CyberFortress

PRODUCT DATASHEET

Cloud Hunter

Cloud workloads need cloud-native analysis

Generic security controls stop at the edge of the cloud. Cloud Hunter goes into it – inspecting the container images you ship, the buckets you store data in and the file systems your workloads share, across hybrid and multi-cloud estates.

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

THE PLATFORM

One incident, not two

Hybrid or multi-cloud, the findings land in the same core as every other module – so a malicious file in a storage bucket and the endpoint that uploaded it are one incident, not two. Container runtime behaviour is read in context by CyberFortress AI, suspicious objects are detonated by the Malware Analyzer 360, and everything reaches your SIEM through the same open interfaces the rest of the platform uses.

MA 360° — the platform core

Correlates cloud findings with endpoint and email activity, enriches them with shared threat intelligence and orchestrates the response – so a container anomaly is read against everything else the platform has seen rather than in isolation.

THE FOUR SECURITY MODULES

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.

Malware Analyzer 360

Dynamic sandbox detonation, static code inspection and CDR – where suspicious files found in buckets and shares are detonated rather than judged on reputation alone.

Threat Hunter

A lightweight endpoint agent backed by central analysis. The workstation that uploaded a malicious object is identified in the same motion as the object itself.

Mail Gateway

Multi-layered defence against phishing, BEC, ransomware and mail-borne APTs, sharing every verdict with the rest of the platform.

Data Layer with CyberFortress TI

Container and bucket activity feeds in; live CVE data and threat context come back out, so an image that was clean last month is re-judged against what is published today.

CyberFortress AI

Reads container runtime behaviour in context, which is what separates ordinary drift from an actual compromise.

WHY CLOUD HUNTER

The supply chain is the attack surface

A modern workload is assembled, not written. Base images, package registries, build pipelines and third-party layers all become part of what you run in production – and each is a place an attacker can reach you without ever touching your network.

Most container scanning is tied to one platform: one cloud's registry, one vendor's cluster. That leaves the images built on a developer laptop, stored in a private registry, or running in the environment you acquired last year completely unassessed. Cloud Hunter assesses containers across all of it and reports the findings in one place, so hybrid and multi-cloud estates get a single answer rather than four partial ones.

And it inspects what actually ships. A vulnerable dependency, a secret baked into a layer, or a container that behaves differently at runtime than it did at build time are all findings the platform surfaces before they become an incident.

WHEREVER THE CONTAINER IS

Local & build time
Developer machines and CI runners, before an image is ever pushed.

Registries
Public and private registries scanned on push and on a schedule.

On-premise clusters
Docker and Kubernetes running in your own data centre.

Any public cloud
Managed Kubernetes and container services, hybrid and multi-cloud.

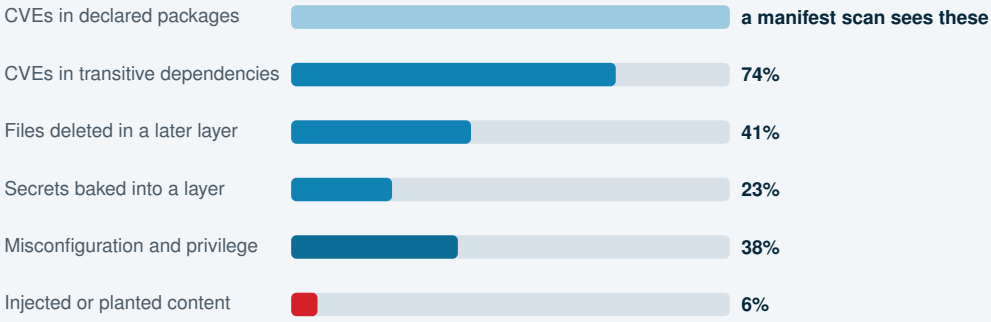
CVE
Container vulnerabilities scanned against live CVE data

Multi
Hybrid and multi-cloud coverage from one console

Real-time
Continuous monitoring of cloud resource activity

K8s
Docker and Kubernetes images, config and runtime behaviour

What a layer-deep assessment finds that a manifest scan does not



Indicative distribution of findings across an internal corpus of production images. A manifest-only scan sees the declared dependency list; everything below it is only visible once the image is unpacked layer by layer.

INSIDE CLOUD HUNTER

Four layers of cloud coverage

Each one addresses a part of the cloud attack surface that traditional tooling tends to leave uninspected.

Container analysis

Images, configurations and runtime behaviour across Docker and Kubernetes are examined in depth. Injected malicious code, misconfigurations, vulnerable dependencies and supply-chain risks are detected automatically, with container vulnerabilities scanned on a CVE basis and critical findings reported the moment they surface.

Bucket scanning

S3, Blob and comparable object stores are scanned continuously for wrong permissions, publicly exposed buckets, malicious content and suspicious file activity – blocking both data-leak paths and malicious uploads early.

File system protection

File movements inside the cloud are analysed in real time. Malicious content, script-based attacks, suspicious executables and anomalous changes are caught immediately – critical defence for shared storage that several workloads read from.

Real-time monitoring

Activity across cloud resources is tracked continuously, raising operational visibility while catching threats before they have an effect to measure.

Six checks on every image

CVE vulnerability scanning

Every package and dependency is matched against current CVE data, with critical findings surfaced the moment they appear rather than at the next scheduled review.

Layer-by-layer inspection

Something deleted in a later layer is still present in the image, and a manifest-only scan will never see it.

Misconfiguration checks

Privileged flags, exposed ports, writable file systems, root users and permissive mounts – the mistakes that turn a contained workload into a foothold.

Malicious content

Injected code, backdoors, cryptominers and weaponised binaries are detonated in the sandbox rather than judged on reputation alone.

Supply-chain risk

Base images, pulled packages and build-time dependencies are assessed as what they are: code from someone else running with your privileges.

Runtime drift

A container behaving differently in production than it did in test is flagged as an anomaly, catching compromise no pre-deployment scan could have predicted.

ACROSS THE LIFECYCLE

Cheapest early, most honest late

Assessment runs at both ends of the pipeline. Gating catches the problem before it ships; registry sweeps and runtime monitoring catch the problem that only became a problem after it shipped.

Where assessment runs in the pipeline

01 Build
Developer machines and CI runners, before an image is pushed.

02 Registry
Public and private registries scanned on push and on a schedule.

03 Gate
A vulnerable or tampered layer fails the pipeline rather than promoting.

04 Deploy
Cluster configuration and admission state are assessed.

05 Runtime
Behaviour is watched after deployment, not only before.

06 Re-assess
Stored images are re-checked as new CVEs are published.

The same engine and the same findings at every stage – so a vulnerability found in production can be traced back to the build that introduced it.

CI/CD image gating

Images are assessed before promotion, so a vulnerable or tampered layer fails the pipeline rather than reaching production.

Registry sweeps

Everything already stored is re-assessed as new CVEs are published – an image that was clean last month may not be today.

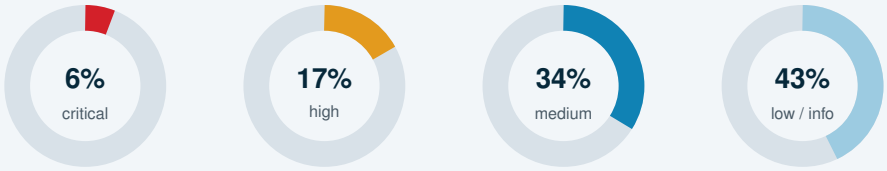
Audit & compliance

Findings, severities and remediation state are reported in a form that satisfies an auditor asking what you run and what is wrong with it.

Incident response

When something goes wrong, the assessment history shows which images carried the flaw and where they were deployed.

Severity of findings on first assessment



Typical first-run distribution across a production namespace. Most of what a first assessment returns is not urgent – the value is in separating the few findings that are.

IN PRACTICE

Where teams put it to work

Common deployments across hybrid and multi-cloud estates – usually starting with a single namespace or storage account.

CI/CD image gating

Images are scanned before promotion, so a vulnerable or tampered layer fails the pipeline rather than reaching production.

Public exposure sweeps

Continuous checks catch a bucket that was made public by mistake – the single most common cause of cloud data leakage.

Shared storage hygiene

Files landing in shared cloud storage are checked for malicious content before another workload or user picks them up.

Runtime drift detection

A container behaving differently in production than it did in test is flagged as an anomaly, not dismissed as noise.

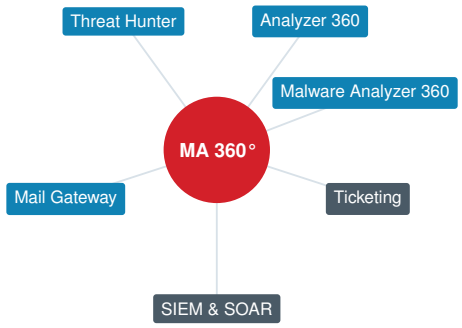
Acquired and inherited estates

The environment you acquired last year is assessed by the same engine as the one you built, so there is one answer rather than two partial ones.

Regulated workloads

Assessment history, severities and remediation state provide the documented evidence trail that a regulator or an auditor asks for.

What happens to a cloud finding



Finding	CVE, exposure or malicious content
Severity	ranked, not a flat list
Correlation	which endpoint or mailbox touched it
Action	pipeline gate, ticket, SIEM event

Scan your first cluster this week.

Point Cloud Hunter at a single namespace or storage account and see what a CVE-based scan and a bucket sweep turn up.

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

SPECIFICATION

Features and capabilities

CONTAINER ANALYSIS

- Docker and Kubernetes images, configuration and runtime behaviour
- CVE-based vulnerability scanning against live CVE data
- Layer-by-layer inspection, not a manifest read
- Content deleted in a later layer still found
- Transitive and build-time dependencies assessed
- Injected malicious code, backdoors and cryptominers detected
- Suspicious binaries detonated in the sandbox
- Secrets and credentials baked into a layer surfaced
- Critical findings reported the moment they appear

CONFIGURATION & POSTURE

- Privileged flags and root user detection
- Exposed ports and permissive network policy
- Writable file systems and permissive mounts
- Cluster and admission configuration assessed
- Misconfiguration ranked by exploitability, not just presence
- Remediation state tracked across re-assessments

BUCKET & OBJECT STORAGE

- S3, Azure Blob and comparable object stores
- Continuous scanning for wrong permissions
- Publicly exposed bucket detection
- Malicious content in stored objects
- Suspicious file activity and access patterns
- Malicious uploads blocked before downstream workloads read them
- Objects scanned on arrival, not only on a schedule

FILE SYSTEM PROTECTION

- Real-time analysis of file movements inside the cloud
- Malicious content and script-based attacks caught immediately
- Suspicious executables identified before execution
- Anomalous change detection on shared storage
- CDR rebuilds documents clean where policy requires it

RUNTIME & MONITORING

- Continuous monitoring of cloud resource activity
- Runtime behaviour compared against build-time expectation
- Drift flagged as an anomaly rather than dismissed as noise
- Behavioural context supplied by CyberFortress AI
- Threats caught before they have an effect to measure

COVERAGE

- Developer machines and CI runners at build time
- Public and private registries, on push and on schedule
- On-premise Docker and Kubernetes clusters
- Managed Kubernetes and container services in any public cloud
- Hybrid and multi-cloud estates from one console
- Acquired and inherited environments assessed by the same engine

PIPELINE & LIFECYCLE

- CI/CD gating – a bad layer fails the pipeline
- Registry re-assessment as new CVEs are published
- Deployment-time configuration assessment
- Post-deployment runtime watching
- Assessment history for incident response and audit

REPORTING & ADMINISTRATION

- Findings, severities and remediation state in one report
- PDF, CSV, JSON and HTML report generation
- Customisable logs streamed to your syslog server
- Role-based user management and access restriction
- Health monitor for every engine
- Full audit trail of assessments 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
- Cloud storage: Amazon S3, Azure Blob, Google Drive, Box, Dropbox
- Threat intelligence: MISP, OpenCTI, ThreatQ, Anomali ThreatStream
- Ticketing systems open, update and close findings automatically
- Syslog streaming for everything else

CyberFortress

Know what is actually in your images.

Cloud 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