SOLUTIONS DATA SHEET

DIGITAL GUARDIAN®

Responder® PRO
Powered by Digital DNA®

Digital Guardian & CounterTack Partner to Fight Advanced Malware

Innovation is important in every business, even in the business of cyber-crime. One of their latest innovations, **fileless malware**, is reaping great benefit for hackers and cyber-criminals and great risk for your business. Fileless infections are exactly what they seem to be: malware or virus infections that don't use any files in the process. The malware is written directly into the physical memory (or RAM) and is capable of eluding most detection technologies such as desktop firewalls and anti-virus programs.

Prior to 2014, fileless malware was rarely seen in the wild, but since then, it has evolved to be one of the most lethal malware threats. Examples like PowerSniff and PowerWare are registry-based threats that hide malicious code in the Windows Registry without leaving any footprint in the form of persistent data – making them very difficult to detect without specialized incident response tools like Responder PRO.

COLLECT AND ANALYZE THREAT INTELLIGENCE IN-MEMORY

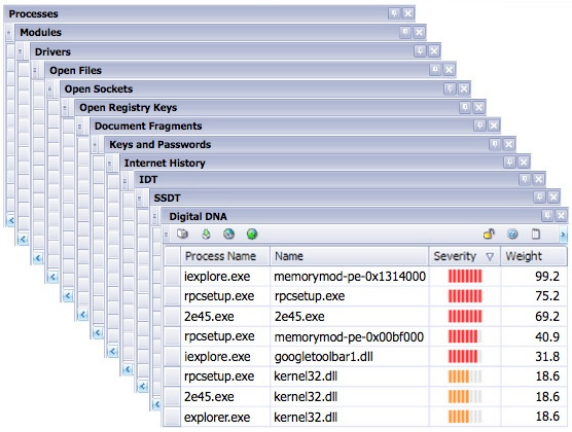
Responder PRO is the industry standard physical memory and automated malware analysis solution designed specifically for Incident Responders. It is the most advanced tool available for reverse engineering available today.

With its powerful memory forensics and malware identification capabilities, Responder PRO allows incident response professionals to collect and analyze critical threat intelligence that can only be found in physical memory such as chat sessions, registry keys, encryption keys, and socket information. With this information, incident responders can effectively validate and respond to a security incident.

Every element of physical memory is provided, from the standard process and module details to extensive details on open files, sockets, registry keys. Document fragments, internet history, and keys and passwords are automatically extracted from memory and made available.

GET COMPREHENSIVE VIEW OF PHYSICAL MEMORY

Responder PRO's deep malware analysis includes automated code disassembly, behavioral profile reporting, pattern searching, code labeling, and control flow graphing and is powered by Digital DNA®. It can analyze both 32-bit and 64-bit memory.



DIGITAL GUARDIAN®

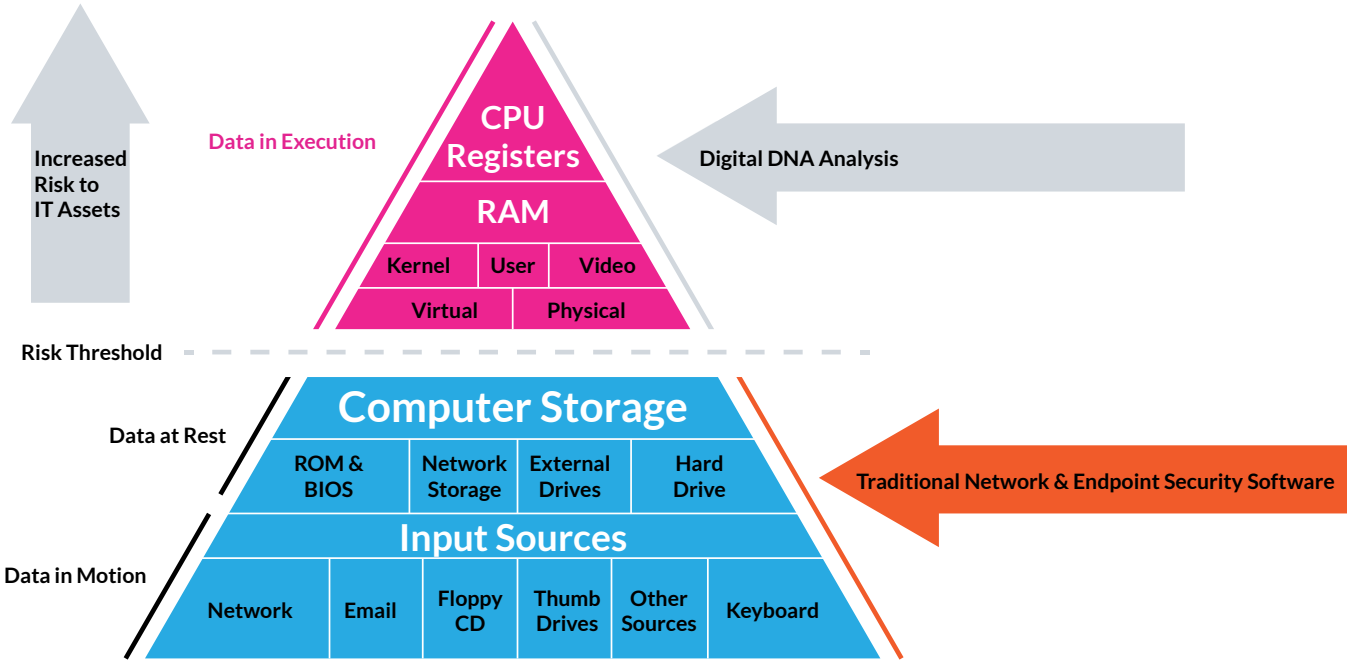
For more information, visit
www.digitalguardian.com

MALWARE DETECTION MADE EASY WITH DIGITAL DNA®

Digital DNA®, the patented core technology, lies at the heart of Responder PRO. With its unparalleled memory forensics and behavioral analysis capabilities, Digital DNA detects zero-days, rootkits and other malware not detected by signature-based solutions. Digital DNA cuts through the wide array of anti-forensic measures employed by today's most stealthy malware and identifies potentially malicious software running in physical memory. It scans live physical memory identifying malicious behaviors rather than matching patterns and signatures.

Digital DNA proactively identifies and analyzes the most advanced malware threats in physical memory, including those used against global organizations for theft of intellectual property, business intelligence, customer records, and classified information. Digital DNA performs the following steps:

- Scans live physical memory or memory snapshots
- Identifies behaviors and techniques rather than patterns and signatures
- Calculates a module-level threat score based on identified behaviors
- Detects malicious software, APTs, zero-days, and rootkits that traditional anti-virus software can't.



ABOUT DIGITAL GUARDIAN

Digital Guardian is the only data aware security platform designed to stop data theft. The Digital Guardian platform performs across traditional endpoints, mobile devices and cloud applications to make it easier to see and stop all threats to sensitive data. For more than 10 years we've enabled data-rich organizations to protect their most valuable assets with an on premise deployment or an outsourced managed security program (MSP). Our unique data awareness and transformative endpoint visibility, combined with behavioral threat detection and response, let you protect data without slowing the pace of your business.

SHARE