Infocyte

DATA SHEET

Infocyte HUNT

THREAT HUNTING. SIMPLIFIED.

Be proactive — deny attackers the ability to persist undetected.

ASSET DISCOVERY + THREAT HUNTING + VULNERABILITIES + INCIDENT RESPONSE

"CYBER THREATS OFTEN RESIDE INSIDE ORGANIZATIONS FOR MONTHS, SOMETIMES YEARS, BEFORE BEING DISCOVERED."

of threats go undetected by automated security tools[1]

average attacker dwell time

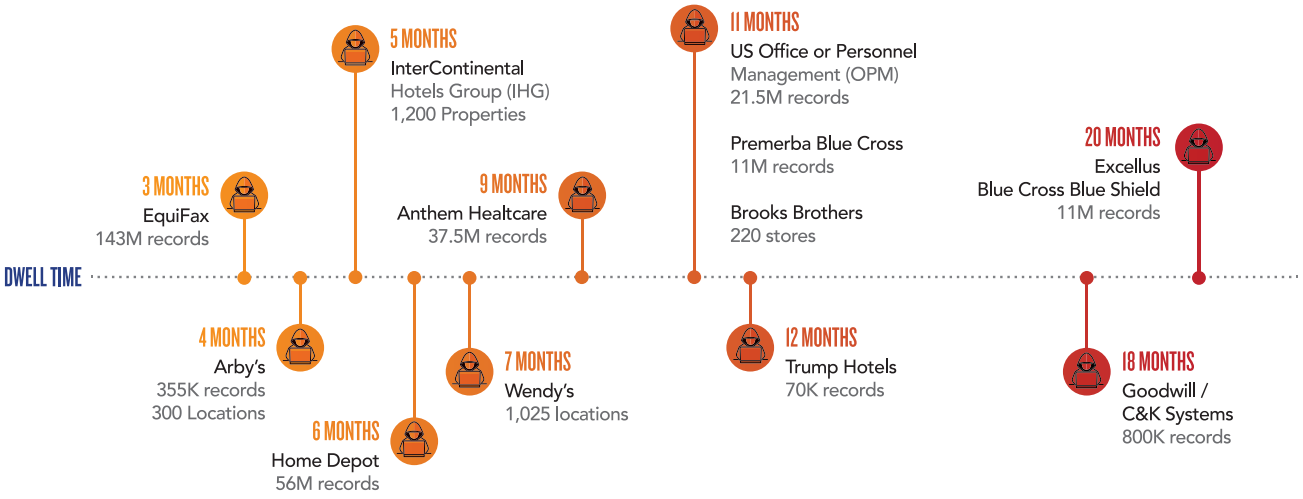
of SOCs say detecting hidden and unknown threats is their top challenge[1]

According to industry research, the average security breach goes undetected for several months before being discovered. In over two-thirds of known cases, breaches are discovered by a third party such as law enforcement or investigative journalists. This delay between breach and detection is known as "dwell time" and it plays a primary role in the cost and impact of a security breach.

Managing cyber risk in the modern age requires more than instituting static controls and assessing vulnerabilities. Organizations must be proactive in the search for threats within their networks – this process is called Threat Hunting.

THE FASTER YOU HUNT AND CONTAIN BREACHES, THE SMALLER THE FINANCIAL IMPACT.

With dwell time averaging 6+ months, research shows organizations that are able to contain a breach in less than 30 days paid nearly $1 million less in total breach costs.[2]



Infocyte HUNT™ enables organizations to seamlessly integrate advanced threat hunting into their cyber risk management process in order to reduce dwell time and mitigate damage that can be caused from prolonged unauthorized access.

AGENTLESS, AUTOMATED, CLOUD-ENABLED THREAT HUNTING.

BE PROACTIVE, NOT REACTIVE.

Infocyte HUNT provides an easy-to-use, powerful solution to limit risk and reduce dwell time by enabling your security team to proactively discover not just vulnerabilities, but stealthy malware and persistent threats that may have successfully bypassed existing defenses.

Infocyte's threat hunting platform is designed to rapidly assess endpoints, including user workstations and servers, using Forensic State Analysis (FSA). Unlike other endpoint protection tools (i.e. Antivirus or EDR) Infocyte is agentless, which means you can easily augment your endpoint protection strategy without the burden of complicated equipment or permanent endpoint software installations.

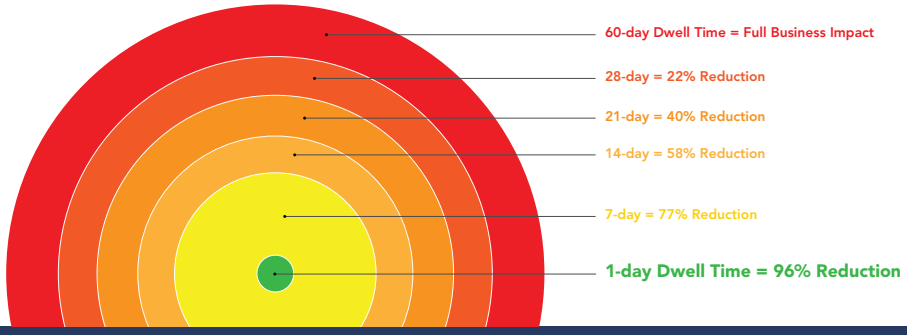
Infocyte enables proactive discovery and analysis of threats, including:

- Active or dormant malware (file-based & file-less)
- Historical attacks or credential misuse via forensic artifacts and indications of compromise
- Unauthorized, risky, or vulnerable applications

Infocyte empowers you to confidently answer the critical questions:

Am I hacked? If not, what can be hacked?

CONTROLLING DWELL TIME PROTECTS YOUR BUSINESS.



WHAT SETS INFOCYTE HUNT APART

Infocyte HUNT is unlike any endpoint detection tool on the market. It utilizes an advanced threat hunting technique called Forensic State Analysis to determine the actual state of your systems. This enables you to identify the presence of unauthorized users or software that may be difficult to categorize by monitoring/logging solutions.

This is made possible by the sheer depth of analysis which includes an advanced survey of a host's volatile memory, application persisence mechanisms, forensic artifacts and a thorough verification of operating system (OS) integrity.

Infocyte HUNT takes the art of memory forensics to a new level of scalability – by surveying the live memory of thousands of endpoints, simultaneously.

SIMPLIFY THE HUNT FOR CYBER THREATS WITH INFOCYTE

THREAT HUNTING

Infocyte HUNT provides a platform to seek out persistent threats that may be residing on endpoints within your network. Infocyte automates and simplifies the threat hunting process so you can reduce dwell time, respond faster, and limit business impact.

THREAT ASSESSEMENTS

The only hunt solution built to measures the full scope of risk on your endpoints. Includes asset discovery, vulnerabilities, as well as the presence of any threats that have exploited those vulnerabilities.

INCIDENT RESPONSE

Infocyte HUNT provides endpoint forensic data that can be used to vet alerts captured by your SIEM, reduce the time and resources needed to respond, and determine the true state of a system.

Infocyte

Threat Hunting as a Service.

NEW: Infocyte HUNT Command

Augment your cybersecurity team with our expert threat hunters and on-demand access to threat & malware analysts + tailored monthly threat intel reports.

THE INFOCYTE HUNT ADVANTAGE

FORENSIC DEPTH

- Detects post-compromise indicators that antivirus and event monitoring tools (EDR) are prone to miss
- Unique, scalable volatile memory analysis finds all fileless implants
- Autostart and Forensic Artifact analysis finds all threats laying dormant

BECOME THE HUNTER

- Automates & integrates the threat hunting process into your risk and vulnerability management process
- Continuously hunt or perform periodic assessements to mitigate risk
- Go beyond vulnerabilities and identify any threats that may have exploited them

EASY TO IMPLEMENT

- Agentless and lightweight
- Survey thousands of endpoints simultaneously vs. 'single-host' forensic tool alternatives.
- Download and deploy HUNT within a day

FAST ROI

- "Zero to Hero" in hours to days — not months or years
- Reduces dwell time to limit breach damage and costs
- Ensures you are prepared for the next one

Infocyte

ABOUT INFOCYTE

Developed by former US Air Force cybersecurity officers, Infocyte's dedicated forensics-based threat hunting platform discovers the post-compromise activity of cyber attackers and malware that have bypassed other defenses. The company's unique approach to security reduces attacker dwell time to help organizations and independent assessors defend networks and critical information.

CORPORATE HEADQUARTERS

3801 N Capital of Texas Hwy, Suite D-120
Austin, Texas 78746

+1 (844) 463-6298 / sales@infocyte.com

www.infocyte.com

1 2017 Threat Hunting Report, Crowd Research Partners
2: Ponemon Institute 2017 Cost of Data Breach Study: Global Overview

TRY INFOCYTE HUNT FOR FREE!

Discover why Infocyte HUNT has been recognized as a Top Threat Hunting Solution by industry leaders.

https://try.infocyte.com

SC 2017 awards finalist

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

CYBERSECURITY BREAKTHROUGH AWARD 2017