CyberFortress

PRODUCT DATASHEET

# Threat Hunter

## Heavy analysis, lightweight agent

The endpoint is where users actually do their work – and where most intrusions become real. Threat Hunter covers corporate devices without turning them into analysis workstations: the agent stays small, the heavy work happens in the platform core.


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

THE PLATFORM

# The agent is small because the core is not

Events collected on the device are processed centrally by MA 360°, which runs the real-time detection. That split is the whole design: the endpoint keeps its performance and its manageability, while the advanced threat analysis – sandbox detonation, static inspection, behavioural classification – happens in the platform core where it belongs.

### MA 360° — the platform core

Collects telemetry from every security layer, correlates it in real time and orchestrates the response. Endpoint detections arrive already ranked by severity, already enriched with threat intelligence, and already correlated with what the mail flow and the cloud estate have seen.

THE FOUR SECURITY MODULES

### 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.

### Malware Analyzer 360

Dynamic sandbox detonation, static code inspection, live URL verdicts and CDR – where every suspicious artefact the agent collects is sent for a real verdict rather than a reputation lookup.

### Mail Gateway

Multi-layered defence against phishing, BEC, ransomware and mail-borne APTs. A weaponised attachment caught in the mail flow is swept for across the endpoint estate in the same motion.

### Cloud Hunter

Container and image analysis with CVE-based scanning, bucket exposure checks and cloud file system protection across hybrid and multi-cloud estates.

### Data Layer with CyberFortress TI

Device telemetry streams in; fresh IOCs and YARA rules come back out. The estate is checked against new intelligence rather than against a rule set frozen at install time.

### CyberFortress AI

Ranks endpoint detections by severity and surfaces quiet, long-running activity that a flat alert list would bury.

WHY THREAT HUNTER

# Detection waits. Hunting goes looking.

Detection waits for something to trip a rule. Hunting starts from a hypothesis – a new campaign in the news, an odd authentication pattern, a tip from an ISAC – and goes to check whether it is already inside.

Both need the same thing from the endpoint: an estate you can actually interrogate. Threat Hunter turns every connected device into something you can sweep with your own rules, collect artefacts from, and detonate what you find in the same engine that runs the rest of the platform.

The agent itself stays deliberately small. It watches the routes malware actually travels – USB devices, file shares, downloads, Outlook and the browser – enforces the controls that stop an intrusion early, and hands everything else to the core. Tamper protection keeps it running when an attacker tries to switch it off, which is one of the first things an intrusion does.

### WHERE THE WORK HAPPENS

**On the endpoint**
Collection, enforcement, USB and share control, watermarking, tamper protection.

**In MA 360°**
Real-time detection, sandbox detonation, correlation and severity ranking.

**In one console**
Policy, sweep results and reporting for the whole estate.

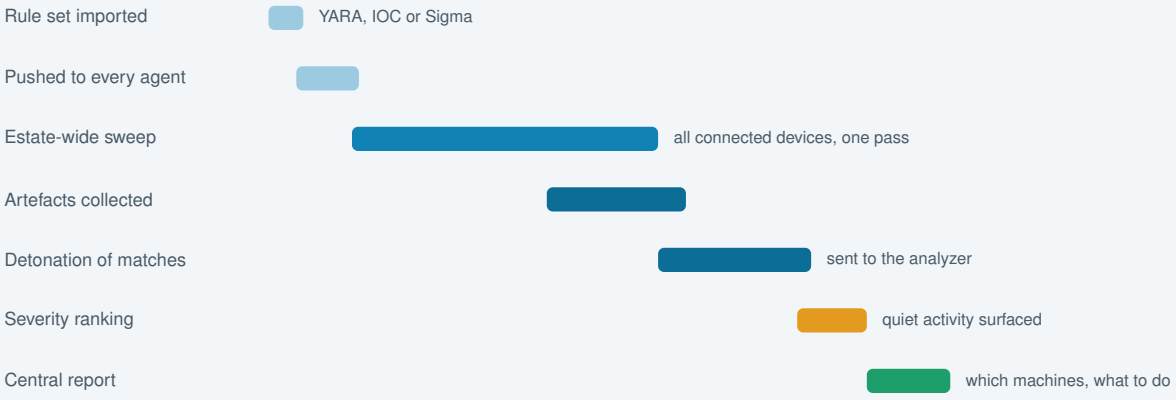
## Central
Detection runs in MA 360°, not on the endpoint

## YARA
Custom rule sets swept across every connected device

## Air-gap
Kiosk and bridge modes for isolated networks

## Always on
Tamper protection keeps the agent from being switched off

**Compromise assessment: one sweep, one answer**




Indicative shape of an estate-wide YARA sweep triggered by a fresh campaign report. The agent collects; the core analyses; the answer arrives as a ranked list rather than a pile of hits.

ON THE ENDPOINT

# Protection, visibility and control

Six capabilities run on the device – without the weight of a full analysis engine on every machine.

### APT control on real channels

USB devices, file shares and downloads are the routes malware actually travels. Files arriving on any of them are checked against MA 360°s real-time analysis before they get to run.

### Automatic triage

Detections are ranked by severity on the device itself, so the security team sees the critical cases first and quiet, long-running malicious activity still surfaces instead of being buried.

### Screen watermark

A dynamic, per-session watermark deters data exfiltration by photograph or screenshot, and makes insider activity traceable back to a user and a session – the one leak path that otherwise leaves no log.

### Tamper protection

Attackers disable security software early in an intrusion. Tamper protection blocks attempts to stop or remove the agent, keeping coverage continuously active.

### Outlook & browser integration

Extra inspection lands in the two applications users spend their day in, catching malicious attachments and links at the point of interaction rather than after the fact.

### YARA rule sweeps

Run your own YARA rule sets across every connected endpoint and get detailed, centrally reported findings – the fastest way to answer “are we affected?” during an active campaign.

### The leak path every other control leaves open

| How data leaves | Leaves a log | Attributable | Covered by |
|---|---|---|---|
| Copy and paste | yes | yes | DLP |
| Email and attachments | yes | yes | Mail Gateway |
| USB and removable media | yes | yes | Threat Hunter |
| Uploads and file shares | yes | yes | Proxy and analyzer |
| A camera pointed at the screen | no | yes | **Screen Watermark** |
| A screenshot of the screen | no | yes | **Screen Watermark** |
| A screenshot from Zoom/Teams | no | yes | **Screen Watermark** |

Copy, email, USB and uploads all produce a record an investigation can work from. A photograph of the screen produces no process, no file and no network event – nothing to work from afterwards. Watermarking is the control that operates on that path, because it works on what the eye and the lens both see.

## What the watermark actually does

### Identifies the session

Each session renders its own unique code, so any capture carries the identity of the machine and the person logged into it at that moment.

### Survives the camera

Because the mark is drawn into what the display shows, it is present in a phone photograph exactly as it is in a screenshot.

### Changes behaviour

Most of the value is preventive. Someone who can see their own identifier on screen understands that a photograph identifies them.

ISOLATED NETWORKS

# Protection inside air-gapped estates

Isolated networks are not a solved problem – they are a harder one. Files still have to cross the boundary, and when they do there is usually nothing watching. The endpoint agent can be deployed at that boundary in kiosk or bridge mode, so safe file flow and real threat analysis are possible even on systems with no route to the outside world.

### Kiosk mode

A dedicated station where staff scan removable media before it enters the secure zone. Nothing crosses the boundary until it has a verdict.

### Bridge mode

A controlled transfer point that analyses files as they move between isolated and connected segments, in both directions.

### Removable media

USB drives are treated as untrusted by default and inspected on every insertion – closing the oldest gap in endpoint security.

### Full audit trail

Every transfer and every verdict is recorded for compliance and later investigation, which is usually a requirement rather than a nicety in these environments.

### A file crossing the boundary in bridge mode

**01 Present**
Media is inserted at the kiosk or bridge station.

**02 Inventory**
Contents are enumerated and hashed, archives unpacked.

**03 Analyse**
Files go to MA 360° for static and dynamic analysis.

**04 Decide**
Clean, rebuilt with CDR, or blocked at the boundary.

**05 Transfer**
Approved content is released into the secure zone.

**06 Record**
Every transfer and verdict is written to the audit trail.

The same analysis engine that protects the connected estate runs at the air-gap boundary. Nothing is trusted because it arrived on physical media.

## Where isolated deployments are used

### OT and industrial

Production networks where a maintenance laptop or a vendor USB stick is the only route in – and historically the only route in for malware too.

### Defence and government

Classified segments that cannot reach the outside world but still have to accept documents and updates from it.

### Regulated research

Environments holding data whose exposure carries legal consequence, where every boundary crossing has to be evidenced.

IN PRACTICE

# Where teams put it to work

The scenarios endpoint teams reach for most often once the agent is deployed – and the loop a hunt actually runs in.

### Phish Control

When a user reports a suspicious message, Phish Control takes it from there: the attachment is detonated, the links are resolved and a spam review is started, without an analyst touching it. Reports that used to sit in a queue become verdicts.

### USB and removable media control

Every device plugged into a corporate machine is treated as untrusted and inspected before its contents can execute.

### Compromise assessment

Push a YARA rule set from a fresh threat report across the entire estate and get a centrally reported answer on which machines match, in one sweep.

### Insider risk and data loss

Screen watermarking plus endpoint telemetry makes it possible to see, attribute and evidence data leaving through a user rather than through the network.

### APT hunting

Suspicious artefacts collected on the endpoint are sent back to the Malware Analyzer 360, turning a quiet anomaly into a named intrusion mapped to MITRE ATT&CK.

### Isolated and regulated environments

Kiosk and bridge deployments extend real malware analysis into OT, defence and other air-gapped estates that normally run blind.

### How a hunt runs

**01**
**Hypothesise**
Start from a campaign report, a fresh IOC set, or an anomaly the AI flagged.

**02**
**Sweep**
Run YARA rules and IOC checks across every endpoint in one pass.

**03**
**Analyse**
Collected artefacts are detonated and read at code level.

**04**
**Operationalise**
New indicators push out to SIEM, EDR and firewall.

A loop rather than a one-off: what you learn at the end becomes detection content at the start of the next one.

## Deploy the agent on one department.

Roll out to a single team, run a YARA sweep across their machines and see what a central analysis engine finds that a local scanner does not.

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

SPECIFICATION

# Features and capabilities

## ENDPOINT PROTECTION & CONTROL

- USB and removable media control on every insertion
- File share access control and inspection
- Download control in the browser
- Files checked against real-time analysis before they run
- Application and process behaviour monitoring
- Outlook integration for attachments and links
- Browser integration at the point of interaction
- Tamper protection against stopping or removing the agent
- Policy enforced per device, per group or per estate

## ANALYSIS & TRIAGE

- Detection runs centrally in MA 360°, not on the device
- Automatic severity ranking of every detection
- Quiet, long-running activity surfaced rather than buried
- Suspicious artefacts sent to the analyzer for detonation
- Static and dynamic analysis, not a reputation lookup
- Findings mapped automatically to MITRE ATT&CK
- IOC extraction from every analysed artefact
- Behavioural anomaly detection from CyberFortress AI

## THREAT HUNTING

- YARA rule sweeps across every connected endpoint
- Your own rules, a vendor's, or one written this morning
- IOC and artefact search – hashes, domains, registry keys, mutexes, dropped paths
- Historic and current endpoint activity both searched
- Centrally reported matches across the whole estate
- Ranked results, so a sweep with hundreds of hits still leads somewhere
- Hunting reaches isolated segments through kiosk and bridge modes
- New indicators pushed out to SIEM, EDR and firewall

## INSIDER RISK & DATA PROTECTION

- Dynamic screen watermark, tiled across the whole display
- Unique identifier for every user and every session
- Present in a phone photograph as well as a screenshot
- Rendered at low contrast so people can work normally
- Cannot be disabled by the user
- Covers the desktop, not one application
- Attribution of a leaked image back to machine and session
- Works on remote, hybrid and contractor sessions

## AIR-GAPPED & ISOLATED NETWORKS

- Kiosk mode – a scanning station at the secure boundary
- Bridge mode – a controlled transfer point between segments
- Removable media untrusted by default
- Archives unpacked and analysed before release
- CDR rebuilds documents clean where policy requires it
- Full audit trail of every transfer and verdict
- Real analysis in OT, defence and regulated estates

## AGENT & FOOTPRINT

- Lightweight agent, minimal load on the machine
- Heavy analysis offloaded to the platform core
- Automatic collection with no user interaction
- Silent installation and central upgrade
- Continues enforcing policy while disconnected
- Windows 7 and above

## DEPLOYMENT & MANAGEMENT

- On-premise, cloud or hybrid deployment
- Roll out to one department or the whole estate
- Central policy, sweep results and reporting in one console
- Role-based user management
- Role restriction on who may read analysis results
- Health monitor for every engine
- Back up and restore your data
- Seamless product update with a single click

## REPORTING & NOTIFICATIONS

- Customisable logs streamed to your syslog server
- Analysis results emailed in any specified format
- PDF, CSV, JSON and HTML report generation
- Evidence-grade retention for forensic and compliance use
- Full audit trail of submissions and admin actions

## INTEGRATIONS

- RESTful API with bi-directional data and action flow
- SIEM: Splunk, Sentinel, QRadar, Elastic, LogRhythm, ArcSight
- SOAR: Cortex XSOAR, Splunk SOAR, FortiSOAR, Tines, Swimlane, Torq
- EDR/EPP: CrowdStrike Falcon and Microsoft Defender
- Threat intelligence: MISP, OpenCTI, ThreatQ, Anomali ThreatStream
- Syslog streaming for everything else

CyberFortress

# Go looking before the alert fires.

Threat Hunter 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