SOLUTIONS DATA SHEET

DIGITAL GUARDIAN®

Active Defense™ 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 Active Defense.

DETECT MALWARE IN-MEMORY WITH ACTIVE DEFENSE™

With unparalleled capability to analyze and detect malicious code executing in memory, Active Defense puts your team firmly in control of every investigation, allowing you to quickly and easily pinpoint compromised systems and determine scope of breach, enabling you to eliminate advanced threats such as fileless infection.

Active Defense is powered by patented Digital DNA® technology that identifies specific behavioral traits of every process running in memory.

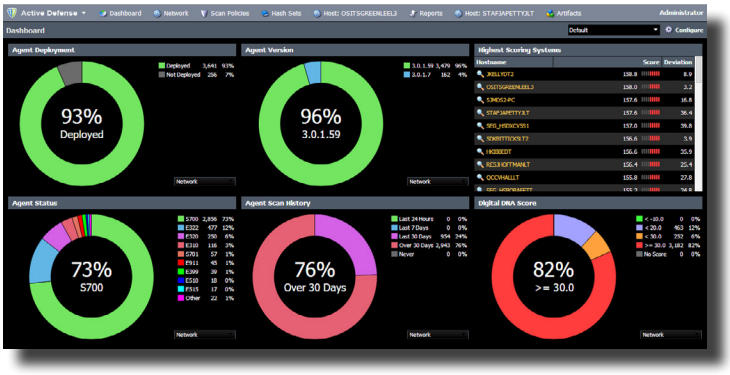
Once a threat has been identified, Active Defense's collection and analysis tools empower you to determine initial points of infection, isolate lingering malicious files and system changes, and generate threat intelligence to harden endpoints against future attacks. By streamlining the incident response lifecycle, Active Defense allows you to rapidly scale your investigative efforts to hundreds of thousands of endpoints without requiring expensive armies of highly skilled analysts.

HUNT DOWN MALWARE ON ENDPOINTS

Active Defense automatically reverse engineers malware packages, showing operators how code modules relate, along with key intelligence on variants, so teams can proactively hunt down malicious code across the enterprise.

Severity information allows Incident Response teams to rapidly prioritize the verified, critical threats, instead of spinning cycles chasing after every alert that could pose a potential threat. Active Defense cuts down the time to detection, and provides teams with a rapid visualization of your malware problem.

Active Defense is the most powerful and most advanced, enterprise-class malware hunting platform for infected endpoints.



Active Defense Console

DIGITAL GUARDIAN®

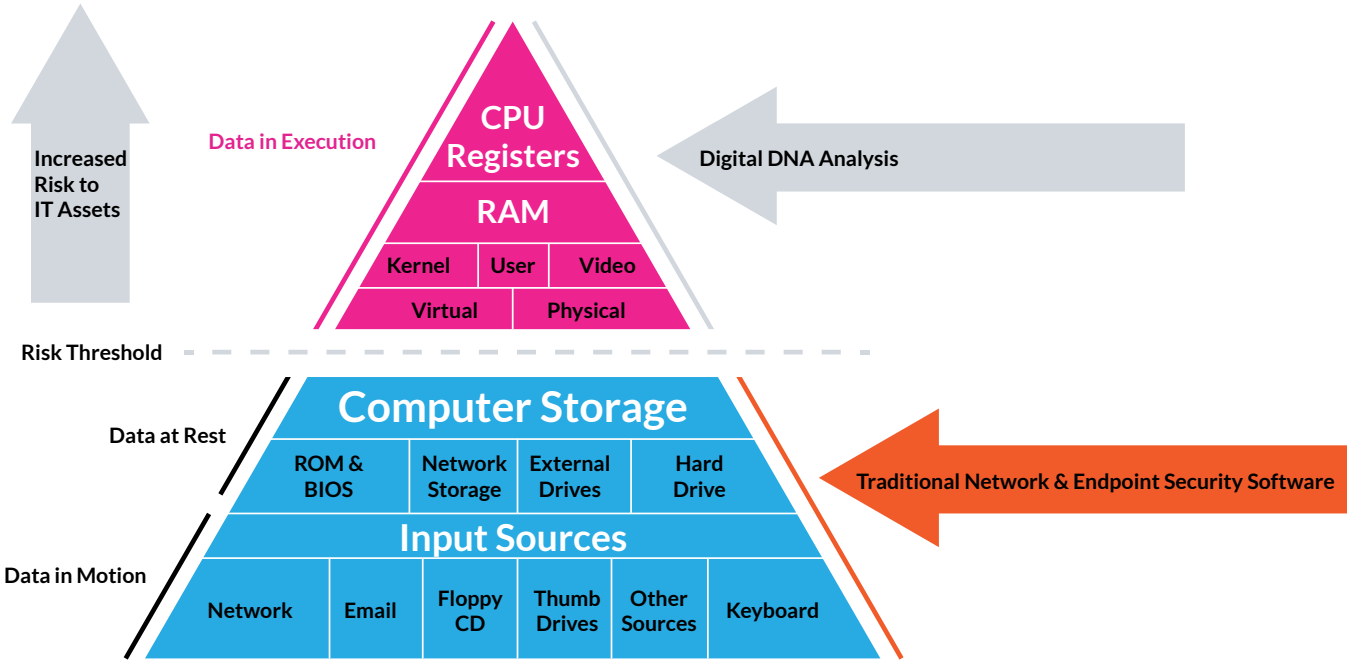
For more information, visit
www.digitalguardian.com

MALWARE DETECTION MADE EASY WITH DIGITAL DNA®

Digital DNA®, the patented core technology, lies at the heart of Active Defense. 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