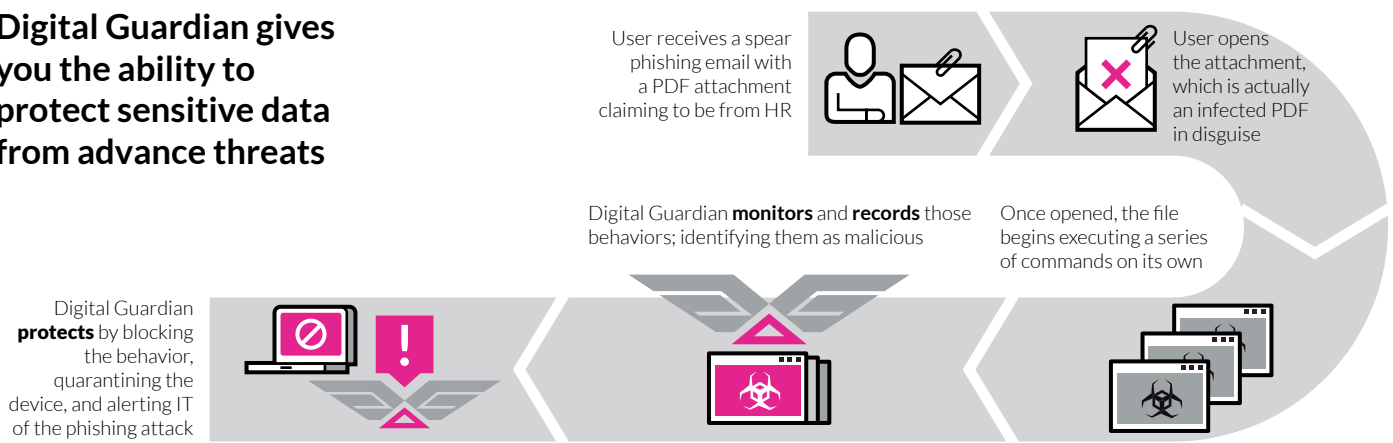**DIGITALGUARDIAN®**
Advanced Threat Protection

PROTECT THE DATA FOR THE BEST DEFENSE AGAINST ADVANCED THREATS

Attacks are inevitable. With the proper protocols and tools in place, you can spot and contain breaches before sensitive data gets out. **Digital Guardian for Advanced Threat Protection** is uniquely focused on understanding and preventing threats targeting your data and placing your systems at risk.

It takes a data-centric approach to advanced threat detection, incident response and prevention that ensures security travels with the data. Adding **DG for Advanced Threat Protection** gives you the only security solution that protects sensitive data regardless of the source of attack.

Digital Guardian gives you the ability to protect sensitive data from advance threats

User receives a spear phishing email with a PDF attachment claiming to be from HR

User opens the attachment, which is actually an infected PDF in disguise

Digital Guardian **monitors** and **records** those behaviors; identifying them as malicious

Once opened, the file begins executing a series of commands on its own

Digital Guardian **protects** by blocking the behavior, quarantining the device, and alerting IT of the phishing attack

PROTECT THE DATA, REGARDLESS OF THE ATTACK VECTOR
- Detect in real-time behaviors indicative of attacks targeting your systems, users and data via Digital Guardian's attack sequencing approach.
- Set rules to alert the user to the presence of an attack (via prompts) stop the attack in progress; notify IT in near real time and initiate collection of artifacts for forensic validation.

CUT ANALYST WORKLOAD, IMPROVE WORKFLOW, INCREASE INCIDENT HANDLING CAPACITY
- Expedite delivery of critical alerts to speed response time and containment.
- View correlated events and individual alerts for visibility of an attack or malicious activity by highlighting the individual rules which triggered the correlated event.
- Automate collection of artifacts to reduce response time and enhance the ability to stop an attack in progress.
- See all systems that are at risk or infected by using Digital Guardian's automated binary analysis to track any file determined to be malicious or suspicious.

MAXIMIZE THE RETURN ON YOUR SECURITY INVESTMENTS
- Protect your endpoints from threats discovered at the network layer using DG's integration with existing malware protection systems (FireEye and Palo Alto).
- Download threat information from third party threat feed sources you define, directly to the DG agent to block agent execution within minutes of identification of known threats.
- Use network security infrastructure to gather and submit suspicious files for detonation before they execute.
- Get additional analysis and guidance on what action to take as a result of direct integration with VirusTotal. For example, automate the submission of a file hash for immediate analysis or industry reputation and if deemed to be a threat, all endpoints can be informed of the threat and set to block and alert should the threat be seen by any system whether on or off your network.

EXTEND YOUR DATA PROTECTION WITH DG ADD-ON MODULES
- Digital Guardian offers a suite of add-on modules that provide advanced encryption, extend your data protection to the network and more.

DIGITALGUARDIAN®
by **VERDASYS**

WHY DIGITAL GUARDIAN FOR ADVANCE THREAT PROTECTION

1 **REAL-TIME VISIBILITY**

To avoid the risk of missing critical artifacts and to maintain a full narrative of an attack you need real-time visibility. Digital Guardian includes real-time and historic visibility into more than 200+ parameters associated with system activities. This includes: process activity, user-mode and kernel execution events, file system activity, network and registry activity, and user-logon activity. Deep visibility ensures you have all the critical information needed to identify patient zero and drastically reduce your overall response time while validating the impact the attack had on your data.

2 **CONTEXT**

Security teams today are overwhelmed with alerts from ineffective products that lack any context or prioritization of attacks; so they end up missing the real threats targeting their data. Digital Guardian provides host visibility as well as contextual intelligence about attacks targeting your data. Our solution gives you the context required to prioritize your response and answer the crucial who, what, why, and how questions.

3 **DATA AWARENESS**

Advanced threats are intent on compromising your systems in order to gain access to your data. To protect your most critical data you must first understand it. New advanced threat protection products have no concept of data and traditional DLP products lack the understanding of threats. Digital Guardian is the first product to bridge the gap between system security and data protection by delivering a single solution combining threat prevention with context based data protection from a single agent.

4 **FLEXIBLE DEPLOYMENT**

Only Digital Guardian offers complete data protection through an on premise, cloud-based managed service, or a hybrid of both. Our cloud-based managed services are the answer if you have more IP than IT. As an extension of your team, we'll expertly develop, deploy, and manage all of your policies enterprise-wide as if they were our own.

DIGITAL GUARDIAN PRODUCT PLATFORM

Digital Guardian is the only data-centric security platform designed to stop data theft.

DGMC
Digital Guardian
Management Console

Your web-based command center. Deploy agents, create and manage policies, alerts and reports.

Advanced Threat Protection
Advanced threat detection, incident response and prevention that ensures security travels with the data.

Data Loss Prevention
Everything you need to stop sensitive data from getting out of your organization.

Data Visibility & Control
Out-of-the-box data visibility and device control.

DG Agent
The only endpoint agent compatible with Windows, Mac & Linux.

ABOUT DIGITAL GUARDIAN

Digital Guardian is the only data-centric 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