DIGITALGUARDIAN®

ICDIGITAL

7 Reasons to Move to SaaS Data Protection

2018

www.icdigital.com/digitalguardian

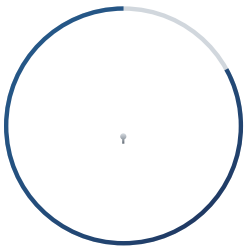
Table of Contents

Introduction

Almost every organization manages data that has value, whether it is personal data used for identity theft or insurance fraud, financial data used for insider trading, or corporate intellectual property sought by competitors. Protecting sensitive data is an ongoing challenge for security professionals.

The challenge grows each year. Cybercriminals are better funded than ever before, attacks are more varied, ranging from those that are very sophisticated, to those that rely on human weaknesses. Defending against these attackers requires much more than purchasing technologies. Successful defense require a combination of the right technologies, people, and processes. While some companies can build and maintain these resources internally, for many others leveraging external expertise and cloud infrastructure can deliver better results.

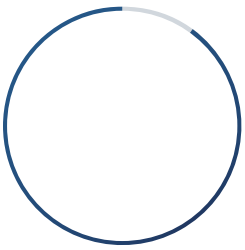
In the early days of the cloud, organizations were reluctant to adopt cloud strategies; security delivered via the cloud wasn't even a consideration. The proven effectiveness of cloud deployments in scalability, cost, and security have changed that. Today, companies of all sizes broadly adopt cloud platforms. According to a report by Oracle and KPMG, 87% of the organizations they surveyed have a "cloud-first" orientation and "83% rate cloud security as good as or better than on-premises security"1. In over 90% of these companies, at least half of their cloud data contains sensitive information.



83%

rate cloud security as good as or better than on-premises security

Source: Oracle and KPMG Cloud Threat Report 2018



90%

of these organization say at least half of their cloud data is sensitive

Source: Oracle and KPMG Cloud Threat Report 2018

As organizations adopt the cloud to run their business more efficiently, it is logical that the cloud and Software as a Service (SaaS) can deliver a more efficient data security platform. Digital Guardian's Data Protection Platform leverages SaaS to provide data protection in a package that results in superior security, better economics, and reduced overhead. Compared to legacy, on-premises infrastructure, this solution is delivered via our secure cloud and provides the performance, scalability and cost advantages enterprises need. With Digital Guardian's team managing the infrastructure, your security resources won't need to spend time learning how to configure, manage, and update applications.

7 Reasons to Move to SaaS Data Protection

You buy security products and services to more effectively manage risk. Purchasing a solution with a deployment model that diminishes your ability to do so doesn't make sense. Here are the 7 reasons why moving to SaaS data protection enables you to manage risk more effectively.

1. Better Use of Scarce Security Resources

No organization has all the security resources it needs. Let your team focus on identifying and mitigating risks to your sensitive data and less time on acquiring, building, and maintaining the infrastructure. With the number of threats facing organizations, it makes no sense to have scarce resources managing software for updates and patching, when they could be conducting higher level tasks or those that require an on-site presence. Digital Guardian's SaaS enables you and your team to focus more time, energy, and resources on identifying and mitigating risks to your sensitive data and less time on acquiring, building and maintaining the infrastructure.

1.5 Million Number of unfilled cybersecurity jobs worldwide, by 2020.

2. Faster Time-to-Value

Software requires infrastructure. This includes servers on which the software runs, databases to store data, and web servers for accessibility, each of these requires time and effort to deploy. With Digital Guardian, these on-premises hardware and software dependencies disappear. Some enterprise solutions can take months to test, configure, and deploy. With Digital Guardian's SaaS solution, our professionals deploy, host, and manage your data protection infrastructure for you. Customers have the luxury of not having to worry about the supporting hardware and software that is required for management and reporting functions.

3. More Compute Power to Detect Threats

Intense CPU functions are easily enabled through cloud compute power and scalability. Processor intensive functions such as threat hunting, anomaly detection, forensic collection, behavioral analytics or risk profiling through the use of advanced statistical models and machine learning, all are well suited for the cloud's flexible scale.

Understanding of risk, vulnerabilities and compromises requires advanced analytics, and advanced analytics require visibility and context.

Digital Guardian's cloud leverages streaming data from Digital Guardian endpoint agents and network sensors to provide the deepest visibility into system, user and data events. That visibility powers security analyst-approved dashboards and workspaces to enable data loss prevention, endpoint detection & response and user entity & behavior analytics from a single console.

Digital Guardian's User & Entity Behavior Analysis (UEBA) capabilities use machine learning and telemetry to gain an understanding of how both users and systems typically behave within an environment. You can also establish malicious intent by analyzing suspect actions in complete context.

Centralized reporting in the cloud gives you the ability to aggregate, analyze and query events across the network and endpoints over longer periods of time and removes storage limitations, so you can detect abnormal file operations or unauthorized attempts to exfiltrate data. Events that fall out of the 'normal' ranges that warrant additional investigation are highlighted for your Incident Response (IR) and security teams.

4. Elastic Scalability

A primary benefit of a cloud architecture is the ability to scale up (or down) in real time. Instead of ordering new hardware, testing updates in a development environment, rebalancing servers, and training new personnel, the Digital Guardian Cloud scales on demand. Adding endpoints anywhere in the world is simple, the Digital Guardian cloud adapts to the increased deployment.

5. Simplified and Cost-Efficient Maintenance

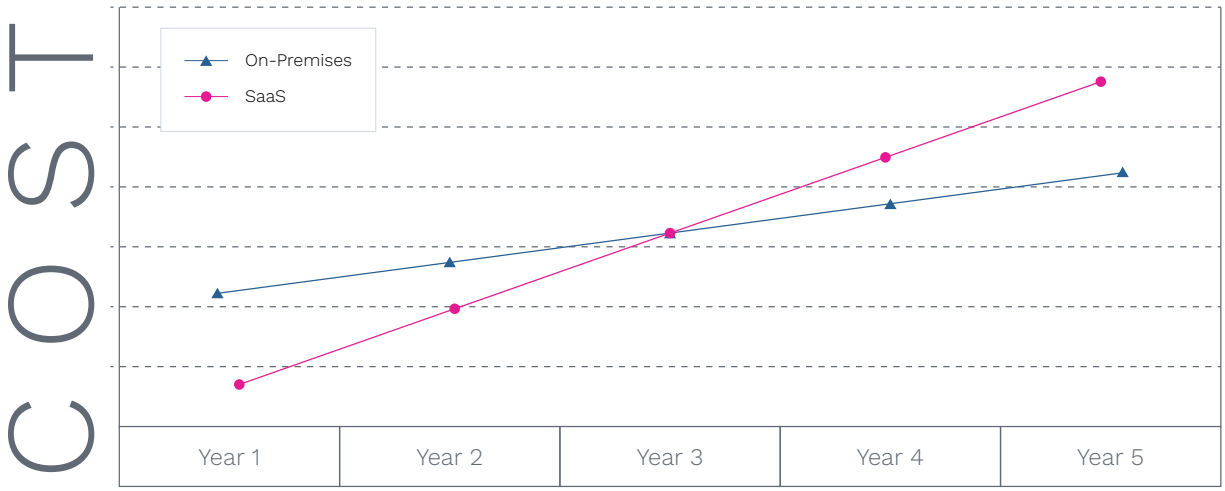
Multi-tenancy is an architecture in which a single instance of a software application services multiple customers, or tenants. Software development and maintenance costs are shared, driving down expenditures, resulting in savings that are passed onto you, the customers.

With a multi-tenant architecture, the provider only has to make updates once in order to share them with all of its 'tenants.' Meaning, Digital Guardian can run one instance of our application on one instance of a database and provide access to multiple customers. Each tenant's data is isolated and remains invisible to other tenants – you do not share or see each other's data. Multi-tenancy architecture also allows Digital Guardian to efficiently service everyone from small customers, whose scale may not warrant dedicated infrastructure, to large enterprises that need access to the cloud's virtually unlimited compute resources.

6. Predictable and Lower Total Cost of Ownership

Many companies forget to consider the total cost of ownership (TCO) of their on-premises investment. Deploying an on-premises solution is expensive to design, build, and maintain, and keeping your software updated and modernized requires a much nimbler IT team. With a SaaS solution, you get a lower entry cost. There is no additional capital expenditure (CAPEX) such as additional software or hardware to be purchased reducing the upfront investment. SaaS solutions also deliver more value over time, due to a reduction of ongoing management

costs. Lastly, as you grow, we take care of the infrastructure, easily scaling with you in real-time.



7. Better Defenses Through Threat Intelligence Feeds

With a standalone solution, organizations analyze their information in isolation. Every anomalous or suspicious activity that hasn't been observed previously must be investigated. To stay ahead of the evolving threat landscape, you need multiple threat intelligence sources.

Digital Guardian's purpose-built architecture and analytics change that, allowing us to enrich your data by integrating with threat intelligence services such as VirusTotal, 50+ open source threat feeds, and even orchestrate with your own security technologies such as FireEye to improve your defenses with every attempted attack. In the event new, unique, or otherwise novel threats are identified, those risks are mitigated via indicator blacklist feeds. In the event of a coordinated, large scale security event, such as WannaCry, Digital Guardian publishes protections for Managed Security Program customers that subscribe to our Endpoint Detection and Response service offering.

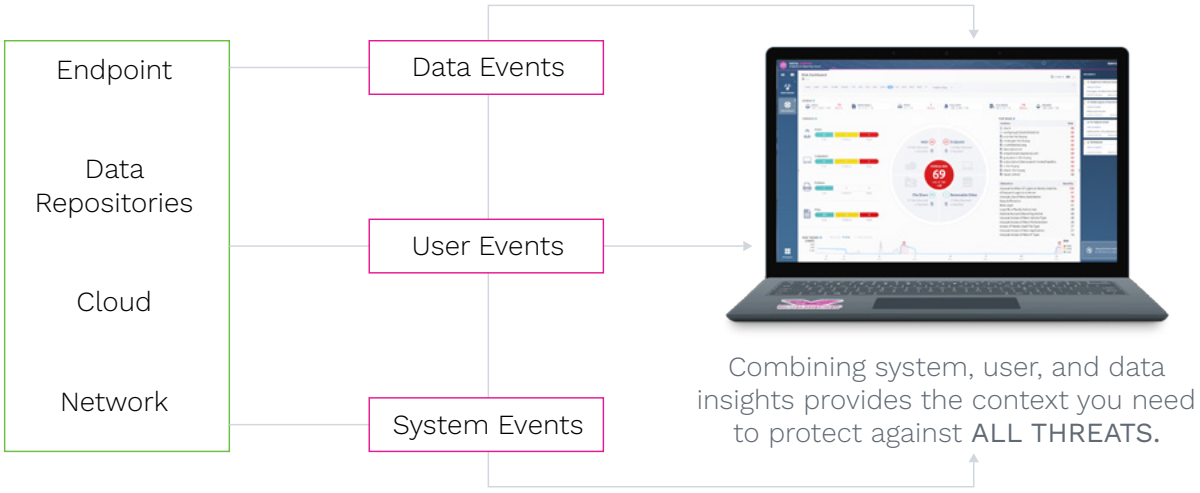
Digital Guardian's Cloud Architecture

When adopting a new security solution, you want to make sure that the provider is one you can trust. This is particularly true with SaaS solutions, since the provider shoulders the burden of security, availability and performance.

Digital Guardian's cloud architecture was built with the latest tools and methodologies to provide the scalability, data visualization, infrastructure and software integrations, and ease-of-use security teams have come to expect from software as a service. Additionally, we bring a team dedicated to your success with experience deploying Digital Guardian in large and small enterprises around the world. Our professional services team works with yours to make sure your priorities are covered and your deployment goals are met.

Big Data Security Infrastructure

Weak infrastructure can undermine a good security solution especially when that solution is tasked with monitoring and securing large and sensitive data sets. Any adequate infrastructure must have these key elements – data collection, data storage, data analysis and data visualization.



The Digital Guardian Cloud provides a purpose-built data protection platform that unifies DLP (Data Loss Prevention), EDR (Endpoint Detection and Response), and UEBA (User and Entity Behavior Analytics) into one platform. We now extend into a much broader awareness of threats, combined with the forensic artifact collection and analytics required to fully assess the risks to your data. Digital Guardian correlates and analyzes system, user and data events from endpoint agents and network sensors to provide the deep visibility and context needed to identify and remediate all threats. No on-site storage or data processing facility needed.

Infrastructure and Application Monitoring

Newly disclosed vulnerabilities in commercial software and open source components require constant vigilance. One only need look at the 2017 Equifax breach (unpatched Apache Struts)

and ransomware attacks on the National Health Services (unpatched Windows) to see the consequences of poor patching practices. Digital Guardian supports all back-end infrastructure and software systems required to run the Digital Guardian solution.

Global Reach

Digital Guardian's SaaS solution isn't limited to a single geographic location. Performance improves and costs are reduced when you remove the need to funnel all traffic through your internal network. Our global presence is matched by instant access to online reporting and remediation, on or off your network and on or off your company laptop, by employing fault tolerance, redundancy and recovery capabilities.

Our fault-tolerant systems use backup components that automatically take the place of failed components, to ensure no loss of service. Redundancy in cloud computing provisions duplicate copies of various data, equipment, and systems, that can be used if part of your cloud computing system fails. Lastly, Digital Guardian enables faster disaster recovery of critical systems without incurring the infrastructure expense of a standing up and managing a second physical site.

Integrations with Your Environment

Digital Guardian's SaaS offering integrates with iDP SAML for self-service provisioning, SIEM solutions for internal analytics and API integrations for your varying solution stack. Single sign on (SSO) allows for easier user management, because end-users are less likely to write down or forgot their multiple passwords by having to only manage one.

Our data-centric view of the extended enterprise finds, understands and protects data across the enterprise and the cloud. This rich data set is delivered directly into your existing SIEM enabling correlation against data from other network infrastructure and logs.

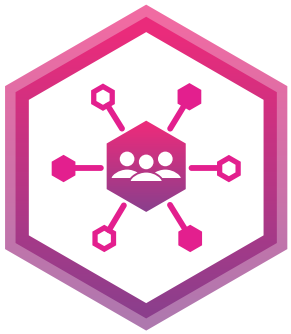
Further, in a digital ecosystem, all components are heavily dependent on one another. Application Programing Interfaces (APIs) allow applications to talk to other applications. Digital Guardian uses APIs to manipulate endpoint policies to allow for custom integration from your in-house applications.

Simplify Audit Compliance

Your users and customers want to know that you protect sensitive information. Digital Guardian utilizes SSAE18 SOC2 certified hosting facilities. Additionally, defenses, are monitored 24x7 by Digital Guardian staff with 20+ years of security experience.

Additional Digital Guardian Offerings

Want us to Manage for You?



The Digital Guardian SaaS offering is perfect for organizations with sufficient bandwidth and security expertise. Enterprises looking for more support should consider Digital Guardian's Managed Security Program (MSP). This adds support from Digital Guardian's Advanced Threat & Analysis Center (ATAC) team, security professionals with over 20 years dedicated to protecting customers' data. The ATAC team works with you to build policies that match your business goals, manages all Digital Guardian deployments and updates, and monitors your data 24x7 for suspicious or malicious actions. When policies are violated, the ATAC team provides alerts, incident response, and forensics capabilities.

About Digital Guardian

Digital Guardian provides the industry's only security platform that is purpose built to stop data theft. Our platform performs across the corporate network, traditional endpoints, mobile devices and into the cloud, buttressed by a big data analytics and reporting cloud service, to make it easier to see and block all threats to sensitive information.

For almost 15 years it has enabled data- rich organizations to protect their most valuable assets with a choice of on premises, SaaS or managed service deployment. Digital Guardian's unique data awareness combined with behavioral threat detection and response, enables you to protect data without slowing the pace of your business.

A Recognized Leader

"Leader" Gartner Magic Quadrant for Enterprise Data Loss Prevention

"The Digital Guardian endpoint covers DLP, advanced threat protection, and endpoint detection and response (EDR) in a single agent form factor installed on desktops, laptops and servers running Windows, Linux and Mac OS X, as well as support for VDI environments..."

Gartner, 2017 *Gartner Magic Quadrant for Enterprise Data Loss Prevention*

"Leader" in Forrester Wave: Endpoint Detection and Response

"Digital Guardian is a newer entrant into the space and has built an extremely exciting EDR solution on top of its data loss prevention (DLP) technology. "

Forrester, *The Forrester Wave: Endpoint Detection and Response, Q3 2018*

DIGITAL GUARDIAN®

ICDIGITAL

advisor@icdigital.com
+9714 503 2100
www.icdigital.com/digitalguardian

SHARE