



Managed Security Program for Endpoint Detection & Response

Get The Latest Cyber Defense Strategies & Intelligence Now

Today's malware is sophisticated, targeted and difficult to detect. With the speed of new threats accelerating, attacks have become inevitable. On the other hand, building and retaining a team of cyber security experts that can detect, respond and remediate these attacks can be incredibly challenging.

Digital Guardian's Managed Security Program for Endpoint Detection & Response (EDR) is led by an elite cybersecurity expert who built the SOC for a Fortune 100 company where sensitive IP was the life blood of the organization. Our elite team of experts proactively hunt, detect and respond to attacks in real-time to contain ransomware and other advanced threats before your organization's sensitive data is breached.

Our service provides the highest level of protection of your data from:

- Zero-day attacks
- Polymorphic Malware
- Fileless Malware
- Ransomware

"With its data-driven approach, Digital Guardian applies analytics to users and content to classify anomalous behaviors, detecting threats from those outside and inside the organization."

*Vendor Landscape: Global Managed Security Services, 2017
Converged Services Thrive While Isolated Offerings Go Extinct
Jeff Pollard*

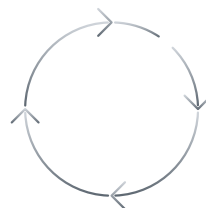
FORRESTER®

A Program-Based Approach

Digital Guardian's unique approach for solving data protection challenges is to offer a proven combination of people, process and technology.



+



+



People

Cybersecurity experts led by a former Fortune 100 cyber-defense leader

Process

Proven methodology for Incident Response and Threat Hunting

Technology

Detection and response technology that has the contextual understanding to protect your data from all threats

What You Get



Current State Gap Analysis

- Initial deep dive review by DG advanced threat team
- Formal presentation with review of identified threats and mediation recommendations



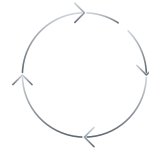
Advanced Threat Policy Deployment, Maintenance & Updating

- 200+ behavior based rules for threat detection & response on the endpoint
- Triage, tuning &/or whitelisting for alerts & alarms



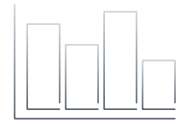
Proven Cyber Experts "Eyes on Glass" at Your Service

- Alert triage & notification of high fidelity alerts
- Alert analysis includes root causes or entrance vectors, remediation recommendations
- Remote incident response and threat neutralization support
- Proactive threat hunting looking for IOCs and IOAs



Ongoing Threat Intelligence

- DG team harnesses external & internal intelligence feeds for immediate detection based on known threat activity
- Advanced network device, SIEM, VirusTotal and custom threat feed integration available



Cyber Threat Advanced Alerting and Reporting

- Executive level reporting on cyber threat activity
- Process usage, threat scan and alerts reporting

Why Digital Guardian MSP for Endpoint Detection & Response

1

Fill Your Security Talent Gap

Leverage our incident responders and threat hunters with experience building incident response and threat hunting programs at data-sensitive Fortune 100 companies.

2

Get EDR That Works

Standing up EDR technology and a successful cyber threat program is complex and resource intensive. Even some of the largest companies turn to our MSP team for effective protection.

3

Use The Resources You Have More Effectively

With the DG MSP team managing the infrastructure and the administration, your team can focus on governance and proactive security.

4

Achieve Exceptional Time to Value

DG MSP customers repeatedly tell us that they were able to establish or improve their EDR program faster than they ever could have done by themselves, or with any other vendor.

5

Take Advantage of Our Programmatic Best Practices

You gain the benefit of our insights, experiences and processes protecting the most critical information for hundreds of customers across a wide range of industries

ABOUT DIGITAL GUARDIAN

Digital Guardian's data protection platform safeguards your sensitive data from the risks posed by insider and outsider threats. By

harnessing our deep data visibility, real-time analytics and flexible controls, you can stop malicious data theft and inadvertent data loss.

