

# THREAT ASSESSMENTS

## VALIDATE YOUR SECURITY CONTROLS & UNDERSTAND YOUR RISK

Sophisticated cyber attacks, like file-less malware and ransomware can dwell for months, sometimes years, before it is detected. Infocyte combines live and historical memory forensics, continuous monitoring, and extensible response capabilities to enable fast and conclusive Threat Assessments.

## THREAT ASSESSMENTS WITH INFOCYTE

Threat Assessments with Infocyte are conclusive, cost-effective, and fast — often completed within days without additional hardware or expensive consulting contracts.

- Configure and deploy Infocyte within minutes via one of several agent-less options.
- Enumerate workstations, systems, and servers (physical or virtual) on your network.
- Inspect host memory across your endpoints, pulling live and historical forensics data.

Infocyte enriches primary forensics data with multiple sources of threat intelligence to prioritize threats, risks, and vulnerabilities resident in your environment.

Infocyte runs independent of your existing endpoint security infrastructure, avoiding potentially compromised detection rules. By leveraging built-in automations, Infocyte Threat Assessments can be completed much faster than Assessments performed manually using traditional security monitoring and incident response solutions.

## BENEFITS

- ▶ **FAST:** Complete a full Infocyte Threat Assessment within days.
- ▶ **CONCLUSIVE:** Detect APTs, file-less malware, ransomware, and more.
- ▶ **AGENTLESS:** Deploy and scan hosts without impacting network productivity.
- ▶ **DETAILED:** Post-assessment reports help you prioritize triage and IR.
- ▶ **REPEATABLE:** Leave Infocyte installed to easily run regular Threat Assessments

## THE IMPORTANCE OF REGULAR THREAT ASSESSMENTS

The first step to any cyber security strategy involves knowing your current security posture. Malicious actors are often resident inside a network for months, sometimes years, before being detected. Prevention technologies are no longer enough to stop threats. While vulnerability assessments and penetration tests look for security gaps and vulnerabilities, they do not detect existing cyber risks and vulnerabilities.

Performing regular Threat Assessments proactively verifies whether a network has been breached and helps mitigate overall cyber risk. Infocyte Threat Assessments determine whether a network is breached and detects the presence of ransomware, file-less malware, advanced persistent threats — active or dormant — and other threats that have evaded your cybersecurity defenses. A detailed report of scan results and providing an easy to understand executive report documenting is a critical piece of the Threat Assessment process to ensure the results are actionable.

## THREAT ASSESSMENT 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. Threat 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 Threat 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, an Assessment should be conducted during due diligence.

### THIRD-PARTY & VENDOR RISK MANAGEMENT

Organizations take on a significant risk when vendors and partners have shared access to sensitive data, intellectual property, or customer info. In many cases, a recent Threat Assessment report should be requested to ensure the integrity of your vendor and partner networks.

### SECURITY PROGRAM AUDIT

The Threat 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.

**PHONE: 844.463.6298**

**EMAIL: [sales@infocyte.com](mailto:sales@infocyte.com)**

## ABOUT INFOCYTE

---

Founded by the leaders of the United States Air Force Cyber Incident Response Team (AFCIRT), Infocyte is the globally trusted leader in proactive threat detection and incident response. The world's leading security and incident response companies use Infocyte's platform to proactively detect and respond to vulnerabilities and threats within their customers' endpoints, data centers, and cloud environments. Infocyte's team and partner ecosystem help organizations maintain compliance, stop ransomware and account takeover, reduce risk, optimize security operations, and scale security teams. Infocyte is the faster, simpler, smarter way to detect and orchestrate response to sophisticated threats. Learn more at [infocyte.com](https://infocyte.com) or follow us on Twitter: @InfocyteInc.