CyFIR ENTERPRISE IS A FORCE MULTIPLIER THAT SIGNIFICANTLY REDUCES THE COST OF A BREACH.

CyFIR Enterprise is a revolutionary platform for Incident Response, Internal Investigation, eDiscovery, Threat Assessment, and Threat Hunting. By stopping advanced threats from compromising your networks and stealing or taking hostage valuable data, CyFIR protects enterprises from millions of dollars in potential losses.

A MOTIVATED ATTACKER WILL FIND A WAY INTO YOUR NETWORK.

THREAT ACTORS ARE CONSTANTLY EVOLVING AND DEVELOPING NEW METHODS TO THWART NETWORK DEFENSES. TRADITIONAL FORENSIC SOLUTIONS CAN TAKE MONTHS TO DETECT THESE THREATS, COSTING ENTERPRISES MILLIONS OF DOLLARS.

Yahoo experienced the largest breach of the 21st century, between 2013-2014, impacting 3 billion user accounts. The breach was likely ensued by "a state-sponsored actor," and compromised names, email addresses, dates of birth, and telephone numbers had been hashed using the robust bcrypt algorithm. There are three key reasons current processes and controls don't address, detect, respond, analyze, isolate, and remediate malware compromises:

1. ADVANCED PERSISTENT THREATS

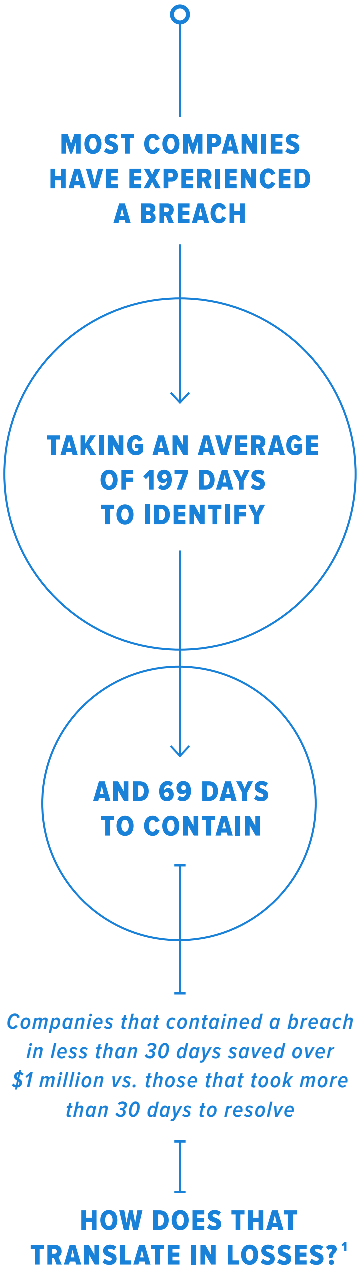
Enterprises lack the ability to identify 100% of the processes that are being executed on their endpoints and internal to their networks. This lack of visibility allows advanced persistent threats (APT) and zero-day malware to get a foothold in the process execution space on the endpoints and can remain undetected for extended periods of time.

2. NETWORK VISIBILITY

Enterprises typically don't have the ability to monitor, query, and receive information in near real-time across their networks. This limits the ability to detect anomalies and act quickly to eradicate the threat.

3. ADAPTIVE SECURITY ARCHITECTURE

Enterprises are not using an adaptive security architecture to protect against advanced threats. This architecture requires continuous monitoring, analytics, and automation between security systems to reduce the time between threat discovery and threat containment.



MOST COMPANIES HAVE EXPERIENCED A BREACH

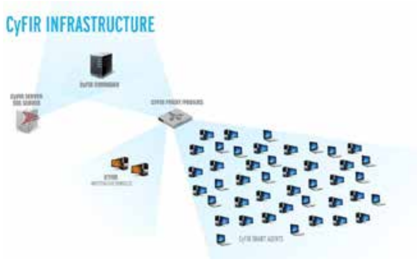
TAKING AN AVERAGE OF 197 DAYS TO IDENTIFY

AND 69 DAYS TO CONTAIN

Companies that contained a breach in less than 30 days saved over $1 million vs. those that took more than 30 days to resolve

HOW DOES THAT TRANSLATE IN LOSSES?[1]

[1] *"2018 Cost of a Data Breach Study" the Ponemon Institute.*



STRENGTHEN YOUR SECURITY STACK WITH A FORCE MULTIPLIER

"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***

KEY BENEFITS

✓ Unmatched speed to resolution

✓ Rapid assessment of all processes leveraging the CyFIR Intelligence Network (CIN)

✓ Immediate enterprise-wide forensic visibility to data in memory and on disc across all endpoints without reliance on indexing

✓ Depth of endpoint visibility strengthens the security posture of the entire enterprise

Parallel Processing saves time, money, and resources.

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.

AVAILABLE ENDPOINT AGENTS:

✓ Microsoft Windows Workstations and Servers

✓ Microsoft Windows Point of Sale

✓ macOS

✓ Linux

Platform

Designed by experienced computer forensic practitioners serving the Federal Government (Special Forces, FBI, DEA, CIA), and Fortune 500 companies, the CyFIR Enterprise platform can forensically analyze workstations and servers, including Point of Sale terminals, concurrently – a first in the enterprise forensics industry. Within the CyFIR platform, analysts can review:

✓ Remote file systems, including attached removable media

✓ Running processes and services in RAM

✓ Exchange and multiple legacy electronic mail systems – without bringing down the server and stopping work

✓ Screen shots, network captures, and more

Services

There are not enough digital forensic specialists to match the increase in demand we've experienced over the last decade. CyFIR's team can help identify and contain breaches with our state of the art platform to minimize your financial loss.

INCIDENT RESPONSE

Live, immediate forensic analysis and incident response on both files on disk and processes running in memory dramatically shortens your company's exposure during an incident.

INTERNAL INVESTIGATION

Instantly reach across geographies to rapidly conduct investigations into employee misconduct, company policy violations, harassment, employee pilfering of customer lists, the exfiltration of intellectual property, and other HR-centric infractions.

E-DISCOVERY

Continuously monitor network activity of your most valuable files. Access to these files will be logged, providing a comprehensive accounting of every person whom opened, copied, or moved a document.

THREAT ASSESSMENT

Provide insight into clients' endpoints in near real-time without causing an impact to your business or network operations to identify data breach activities, zero-day exploits, insider threat, and unapproved software installations in minutes or hours vs months or years.

THREAT HUNTING

A proactive, "eyes-on" approach to analyzing selected endpoints in an environment by experienced analysts. This isn't scripted analysis; it is a thorough, human review, profiling content on selected systems.

Speed to Resolution

Malicious code in an organization's network often goes undiscovered for months or even years. Recent studies have shown the security breaches are discovered, on average, 169 days after the event, and notification usually arrives as the result of a third party. CyFIR dramatically shortens breach impact through its ability to rapidly identify, isolate, remediate, and remove threats from a network by applying a force multiplier to your existing security stack, and quickens speed to resolution through:

✓ Centralized Searching for Worldwide Response

✓ Total Dynamic Visibility

✓ Live Database Search

✓ Full Forensic Fidelity