imperva

WHITEPAPER

Meeting Data Security Challenges in the Age of Digital Transformation

Your data is the most valuable resource on the planet

Data is one of the world's most important commodities. An explosion of data has enabled companies and brands to more easily build personal relationships with consumers, using what they know about them to provide tailored experiences and recommendations. The internet has been the catalyst, enabling connected consumers to leverage the most transformative innovations of the modern era for purposes such as entertainment, education, knowledge, social sharing and shopping. They willingly (or unwittingly, in some instances) trade their personal data to enterprises to streamline interactions or get something they want in return.

Today, connectivity has given power to enterprises born in the modern era as data emerges as the world's most valuable asset. The most valuable companies are no longer the likes of Standard Oil and Ford, but instead Apple and Amazon, the biggest purveyors of data.

As with every important and valuable commodity, it is critically important to protect data. Virtually everything in our personal and professional lives today soon will be interconnected with everything else, providing many points at which data can be stolen, corrupted, or compromised in some way. Security threats are no longer just outside-in. The paths to data are manifold and each path must be protected to ensure the integrity and security of every other path.

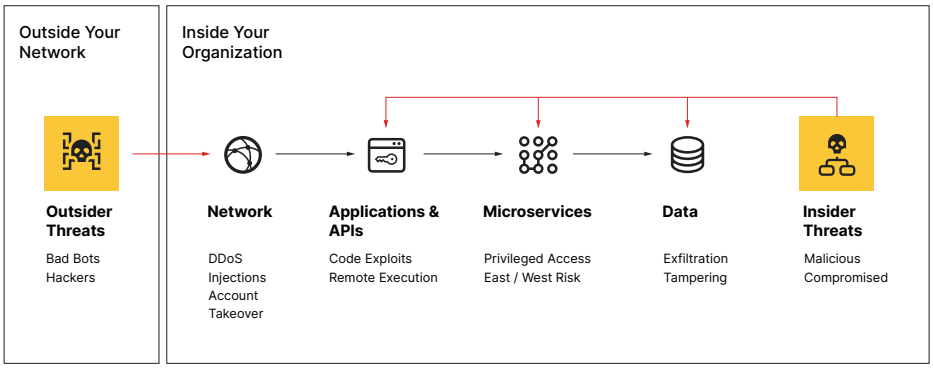
Protecting data and all paths to it is the defining challenge for the Digital Age. The business value of leveraging data to gain efficiency and generate revenue was established long before most people thought about how to secure it, but now enterprise data security must close the gap. In 2019, attackers exfiltrated 11.3 billion sensitive records from data sources worldwide, resulting in billions of dollars in losses. Modern requirements for securing data have grown beyond most enterprises' capacity to meet them. Enterprises struggle to discover and identify malicious data access internally and externally. Applications and APIs have become the largest targets for accessing sensitive data. This is an existential problem for all enterprises and must be addressed.

This paper will explain where the threats are on the paths to your data. We'll also discuss the acceleration of digital transformation and the ways in which this phenomenon has upended how data security works and created immediate challenges for enterprises. We'll explain where in your architecture you need to apply new, more effective security controls, focusing primarily on data security. And we'll give you a glimpse into a future that offers an edge-to-end data security solution that protects your entire data estate.

In 2019, attackers exfiltrated **11.3 billion sensitive records** from data sources worldwide, resulting in billions of dollars in losses.

Paths to your data and how to protect them

Businesses are interconnected like never before. When you provide sensitive data to one enterprise it means dozens of other enterprises likely have access to it as well. If those other enterprises are not committed to protecting your data, your sensitive information has a far greater chance of exposure. In addition, as businesses give consumers who work with them greater access to company data, the potential for exposure grows even more.



Enterprises need to shift from siloed thinking and develop a model that looks holistically across the entire stack and outlines all paths to their data.

Multi-layered paths require multi-layered protection to make applications, websites, and data always available and always secure. You need a solution that allows legitimate traffic through and keeps bad traffic out. You need to ensure bad actors cannot block access to your website and network infrastructure. When there are security threats, you need the tools to respond quickly and decisively to stop them.

You must have a solution that enables you to detect and react to dangerous user activity that puts your business at risk, **wherever the data lives.** Simply meeting compliance regulations does not provide real security for your data.

How digital transformation has upended the way data security works

Digital transformation has ushered in an explosion of new databases in new locations and enterprises are rapidly moving from monitoring all workloads and data on a few choice on-premises databases to monitoring and securing up to ten times that number both on-premises and in the cloud. The proliferation of the cloud-based services has made our data environments exponentially more complex. A 2020 report claims 59 percent of enterprises expect cloud usage to exceed prior plans due to COVID-19 and as many as 93% of enterprises are running on a multi-cloud strategy[1]. The task of securing this data has grown in parallel.

Today, data security has grown far beyond monitoring and is now a part of every critical business decision. The business value of moving workloads to the cloud was established long before most people thought about how to secure the data, but now they must. Securing data in the cloud is a rapidly changing target. In the past, on-premise databases could be used for a few years. In the cloud, they can be built and taken down in a matter of a few weeks. The tools companies use on-premise are not suitable for securing data in the cloud. The explosion of data, and security teams' inability to extract actionable information from it, has caused security operations teams to suffer from alert fatigue and struggle to respond quickly to security threats. Security teams today must have the tools to discover and identify suspicious data access internally and externally, both intentional and unintentional such as malicious threats from compromised users, misconfigurations and bad passwords so they can protect enterprises across a fragmented technology ecosystem and through all stages of their digital transformation. They must have a solution that enables them to focus only on securing data that matters.

Security teams today **must have the tools to discover and identify malicious data access internally and externally** and protect enterprises across a fragmented technology ecosystem and through all stages of their digital transformation.

Securing application and data migrations to the cloud is a rapidly changing target

SOCs are suffering from alert fatigue and struggling to respond quickly

The fragmented technology ecosystem is complex for enterprises to secure

Security is now a part of every critical business decision

[1] Cloud Computing Trends: 2020 State of the Cloud Report

What an “Edge-to-End” posture brings to a modern enterprise

Gartner asserts one of the principal challenges to protecting data is no single entity can implement the required data security governance controls across an entire enterprise. This is due in large part to the reality that their various security, privacy and identity access management products do not share policies or integrate. An Edge-to-End approach to data security will enable the enterprise to secure all workloads and data anywhere it lives. It will be possible to prevent security events by identifying, discovering and then classifying data across the enterprise and detect anomalies by mapping and monitoring all data access privileges. It will be possible to respond to events by monitoring and reporting any inconsistencies or unusual changes and predict future events using a data risk assessment to identify gaps or inconsistencies in policies. At that point, your approach will be holistically top down, delivering a strategy that addresses key business priorities and governance requirements. Enterprises will need to deploy this strategy universally across three main areas of enterprise cybersecurity:

An Edge-to-End approach to data security will **enable the enterprise to secure all workloads and data anywhere it lives.**

EDGE SECURITY

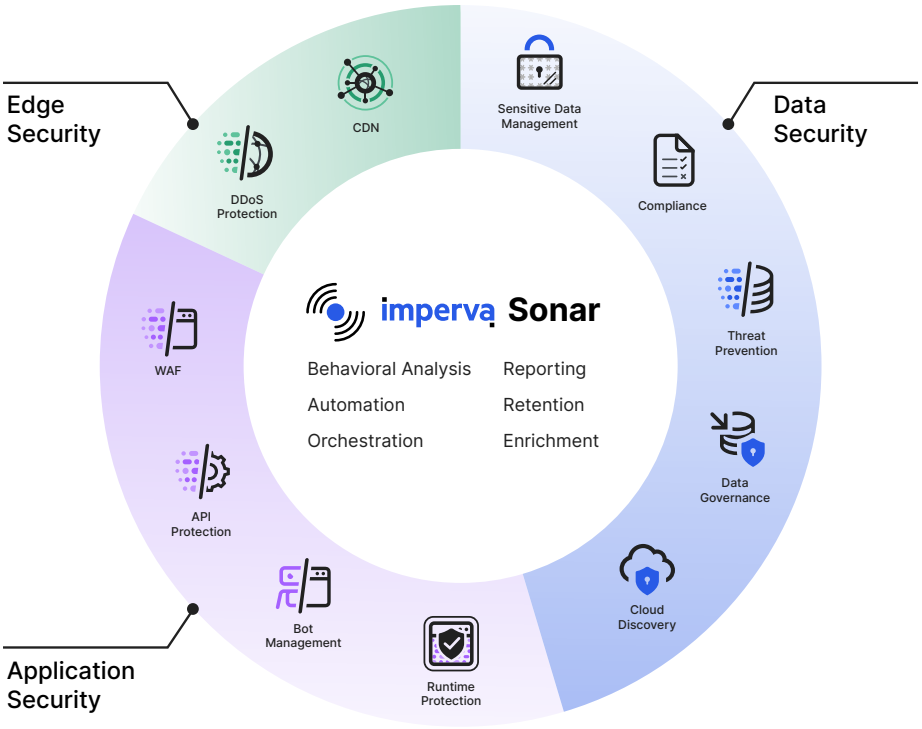
The solution will protect the enterprise’s websites, mobile applications, and APIs from automated attacks without affecting the flow of business-critical traffic. It must also defend against DDoS injections and account takeovers outside the network core.

APPLICATION SECURITY

The solution will provide your business applications with full-function defense-in-depth. This means best-in-class web application firewalls (WAFs), bot management and runtime and API protection.

DATA SECURITY

The solution will automate the extension of an enterprise’s security controls to several years’ of retained data to ensure continued compliance reporting and governance for all data sources. The solution will enable the efficient discovery and tagging of sensitive data as well as the ability to enrich and correlate the data to provide accurate behavioral analysis for threat prevention and mitigation.



Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.

Conclusion: out of many, one

You may know that *e. pluribus unum*, Latin for *out of many, one*, is the motto of the United States. Today, it may well be the motto for creating an effective holistic approach to ensuring cybersecurity in any enterprise. The only way for a security apparatus to shake loose from a siloed approach to cybersecurity is to commit to a top-down strategy and look for solutions that address the full stack of challenge areas.

Imperva enables enterprises to secure all data, anywhere it lives. More than 6,200 enterprise customers use Imperva data security technology to protect their data from cyber attacks through all stages of their digital transformation. Find out what Imperva can do for your enterprise at www.imperva.com.

Copyright © 2021 Imperva. All rights reserved
imperva.com
+1.866.926.4678