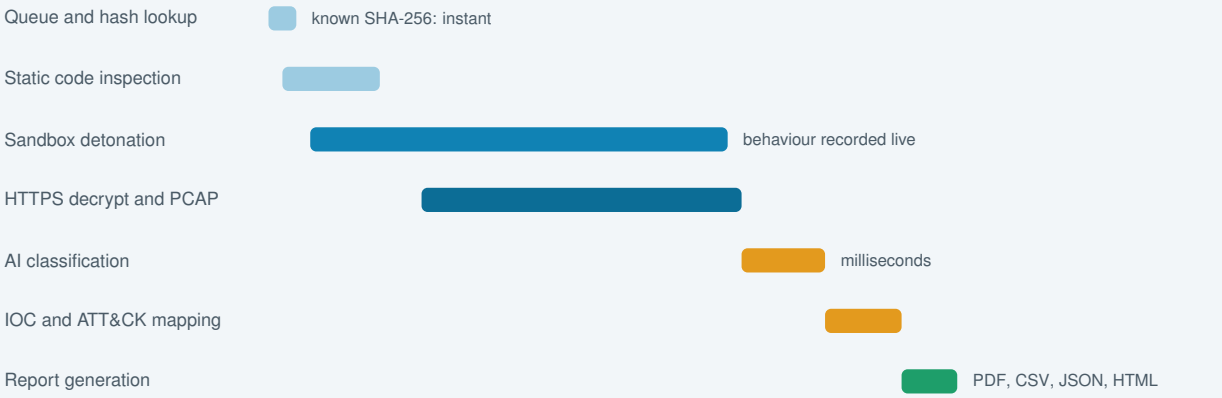
99.7%
Detection rate across known and previously unseen samples

~2 min
Full triage report for an APT sample, static and dynamic

18
Distinct characteristics every attack is profiled against

ATT&CK
Findings mapped to tactics, techniques and procedures

From submission to report – where the two minutes go



Indicative timings for an APT-grade Windows sample. Passes run concurrently; the static read is already finished while detonation is still recording.

INSIDE THE ENGINE

Four analysis layers, one verdict

A file or link entering the analyzer is examined from every angle at once. Behaviour is watched in isolation, code is read without ever being run, destinations are resolved live, and anything reaching a user can be rebuilt clean before it arrives.

Dynamic analysis

The sample is executed inside a hardened, isolated environment where every system call, registry change, memory movement, network connection and spawned process is recorded in real time. Free-Run technology lets an analyst watch the malicious activity as it happens.

Static analysis

The file is read without being run: signature extraction, suspicious API and function calls, packing and obfuscation techniques, embedded resources and known malicious code patterns.

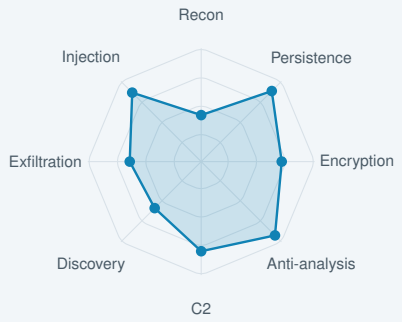
URL analysis

Links are resolved and followed through redirects to their real destination – phishing and credential-harvesting pages, command & control endpoints and drive-by download chains – without exposing a single production machine.

Content Disarm & Reconstruction

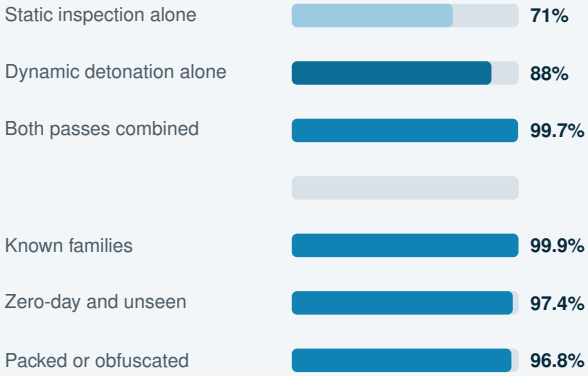
CDR strips active content – macros, embedded scripts, malformed structures – and rebuilds the document as a clean, usable file, so the business is not waiting on a verdict it cannot afford to wait for.

Behavioural classification



Illustrative profile for a banking-trojan sample. Every attack is scored probabilistically against 18 characteristics rather than reduced to a single verdict.

Why both passes run



Coverage of an internal corpus mixing named families with previously unseen samples. Neither method reaches the combined figure on its own, and the combined engine holds up where evasion is deliberate.

WHAT THE ANALYST GETS BACK

Attack Map

A fully dynamic map of the execution chain – every process, file and system change the sample produced, navigable branch by branch.

Classification

AI-driven probabilistic scoring across the 18-characteristic spectrum, presented as a radar chart so family and intent are visible at a glance.

Network Traffic

After decrypting HTTPS traffic, contacted domains and ports are shown geographically – exposing the C2 infrastructure and where data was headed.

Full Report

A comprehensive report including all findings, indicators, and ATT&CK mappings.

IOC List

A comprehensive list of indicators of compromise extracted from the analysis.

OPEN ARCHITECTURE

Fits the stack you already run

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.

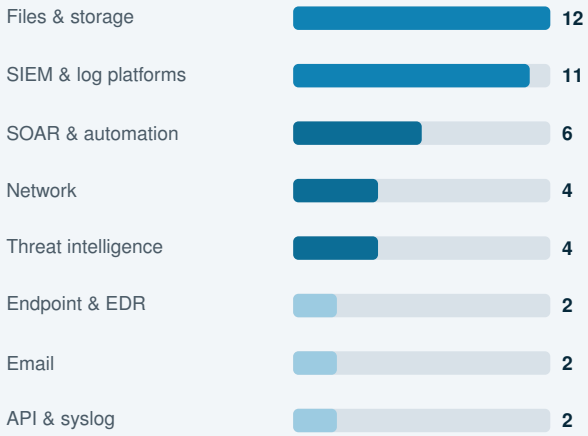
43
Integrations available today across eight categories

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

Where teams put it to work

The analyzer runs as a service behind the rest of the platform – and answers directly to your own tooling through the API.

Email attachments

Every attachment arriving through Mail Gateway is detonated and, where policy requires it, rebuilt clean with CDR before delivery.

User-uploaded files

Portals, ticketing systems, SharePoint, OneDrive and file shares submit uploads for a verdict before the file is ever stored or opened.

Suspicious URLs

Analysts and automated playbooks resolve a link's real destination and intent without exposing a single production machine to it.

APT hunting on endpoints

Suspicious artefacts collected by Threat Hunter are sent back to the analyzer, turning a quiet anomaly into a named, mapped intrusion.

Forensic and IR case work

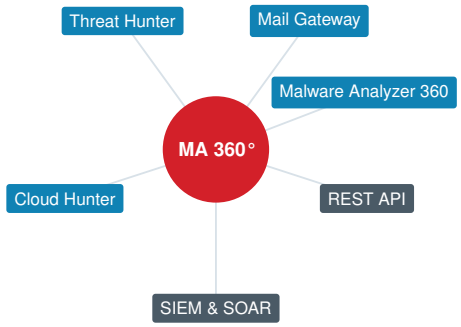
Bulk submission, retained logs, screenshots and process timelines give incident responders the evidence trail a case actually has to produce.

SOC escalation

The case an L1 analyst could not close comes back with a definitive answer instead of an inconclusive verdict passed further up the chain.

One submission, many destinations

A verdict is not the end of the process. Extracted indicators are pushed straight into the tools that enforce them, and the incident record updates itself.



Verdict	malicious or clean
IOCs	hashes and infrastructure
ATT&CK mapping	tactics and techniques
Report	PDF, CSV, JSON, HTML

Send us the sample that got through.

Run a 30-day proof of concept inside your own environment, or bring us the file that came back inconclusive elsewhere.

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

SPECIFICATION

Features and capabilities

DETECTION & ANALYSIS ENGINES

- Dynamic behavioural analysis in a hardened, isolated sandbox
- Static code inspection with no execution of the sample
- Live URL analysis with full redirect chain resolution
- Content Disarm & Reconstruction for documents and archives
- AI-driven probabilistic conclusions on *Malicious* and *Clean*
- Attacks profiled across 18 distinct characteristics
- Packed, obfuscated and polymorphic samples caught by behaviour
- Multi-stage attack chains followed through every stage
- Sleep, VM-check and other sandbox-evasion techniques defeated
- Snort and Suricata signature matching
- YARA rule matching against submissions and retained artefacts
- Parallel concurrent analysis that holds up under high volume
- Memory, process, registry, file system and network sensors
- Thousands of behavioural pattern checks per detonation

COVERAGE

- All file types, including nested and password-protected archives
- Office documents, PDFs, scripts, installers and executables
- Windows, Linux, Android and container payloads
- Fully customisable VM images and installed software
- Custom detonation timeouts, locales and network profiles
- Submissions by file, by URL, in bulk or through the API

ANALYSIS & REPORTING

- Fully dynamic Attack Map to navigate the attack topography
- Interactive artefact and network maps with drill-down
- Observe malicious activity live in VMs via Free-Run technology
- Probabilistic classification presented as a radar chart
- Decrypts HTTPS traffic and maps activity origins and destinations
- Contacted domains and ports displayed geographically
- Operation logs with associated vulnerability matches
- Download memory dumps, dropped files, extracted payloads and PCAPs
- Screenshots and process timelines retained per submission
- Automatic IOC extraction – hashes, domains, IPs, mutexes and dropped paths
- Automatic MITRE ATT&CK tactic and technique mapping
- VirusTotal, YARA and MITRE ATT&CK integration
- Instant reports for previously analysed files, SHA-256 verified
- Generates PDF, CSV, JSON and HTML reports
- Evidence-grade retention for forensic and compliance use
- AI assistant interprets findings in plain language

AUTOMATIC TRIAGE

- Severity scoring ranks the submission queue automatically
- Known-clean and known-bad drop out of the queue immediately
- Absorbs up to 80% of the manual work of an L1/L2 team
- Quiet, long-running malicious activity surfaced rather than buried

NOTIFICATIONS

- Sends customisable logs to your syslog server
- Emails analysis results in any specified format
- Distributes dynamic, user-friendly reports to third parties
- Webhook callbacks on verdict completion

SYSTEMS & INTEGRATIONS

- 43 integrations across eight categories – 16 built-in connectors
- 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
- IMAP and SMTP integration; Postfix mail flow
- Cloud storage – SharePoint, OneDrive, Drive, Box, Dropbox, S3, Azure Blob, Nextcloud
- Local file-sharing system and FTP/SFTP integration
- ICAP proxy and network TAP interface integration
- Broadcom CAS and OPSWAT MetaDefender as upstream feeders
- Dedicated Outlook add-in
- Syslog streaming for everything else

DEPLOYMENT

- On-premise, cloud or hybrid deployment
- Air-gapped deployment with kiosk and bridge modes
- Scales from a single node to national-scale estates

RULE SETS & UPDATE CYCLE

- Overnight bots validate our algorithms against global malware databases
- AI is retrained whenever a shortcoming is observed
- Content team writes new rules daily from live attack research
- Custom YARA, Snort, Sigma and IOC content alongside ours
- Seamless product update with a single click

ADMINISTRATOR FUNCTIONS

- Role-based user management
- Role restriction on who may read analysis results
- Back up and restore your data
- Health monitor for every engine
- Real-time disk capacity monitoring
- Full audit trail of submissions and admin actions

CyberFortress

Because we detect the undetectable.

Malware Analyzer 360 is one of four modules on a single core. Deploy it on its own, or switch on the layers around it and let one verdict drive the whole estate.

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