CyFIR™

SPEC SHEET

CyFIR Enterprise

Forensics & Incident Response

Key Benefits

- ✓ Discover and react to cyber risks that may have gotten through other layers of defense.
- ✓ Dramatically reduce the cost of any active or potential breach through our speed to resolution using our instant access to remote endpoints instead of traditional and costly "boots on the ground" incident response methods.
- ✓ Remotely bring both the necessary tools and talent to address any ongoing cyber challenges.
- ✓ Address the ever changing landscape of potential cyber risk issues, such as malware infection, eDiscovery collection, IP protection, incident investigations / data spills, mergers and acquisitions, remote asset investigation, threat hunting, and internal investigations.

Become Cyber Resilient.

In today's threat environment, cybersecurity isn't just about knowing when a data breach occurs. To be cyber resilient, organizations need a combination of tools, methodologies, and hands-on personnel to discover, react, and minimize the potential impact of any digital security threat. CyFIR Enterprise goes beyond breach protection and enables real-time investigation, analysis, and resolution of active or potential threats no matter the origin. No other solution provider matches CyFIR's depth of endpoint visibility and **speed to resolution.**

CyFIR Enterprise provides Information Security (IT) teams with unparalleled performance in incident response, threat hunting, digital forensic investigation, insider threat analysis and malware detection. CyFIR enables cybersecurity personnel to quickly perform remote triage and forensic analysis, evidence capture, and incident remediation across networked servers and endpoint workstations, empowering forensic investigators to *See More, Know More, and Respond Instantly* to a wide range of digital security needs.

See More. Know More. Respond Instantly.

With CyFIR Enterprise, IT teams can evaluate running processes on every endpoint in near-real-time without impact to business or network operations. This unparalleled depth of endpoint visibility provides comprehensive investigation of data breach intrusions, zero-day exploits, and insider threats, providing a critical last line of defense for your network operations.

See More

- → Search globally across your enterprise concurrently
- → Perform remote, in-depth forensic investigations without leaving your office
- → Perform live investigations in real time
- → An optional agent stealth mode makes CyFIR's investigative activity difficult to detect on the endpoint

Know More

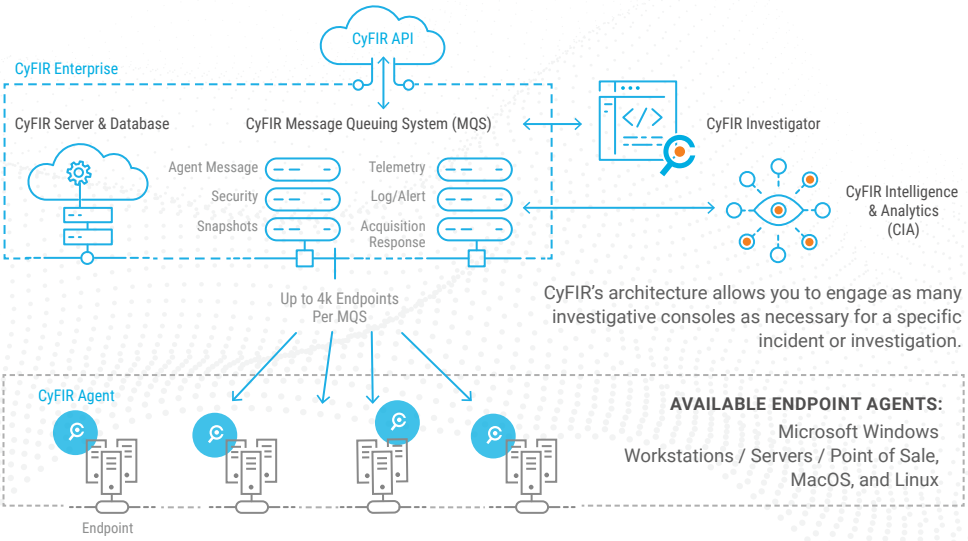
- → Provides intelligence into system and network level activities through network and process telemetry
- → View data about processes and their associated files, modules, registry settings, network connections and child processes running in RAM in real time
- → View, analyze, recover, and acquire (if necessary) files and directories on disk
- → Find malware or other indicators of malicious activity your other security tools and antivirus/EDR solutions might have missed

Respond Instantly

- → Full remote imaging of hard drives (physical or logical), files, memory, or processes
- → Collect screen shots of active user desktops and running process snapshots of remote systems
- → Search across any number of endpoints for critical indicators of compromise
- → Gain privileged command line access to any endpoint
- → Selectively kill processes on an endpoint to stop active events
- → Remotely mount an endpoint's media as a local drive to enable the use of additional forensic or operational tools

CyFIR™ Enterprise

Unlike solutions that limit your analysts to searching a small number of connections, CyFIR allows enterprises to search across the entire network of connected services and workstations concurrently.



Investigator

Forensic Analysis and Remote Remediation

CyFIR Enterprise Investigator is the core platform for both controlling the functionality of CyFIR and for performing forensic investigation and remediation that allows analysts to search and analyze large numbers of endpoints in complex networks, without geographic limitations.

Core Platform

- Authentication service
- Agent connection terminations
- Licensing enforcement
- Investigation/data management

Agents

- Data collection (applications, screen shots, network interface, file system, running processes, etc)
- Artifact retrieval
- Telemetry reporting
- File Search

Concurrent Endpoint Access

- Launch searches to concurrent endpoints
- Up to 4k endpoints per server
- Begin analyzing results almost immediately

Remote Forensic Analysis

- Connect remotely from anywhere to conduct or initiate an investigation
- System snapshots

CIA

Intelligence and Analytics

CyFIR Intelligence and Analytics (CIA) extends the functionality of CyFIR Investigator by providing analysts with additional tools for evaluating data telemetry and responding to security incidents.

Intelligence

- Threat Posture
  - Analytics
  - Intelligence
  - Aggregation

Sandbox

- Suspicious File Detonation
  - Analysis of unknown or suspicious files in an isolated environment
- Threat Report Generation

Visual Dashboard

- Posture of your endpoints
- Threat level assessment
- Threat Hunting Analytics
- Telemetry

Process Disposition

- Process enumeration
  - Good
  - Bad
  - Unknown

*"After we added CyFIR to our security stack, we were able to capture and analyze about **80% more data** on our endpoints' health and activities than we could using 'our anti-virus solution' alone."*

- Major Financial Services Institution, CISO

*"Once we demonstrated the capabilities of CyFIR™, our legal department stopped requesting traditional full disk captures. Today, they just ask us to **'CyFIR it.'** By eliminating technical and logistical hurdles, CyFIR has been a tremendous help in expediting our cases through increased productivity."*

- Global Cloud Provider, Director

CyFIR Solutions

CyFIR Enterprise
Forensics & Incident Response

CyFIR Fast Forensics™
Digital Investigations

CyFIR Instant Response™
CyFIR Enterprise as a Service

Get In Touch

For more information or to request a quote, visit us online

CyFIR.com