



# Digital Guardian for Insurance

## Importance of Regulatory Compliance and Data Protection for Insurance

The leading insurance companies all know how to effectively manage risk throughout their business. Mitigating that risk includes safeguarding the volumes of digital data created every day, like personally identifiable policyholder information and intellectual property like actuarial tables and pricing models. Business leaders need a way to know they can offer innovative solutions to their customers securely. Information security leaders need to document compliance and see when sensitive data is at risk to prevent breaches.

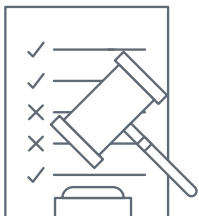
*“It is critical that insurance companies make sufficient investments and become much more sophisticated in the application of the breakthrough technologies that are increasingly being used by cyber criminals.”*

*(Source: Accenture Security, 2018 State of Cyber Resilience for Insurance)*

Achieve meaningful impact in reducing cyber risk with Digital Guardian, a Marsh Cyber Catalyst.



## Key Challenges



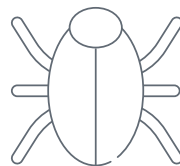
### Regulatory Pressure

Compliance requirements such as GDPR, SOX, and GLBA demand that policyholder data be protected.



### Consumer Expectations

To establish trust and meet customer needs, insurance firms need to deliver an innovative digital experience without sacrificing data privacy.



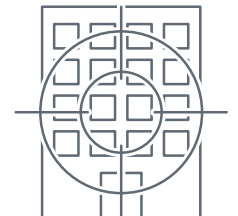
### Malware

Malicious software including ransomware, keyloggers, and cryptojackers needs to be detected and remediated quickly before policyholder details leaks.



### Insider Threats

Employees, either by malice or mistake, can leak sensitive data exposing the organization to penalties, reputational damage, or loss of competitive advantage.



### External Threats

Cyber criminals compromise trusted service providers, payment partners, and contractors to gain backdoor access to policyholder data for sale on the black market.

# Digital Guardian's Data Protection Platform Delivers

## Visibility into What Data to Protect

Digital Guardian sees and correlates the most comprehensive set of system, user, and data events enterprise wide. This enables you to identify both structured (PII, PHI) and unstructured data (actuarial tables, pricing models). Digital Guardian automatically identifies and tags sensitive data, even before you develop formal policies.

## Understanding of What Data is at Risk

Understanding when data is at risk requires visibility into user behavior, data access and movement. Digital Guardian combines DLP, EDR, and UEBA to flag risky activity. Our platform secures sensitive data wherever it lives and wherever it is shared, performing equally across Windows, mac, or Linux operating environments.

## Enforcement and Education with Flexible & Automated Controls

Digital Guardian ensures that policyholder data and intellectual property remains under your control. Our context and behavior-based rules range from logging to blocking prohibited actions, stopping insider and outsider threats immediately. Real-time prompts increase employee awareness and educate users on proper use of sensitive data.

## Support for Evolving Compliance Regulations

The value of policyholder data has led to a growing list of compliance regulations including GDPR, GLBA, and SOX. You can find, tag, and protect all your regulated data with Digital Guardian and deliver full compliance reports to support internal and external audits.

# Secure Your Sensitive Assets Against Insider and Outsider Threats



## Policyholder Details

- Personally Identifiable Information (PII)
- GDPR Special Data

## Compliance Data

- Payment Card Industry Data Security Standard (PCI DSS)
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)

## Intellectual Property

- Actuarial Tables
- Client Acquisition Strategy
- M&A Plans

## 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.

