DIGITALGUARDIAN®

For Ransomware Protection

RANSOMWARE IS ON THE RISE

DETECT, BLOCK AND PREVENT RANSOMWARE WITH DIGITAL GUARDIAN

Cybercriminals have turned to ransomware as the latest go-to tool for attacking and extorting businesses using a wide range of variants such as WannaCry, Cryptowall, Samas, Locky, and TeslaCrypt. The recent outbreak of WannaCry was one of the largest and worst ransomware campaigns ever, as the ransomware spread to over 200,000 computers spanning 150 countries in the course of a weekend.

Traditional signature-based antivirus and threat detection methods has proven to be woefully ineffective during such unprecedented attacks. Digital Guardian's Managed Security Program for Advanced Threat Protection (ATP) provides the highest level of protection from ransomware attacks by focusing on understanding and protecting the attackers' main target - your data.

HOW DOES DIGITAL GUARDIAN STOP RANSOMWARE?

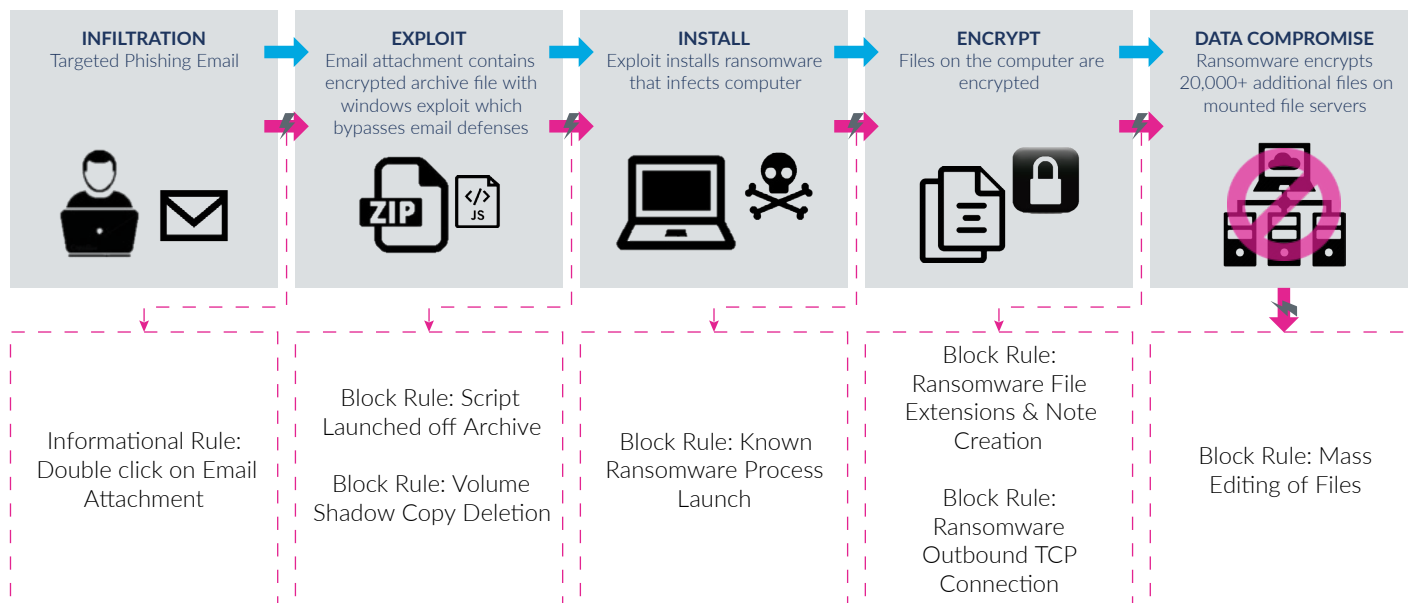### DETECT AND PREVENT RANSOMWARE IN REAL-TIME

Our Advanced Threat Protection (ATP) software uses a combination of threat intelligence and behavior-based detection to stop ransomware before it compromises your organization. Digital Guardian's ATP provides deepest visibility into infection sequence and detects behaviors indicative of ransomware.

The behavioral rules detect and block advanced threats across entire lifecycle. The below chart highlights each of the stages as ransomware is delivered, and the corresponding rules of Digital Guardian's ATP that mitigates against the attack Our rules can even prevent the encryption routines from being applied to your most sensitive data and protect them from being compromised.

Our ATP solution is delivered as fully managed service so you can focus on your core business and leave ransomware worries to our data protection experts.

Digital Guardian Detects and Blocks Ransomware
This chart explains each of the stages as ransomware is delivered, and the corresponding rules of Digital Guardian's ATP that mitigates against the attack.

INFILTRATION	EXPLOIT	INSTALL	ENCRYPT	DATA COMPROMISE
Targeted Phishing Email	Email attachment contains encrypted archive file with windows exploit which bypasses email defenses	Exploit installs ransomware that infects computer	Files on the computer are encrypted	Ransomware encrypts 20,000+ additional files on mounted file servers
Informational Rule: Double click on Email Attachment	Block Rule: Script Launched off Archive Block Rule: Volume Shadow Copy Deletion	Block Rule: Known Ransomware Process Launch	Block Rule: Ransomware File Extensions & Note Creation Block Rule: Ransomware Outbound TCP Connection	Block Rule: Mass Editing of Files

WHY DIGITAL GUARDIAN FOR RANSOMWARE PROTECTION?

1

INSTANT TIME-TO-VALUE

Implementation and management of your advanced threat protection infrastructure. No in-house infrastructure, training or subject expertise required

2

24*7 EXPERTS SUPPORT

Our cyber security experts are constantly reviewing your data for anomalous behavior and alerting you immediately upon discovery of ransomware and other advanced threat types

3

HUNT PROACTIVELY AND RESPOND IMMEDIATELY

Our proven Incident Response and Threat Hunting methodology help your operationalize these complex tasks and respond to threats immediately

4

DATA-CENTRIC THREAT PROTECTION

Industry's only Advanced Threat solution that fully understands and protects your DATA. Our MSP for ATP protects from multiple sources of attacks - ransomware, malware, malware-free attacks and other suspicious data movements/egress

5

ONGOING THREAT INTELLIGENCE

Our team harnesses both externally and internally generated intelligence feeds for immediate detection based on known ransomware variants

Gartner®

Magic Quadrant Leader