

### The Challenge

When there is a data breach, incident responders are required to answer questions relating to **who, what, when, where, how, and why**. Without a commercial-grade platform, investigating hundreds or thousands of systems simultaneously becomes an uphill battle. There is the continuous need to conduct investigation at scale, regardless of the geolocation of the evidence (on-prem or cloud) while avoiding business interruption.

ThreatRESPONDER | NEUTRALIZING ADVANCED CYBER THREATS

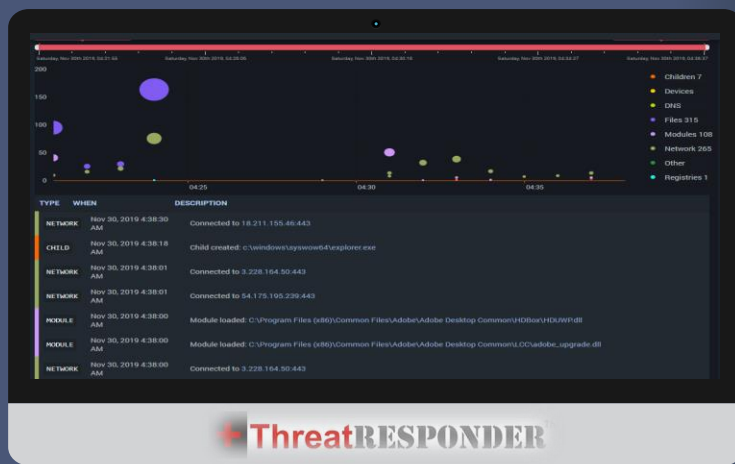


### The Solution – ThreatResponder® Platform

ThreatResponder® Platform is an all-in-one cloud-native endpoint threat **detection, prevention, response, analytics, intelligence, investigation, and hunting** product. Once lightweight agents (“Rovers”) are deployed, you gain situational awareness and immediate threat visibility into hundreds and thousands of endpoints, respond to nation-state and insider threats, and neutralize cyber attacks quickly. ThreatResponder® allows investigators to conduct incident response and computer forensics investigation on a remote endpoint.

### Benefits to Incident Response

- Significantly save cost (or increase revenue) by eliminating the use of technologies that are ineffective, manual, or do not scale
- Conduct multiple enterprise IR investigations simultaneously with a single Incident Responder
- Quickly identify and mitigate threats
- Perform remote enterprise investigations from the comfort of your home or office
- Conduct legally defensible investigations



November 2, 2019 - December 2, 2019

ID	INDICATOR	REASON	ACTION TAKEN	ENDPOINT	WHEN	#
A-40	194.188.137.46	Process chrome.exe connected to a malicious IP	NONE	JENNIFER-PC	8 hours ago	18
A-37	6e59861931f2796e3876c278f6d480	A process (6e59861931f2796e3876c278f6d480) that was found MALICIOUS in TRIP tried to execute.	6e59861931f2796e3876c278f6d480 execution was blocked	MARY-PC	9 hours ago	1
A-36	15k49364c4733a3d376f99f7497753	Elmalika type attack detected from IP 10.100.0.120	Connection to 10.100.0.120 was terminated	MARY-PC	9 hours ago	1
A-34	c811c2158b86c732f3f2f64c563ad	Process injection attempt detected	powershell.exe execution was terminated	MARY-PC	9 hours ago	1
A-33	f5ae036e4d8f93176271c48402fe	Malicious macros execution detected	cmd.exe execution was terminated	MARY-PC	9 hours ago	1
A-2	ff9e774d8173abd31e6c1e6c1c6	Process injection attempt detected	powershell.exe execution was terminated	PAUL-PC	9 hours ago	2
A-3	e5f86232c7928d881f751c3262485	Process injection attempt detected	inject.exe execution was terminated	PAUL-PC	9 hours ago	2
A-25	622d21c40e29f983e8b8f6f1473ac1	Malicious macros execution detected	cmd.exe execution was terminated	JENNIFER-PC	12 hours ago	3
A-27	6e59861931f2796e3876c278f6d480	Malicious macros execution detected	ipfs.exe execution was terminated	JENNIFER-PC	12 hours ago	1
A-23	16d836f928764e4b35f1c2714164f51	A process (16d836f928764e4b35f1c2714164f51) that was found MALICIOUS in TRIP tried to execute.	backenergy.exe execution was blocked	JENNIFER-PC	12 hours ago	2

### Threat Detection

- Detect exploit, fileless, and malware attacks
- Monitor process, file system, registry, network, and memory activities
- Leverage threat intelligence, IOCs, signatures, MITRE ATT@CK techniques, behavior, and Artificial Intelligence (AI) and Machine Learning (ML) algorithms to detect threats quickly

### Threat Hunting

- Sweep through enterprise endpoints and quickly find “the needle in the haystack”
- Search for unknown or hidden threats
- Query using natural language commands – “Ask Curiosity”



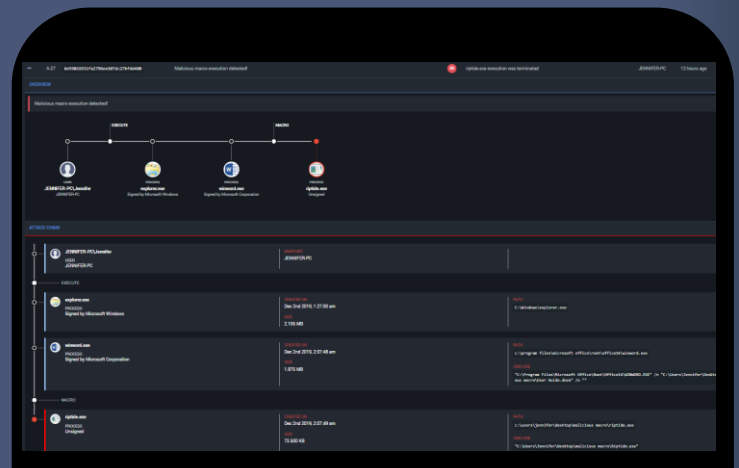


### Malware Analysis

- Onboard Malyzer<sup>®</sup> performs automated dynamic and static malware analysis with the click of a mouse and produces results within minutes
- Avoid uploading targeted malware or potentially sensitive files to VirusTotal or “detonation chambers”
- Gain contextual information via “Tell-the-Story” into everything you want to know about a malware’s intent, capabilities, and risk, including process, network connections, registry, memory, and file system activities

### Threat Response

- Contain/quarantine infected or compromised endpoints to avoid lateral movements
- Terminate a process and kill active network connections
- With **LiveView**, drill into a remote endpoint through a secure console and execute native OS commands and explore the file system and registry of remote endpoints
- Acquire detailed forensics evidence for post-incident investigation



### Forensics Investigation

- Conduct full-blown incident response life cycle activities – from detection to remediation
- Gain situational awareness and insight into the extent of a breach
- Know the dwell-time of malicious activities since the target endpoint was commissioned
- View the timeline of events since the system was installed to the present time
- Perform forensics and incident response on remote offline and online systems

### Incident Remediation

- Immediately remediate and eradicate threats within minutes of deploying agents
- Enforce endpoint access control
- Whitelist or blacklist file hashes and signers
- Kill or terminate a malicious code or IP connection



Founded in 2004, NetSecurity’s vision is “to be the brand of choice in security, forensics, and training.” Our mission is to protect your assets from advanced cyber attacks and data breaches. NetSecurity provides unparalleled innovation, world-class quality, customer-focused, and timely solutions.

GSA IT 70 Contract (#GS-35F-0288Y) | GSA 8(a) STARS II (#GS00Q17GWD2269) | SBA Certified 8(a) SDB | Cage Code: 3CCJ4

© NetSecurity<sup>®</sup> Corporation | 22375 Broderick Drive, Suite 210, Dulles, VA 20166

Phone: (703) 444-9009 | Toll Free: 1-855-NETSECURITY | Web: netsecurity.com | Email: 911@netsecurity.com

NetSecurity<sup>®</sup>, NetSecurity Logo, ThreatResponder<sup>®</sup>, ThreatRover<sup>™</sup>, Who is Hacking Your Network<sup>™</sup> and Hands-On How-To<sup>®</sup> are registered trademarks of NetSecurity Corporation.