Infocyte + ForeScout

SOLUTION OVERVIEW

Automated Threat Response

Powered by ForeScout CounterACT®

Automatically prevent compromised devices from entering your network.

AUTOMATED, INTELLIGENT THREAT DETECTION & ISOLATION

Infocyte + ForeScout® =

AUTOMATIC Threat Prevention

OVERVIEW

Infocyte HUNT provides an easy-to-use, yet 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 and established a beachhead in your network.

When combined with agentless visibility, control, and orchestration provided by ForeScout CounterACT®, Infocyte HUNT equips enterprises with the ability to automatically discover devices upon connection, continually assess while connected, forensically evaluate their state, and enforce endpoint and network compliance policies that prevent malware, compromised systems or malicious/unauthorized accounts from infiltrating your network.

Infocyte's threat hunting platform — Infocyte HUNT — is designed to rapidly assess endpoints, including user workstations and servers, using Forensic State Analysis (FSA). Unlike other endpoint protection tools that require a management agent to be installed on the endpoint, both Infocyte and ForeScout are agentless, which means you can easily augment your endpoint protection strategy without the burden of complicated equipment or managing numerous endpoint software installations.

Infocyte HUNT enables automated and proactive discovery and analysis of cybersecurity threats including:

- ✓ Active or dormant malware (file-based & file-less)
- ✓ Historical attacks or credential misuse via forensic artifacts & IOC
- ✓ Unauthorized, risky, or vulnerable applications

USE CASES

1. Connect to Comply & Comply to Connect
2. Network access control to not allow any device/ endpoint onto the network unless it passes an Infocyte scan — is clear of threats and compliant per corporate policy.
3. Immediate threat isolation and remediation of compromised, non-compliant endpoints to prevent threat infiltration.

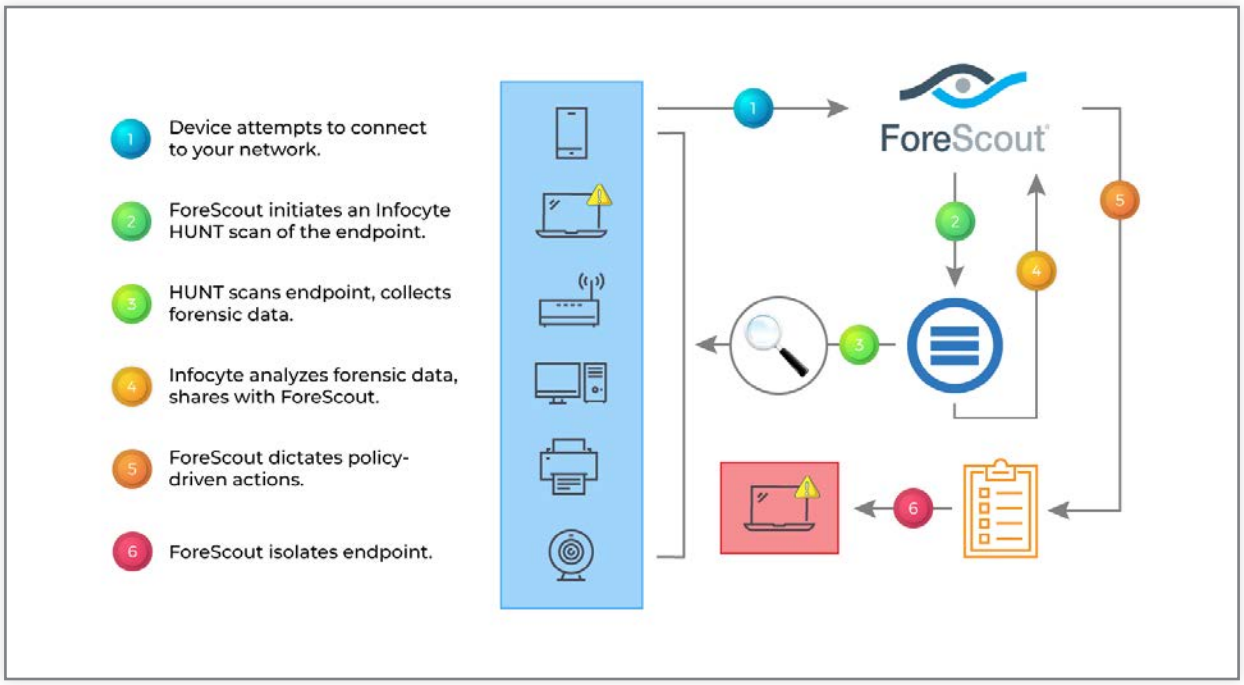
HOW IT WORKS

ForeScout CounterACT discovers, classifies, and assesses endpoints as soon they enter the network and continually while connected – including devices with local privileged accounts not yet in Active Directory.

If the endpoint has not been recently inspected, ForeScout will initiate a forensic threat hunt with Infocyte HUNT to determine if endpoints are compromised with any hidden, dormant, or active threats.

ForeScout immediately responds to threats by taking policy-driven actions to isolate any compromised endpoints from the network and drive other needed network or system actions to help remediate the threat.

1. ForeScout discovers endpoint and notices that endpoint is out of compliance without recent scan
2. ForeScout initiates an Infocyte scan
3. Infocyte HUNT inspects the endpoint and collects forensic data
4. Infocyte HUNT then analyzes the forensic data for signs of a compromise
5. HUNT sends inspection results to ForeScout which dictates policy-driven actions by ForeScout
6. ForeScout takes network and system actions to isolate the endpoint



REQUIREMENTS

ForeScout:
- ForeScout CounterACT
- ForeScout Open Integration Module (OIM) platform

Infocyte:
- Infocyte HUNT server instance
- Python 3.6 or higher (pip or virtual env)

"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

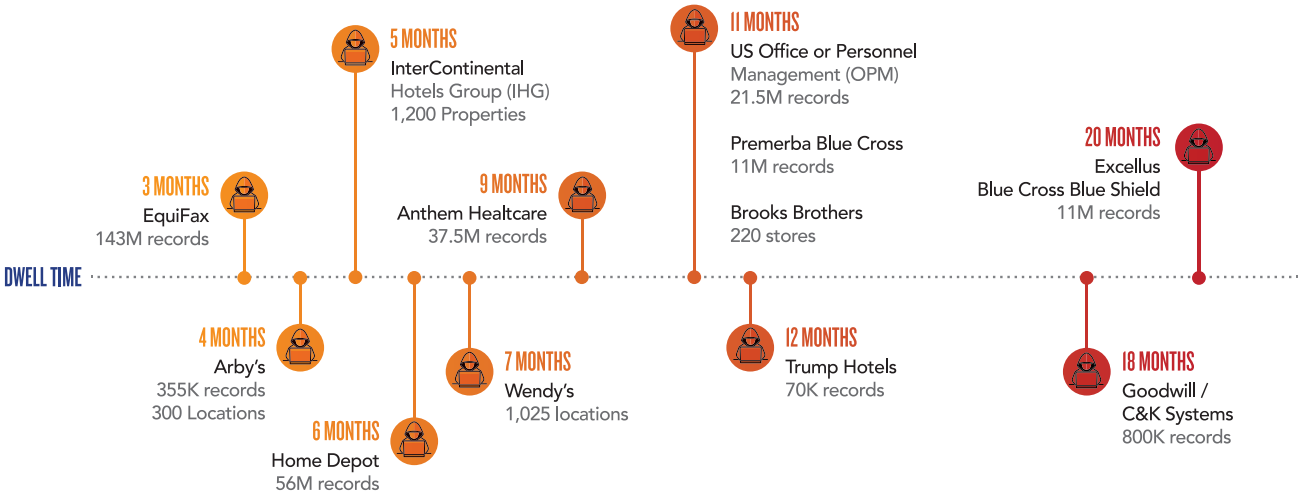
of SOCs say detecting hidden and unknown threats is their top challenge[1]

According to industry reports, the average security breach goes undetected for several months before being discovered. In over two-thirds of cases, breaches are discovered by a third party such as law enforcement or investigative journalists. This delay and whether the breach was found internally or externally, both play critical roles in the cost and business impact of a security breach.

Managing cyber risk in the modern age requires more than static controls and anti-virus. Organizations must be proactive in the search for threats (i.e. malware and unauthorized access) 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, organizations able to contain a breach in less than 30 days paid nearly $1 million less in total breach costs.[2]



Automated Threat Response, powered by ForeScout CounterACT, enables organizations to automatically inspect endpoints as they connect to your network. In the event a threat is found, HUNT and ForeScout can identify and isolate the compromised device.

Threat Hunting as a Service.

Managed Threat Hunting

Augment your security team with access to expert threat hunters, malware analysts, and tailored monthly threat intelligence reports.

ADVANTAGES

DIG DEEPER

- Focuses on the post-attack indicators that protection and monitoring tools are prone to miss
- Hunt within memory for active and fileless threats
- Hunt for persistence and analyze forensic artifacts to find historical or dormant threats

BECOME THE HUNTER

- Automates & simplifies the threat hunting process
- Continuously hunt or perform periodic assessements according to your risk profile
- Mature your security posture by hunting and mitigating threats

EASY TO IMPLEMENT

- Deployment Options: Agentless or Agent-based
- Zero business disruption and no change management (for agentless model)
- Download, install, and hunt within an hour

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

Infocyte HUNT is a forensics-based threat hunting platform, developed by former US Air Force cybersecurity officers. HUNT is designed to continuously inspect your endpoints threats (breaches, malware, ransomware, and more) that have bypassed other defenses. Our unique approach to security eliminates attacker dwell time — enabling you to protect your organization's critical information and assets.

ForeScout®

ABOUT FORESCOUT

ForeScout pioneered an agentless approach to network security to address the explosive growth of the Internet of Things (IoT), cloud computing and operational technologies (OT). ForeScout provides Global 2000 enterprises and government agencies with agentless visibility and control of today's vast array of physical and virtual devices the instant they connect to the network — continuously assessing, remediating and monitoring devices to help accelerate incident response, break down silos, automate workflows and optimize existing investments.

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.

infocyte.com

SC 2017 awards finalist

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

CYBERSECURITY BREAKTHROUGH AWARD 2017