FEATURE OVERVIEW

Compromise Assessments

Determine if your network is breached with Infocyte HUNT

ARE YOU CURRENTLY BREACHED?

Malware and persistent threats are often resident inside an organization for months, sometimes years, before being detected.

HUNT is the most effective solution for conducting in-house Compromise Assessments objectively, rapidly, and cost-effectively.

- Identify all endpoints on your network and scan them to discover the presence of active or dormant malware or suspicious code.
- Detailed reports provide collected intelligence to allow your team to take action with swift remediation and incident response.
- Compromise Assessments can be completed 10x faster than assessments performed manually using traditional security monitoring and incident response solutions.
- Run as frequently as needed: monthly, quarterly, or annually.

ASSESSING THE STATUS OF YOUR NETWORK

Malware poses a singular and growing risk to enterprises globally. From impacts on efficiencies to legal implications and civil and statutory damages, cyber security is a critical business function.

The first step to any cyber security strategy involves knowing your current security posture and state. Attackers are often resident inside a network for months, sometimes years, before being detected using malware to infect endpoints. As evidenced by the growing number of breaches, existing technologies are no longer enough to stop all threats from penetrating the perimeter. While vulnerability assessments and penetration tests look for security gaps and vulnerabilities, the do not detect existing compromises. Today's enterprises need to add compromise assessments to their security practices to proactively verify whether a network has been breached and mitigate risk.

A Compromise Assessment run using Infocyte HUNT determines whether a network is breached using proprietary scans to proactively discover the presence of know and zero day malware and persistent threats – active or dormant – that make have successfully evaded an organization's existing security defenses. Infocyte HUNT delivers detailed scan results and provides an easy to understand executive report documenting the results.

Compromise Assessments conducted with Infocyte HUNT are more comprehensive and cost-effective than alternative approaches – and complete within days.

THE INFOCYTE COMPROMISE ASSESSMENT

Compromise Assessments with Infocyte HUNT aim to identify every endpoint, work station and server on the network and look for signs of compromise. Our methodology combines agent-less scans with our File Intelligence Services and our Digital Forensics Analytics Services into statistical models that determine the risk profile of endpoints.

Infocyte HUNT scans validate everything currently running or scheduled to run on endpoints, and analyzes each system's volatile memory to discover signs of manipulation or hidden processes using patent-pending techniques. For speed and efficiency, the scans are agentless and do not require software to be pre-installed, typically taking just minutes to complete. Infocyte scans are completely independent of the network's existing security infrastructure and do not rely on a potentially compromised host opening system to deliver results.

By leveraging the automation built into Infocyte HUNT, Compromise Assessments can be completed 10 times faster than assessments performed manually using traditional security monitoring and incident response solutions.

USE CASES

RISK MANAGEMENT & REGULATORY COMPLIANCE

Current regulatory requirements and data breach disclosure laws are creating a hostile environment for enterprises. Compounding the risk are civil actions that claim enterprises should be liable for not detecting malware that persist for long periods of time. Compromise Assessments indicate organizational due diligence and provide proof that an enterprise is malware free at a given point in time.

MERGERS & ACQUISITIONS

Prior to an M&A transaction, the compromise assessment serves as a pre-existing conditions check to ensure the buyer is not accepting the risk associated costs of an existing compromise. When feasible, the assessment should be conducted during due diligence.

THIRD-PARTY & VENDOR RISK MANAGEMENT

Organizations take on a significant risk when cringing on vendors and partners where sensitive data, intellectual property, or customer data is shared. In many cases, a current compromise assessment report should be requested to ensure the integrity of the vendor's information networks.

SECURITY PROGRAM AUDIT

The compromise assessment serves to validate the effectiveness of current security controls and catch threats that may have breached existing defenses, and provides insight into which defenses are functioning effectively and which are outdated or obsolete.

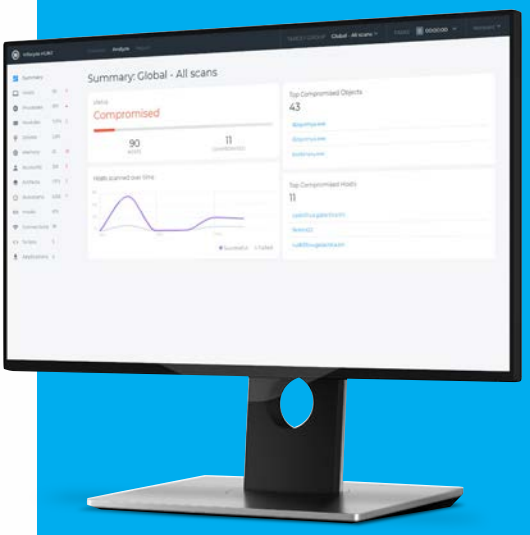
BENEFITS

- Definitively answers if you have been breached.
- Final report provides collected intelligence and drill down into identified issues to allow your team to take action with swift remediation and incident response.
- Speed of assessment — provides active intelligence within hours followed by a full review and report in 3 days on average.
- Effective in identifying signs of hidden backdoors and Remote Access Tools — simply put, malware that gives an attacker remote access or control.
- Advanced detection combines forensic automation and patent-pending memory analysis techniques tailored to detect malware and compromised systems.
- Agentless scans gather system information and scan volatile memory with no pre-installation of software for seamless deployment and minimal impact on your systems.
- Infocyte HUNT does not rely on the operating system or existing security tools, so results are untainted by any existing compromise.

CONCLUSION

A Compromise Assessment with Infocyte HUNT offers organizations a fast and cost-effective solution to validate the health of your endpoints and combat existing threats, ensuring the security of your networks.

Call **(844) 463-6298** or email **sales@infocyte.com** to learn more.



"The HUNT Compromise Assessment was essentially seamless and non-invasive; and we were very pleased with the speed of the entire process."

- Keith Messner
CTO, PierceTransit

Infocyte

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

(844) 463-6298
sales@infocyte.com
www.infocyte.com

© 2018 Infocyte Inc.

All Rights Reserved. Infocyte and Infocyte HUNT are trademarks of Infocyte Inc. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.

TRY HUNT FOR FREE »

Discover why Infocyte HUNT has been recognized as a top threat hunting solution by industry leaders.

www.infocyte.com