The Art of Data Privacy & Protection—

Less risk, more data privacy

Today, every company is a data company—

Each one of us creates 1.7 megabytes of data every second, and 90% of the world's data was created in the last 2 years alone.

With this data explosion and the IoT revolution showing no sign of slowing down, organizations are finding themselves armed with more data - structured and unstructured -than ever before.

This data explosion has introduced a new challenge for enterprises' IT. **Managing this data is an insurmountable task for many internal teams, leading organizations to rapidly adopt cloud services.** Leveraging cloud allows enterprises to benefit from infinite scale, improvements in responsiveness and agility, better consumption-based pricing, and a wider range of capabilities.

Infrastructure as a Service (IaaS) is especially useful for business services and applications such as high-performance computing and big data analytics.

However, migrating sensitive and regulated data into the cloud has the potential to increase the risk and number of data breaches. This is because of a lack of awareness of cloud security policies, cloud security controls that are difficult to understand for security teams, and misconfiguration, which is the number one cause of data breaches in the cloud. But not all data is in the cloud, with many organizations adopting a hybrid model. **Legacy systems may be modernized in order to avoid performance deficiencies and enable digital transformation.**

Furthermore, **the pressure of security frameworks is increasing,** with the introduction of data privacy regulations such as GDPR, CCPA, and PIPEDA adding to an already confusing and vast regulatory landscape.

When used appropriately, your customer's data can provide valuable insights and give you the ability to rapidly and consistently tailor and innovate your product and service offerings. And with businesses increasingly looking at how the data they have can be monetized, there is potential to create new revenue streams through a variety of analytical activities, new data-driven products and services, internal cost optimization, sales funnel optimization, and various other processes.

Whether an organization produces data, aggregates it, or simply consumes it, they can realise the value of data monetization.

For customers and enterprises to get the most value out of their data, **organizations must design an end-to-end framework to deliver insight and control, data protection, and usability,** across the entire data lifecycle, from discovery to disposal.

This framework should be flexible enough to preserve brand value and boost customer trust, ensuring that the data is leveraged to help grow the business. This means that data will be protected wherever it resides and however it is used.

Acceleration to the Cloud—

Enterprises simply don't have the processing power to cleanse, store, and manage the huge amount of data that they now hold, or to provide services such as data lakes, processing, and analytics that are provided on demand in the cloud.

This has led to a rapid increase in cloud adoption. Leveraging cloud services means greater business agility at a lower cost, improved analytics, and collaboration within the workforce, which drives productivity. However, **legacy security controls that are embedded within existing IT infrastructure are proving increasingly ineffective as data has become more pervasive, mobile, and cross-functional.** With most organizations now using multiple cloud providers, protecting sensitive data across hybrid IT is increasingly challenging.

The increase in scope and scale of data breaches and the complex landscape of privacy regulations has meant that more effective solutions are required to protect data on-premises, in cloud infrastructure and applications, and in analytics platforms.

Cloud service providers are not responsible or liable for the security of the data that customers ingest into their services. Enterprises need to develop a strategy for cloud data security early in their cloud migration journey. They should implement data-centric security, preferably prior to the sensitive data being migrated to the cloud.

Acceleration to the Cloud—

There are three major focus areas for enterprises migrating to the cloud:

Secure Data Analytics

When integrating and migrating data to a cloud service, or multiple cloud services, organizations must be able to unite separate analytics functions, whether they're on-premises or cloud-native, and continually perform secure analytics on their consumer data without violating privacy protections.

Cloud Data Security

As data is being moved into the cloud, it should be secure across the entire lifecycle, at rest, and while in use. Consistent data protection results in cost and competitive efficiencies and protects the data that matters most.

Secure Information Sharing

Being able to easily share information like intellectual property, business plans, customer data, or financial records, is key to an organization's success. Without a secure collaboration system, sensitive data can be lost or leaked, resulting in fines, lawsuits, and reputational damage

2020

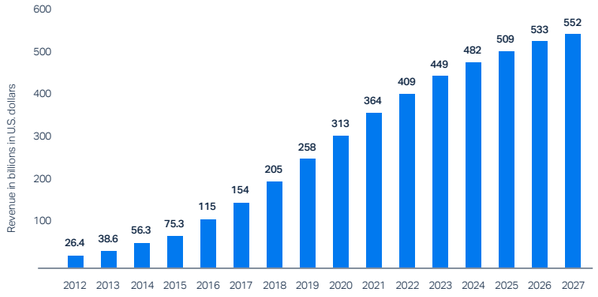
$313bn

2025

$509bn

▲ Public cloud services market growth prediction

Public cloud market revenue worldwide 2012-2027



©Statista 2020

How we help

We provide data-centric technology and analytics-preserving encryption which keeps data secure at all times, regardless of where it is stored, when it is used, or migrated to the cloud. Our data privacy protection framework enables analytics in the cloud, allowing users to drive insights and business value, as well as accelerating regulatory compliance.

Big data deployments can be shifted from on-premise to the cloud, with encrypted files agnostic to the system, applications, and user. Voltage customers benefit from reduced data breaches and insider attacks, secure files across collaboration platforms, and total control over sensitive files across the data lifecycle.

Management in the cloud and on-premise ▾

> **"Our clients want to lock down their sensitive data, but still be able to unlock the value in that data at scale."**
>
> HEAD OF CYBERSECURITY PRACTICE
> Global Systems Integrator

Stories and Solutions

The Problem

This large insurance and financial services firm were looking to modernize and move more of their data into the cloud in a way that would utilise the cloud's unique capabilities. The company moved a lot of Personally Identifiable Information (PII) through internal and external systems, however their internal systems were integrated with 3rd-party brokers and additional external systems, opening up PII to an increased risk of breaches. Additionally, an NYDFS audit outlined a series of data privacy regulations that the company was required to meet. Sensitive data held in on-premises legacy systems was also critical to analytics objectives, and presented a further challenge to their cloud migration plans.

How Did We Add Value?

Demonstrating Voltage encryption as a feature inside the cloud-based Vertica analytics platform provided the needed cutting-edge solution and tight integration the firm was seeking. No alternative solution could provide this level of built-in data privacy and protection.

The solution

The existing on-premises enterprise data warehouse (EDW) was modernized to Vertica + Voltage Inside with Voltage Format-Preserving Encryption (FPE) protecting personal data in use for big data analytics. Because sensitive customer data can be analyzed in its protected form, more users can safely be provided access to the data for business intelligence and analytics use cases to drive business value. Voltage then further assisted the IT team with planning expansions to encrypt any data in internal systems which was frequently accessed by 3rd parties, using a Center of Excellence (CoE) strategy to deploy Voltage across their systems and applications.

The outcome

The company's PII data for use in analytics is now encrypted at the source, allowing 3rd-party systems to access protected data without risking non-compliance with privacy regulations. Through strong collaboration by Voltage with the CISO and technical architects, this major insurance and financial services enterprise benefits from the secure use, movement, and analysis of high value, sensitive, and regulated data in the cloud without risk of a data breach.

Regulatory Pressures—

Regulatory frameworks are one of the most important considerations when dealing with your customers' data.

However, this has to be done in the context of a tightening and confusing regulatory landscape; 10% of US companies are actively working to comply with 50 or more privacy laws.

However, 75% of organizations believe that GDPR has a beneficial impact on consumer trust, and 97% recognized that they were realizing benefits such as competitive advantage and investor appeal from their privacy investments.

With so many regulations to consider, **enterprises are challenged with understanding which frameworks apply to them and implementing the correct data protection policies to achieve compliance.** The financial penalties of non-compliance are strict, and the associated reputational damage can deter new and existing customers and clients.

Regulatory Pressures—

There are three key use cases within regulatory pressures that enterprises are looking to address:

Data Privacy Readiness

To ensure that they meet the requirements of data privacy mandates, enterprises need to first discover, classify, and analyze data based on a contextual understanding of the data elements and document content, enabling further actions such as protection, retention, and disposal.

Test Data Management

Due to data privacy laws, organizations can no longer use real production data for testing, development, quality assurance, or education. It's therefore vital to have effective tools to generate anonymized and protected data that will deliver the required outcomes.

PII/Personal Data Encryption

Technology has a key role in data privacy compliance. After conducting a Personal Data Assessment to understand readiness and risk exposure, organizations should apply technology which has been mapped to their risk scenarios, quickly and cost-effectively encrypting data to enable its secure use.

Regulations to take into account

California's recently enacted **CCPA**
India's **Personal Data Protection bill of 2018**
Brazil's **General Data Privacy Law 2018**
Turkey's **KVKK**
Thailand's **PDPA**
Canada's **PIPEDA**
and Australia's **Notifiable Data Breaches Act 2017**

That's not to mention industry-specific regulations such as **HIPAA for US Healthcare Providers**

How we Help

Organizations must design a unified framework to deliver insight and control where they need it most, across the entire data lifecycle from data discovery to disposal. Micro Focus enables the discovery of sensitive data across hybrid IT and multi-cloud ecosystems, implementing a single framework for regulatory compliance. We ensure that data is properly managed and protected, both on premise and in the cloud, leveraging AI-driven data analytics to understand the context of data.

Our framework elevates the management of test data by automating the extraction, encryption, and archiving of test data as needed, accelerating the understanding of production data issues in development. Our customers are able to work toward IT modernization and cloud migration by protecting data wherever it travels, establishing data-centric cyber resilience.

"Structured Data Manager has made our operations much more streamlined. We eliminated unnecessary and burdensome processes, improving our workload as well as our overall performance."

IT GENERAL MANAGER
Distribution and Logistics Company

Stories and Solutions

The Problem

This leading integrated distribution and logistics company needed to streamline its data in order to improve enterprise resource planning and their customer, order, and inventory information. The client required a complex approach due to its size and large number of users. The unmanaged growth of the company had put a huge burden on the already-stretched IT team, who were challenged with 18 terabytes of data that was growing at 300-400 gigabytes per month.

How Did We Add Value?

The client could not find a solution that covered all their regulations in a single product. After they identified that Micro Focus Voltage had the integrated solution to meet their various needs, we made sure to demonstrate that we understood their unique challenges and regulations, showing them the value of proactively managing growing data.

The Solution

By implementing Micro Focus Structured Data Manager, the organization was able to identify, organize and streamline the data created by more than 5000 employees across 46 branch offices and 200,000 corporate customers. We provided a flexible, configurable interface for setting up data retention policies, making processes transparent and optimizing data management. This ultimately gave their IT teams visibility and control, making archiving, replicating, and restoring data manageable.

The Outcome

Our solution reduced the size of the database by several terabytes, allowing for backups to be done in a single day. We gained control of batch processing performance, making the backup, cloning, and replication processes require just a fraction of the time and manpower taken before. By using our faster and smarter data management for 9 years and counting, the organization has increased efficiency, cut costs, and saved valuable time.

86% of enterprises use IT products that are over 10 years old.

These **legacy systems are often unable to keep up with data storage capacity requirements, resulting in application performance deficiencies** and increased downtime.

Additionally, the often-inadequate data security of legacy systems makes complying with the relevant regulatory frameworks near impossible.

Enterprises must modernize their IT in order to avoid non-compliance fines and severe reputational damage, and to enable digital transformation.

IT Modernization—

IT Modernization—

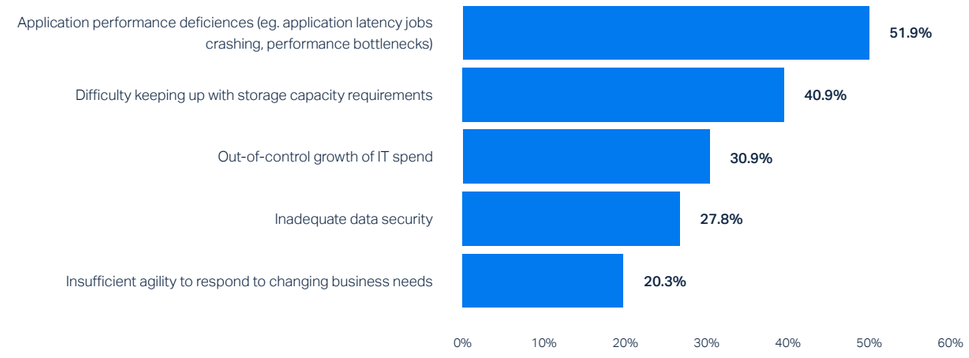
There are three key areas of consideration within IT modernization that relate to data privacy and protection:

Data Minimization
Enterprises face higher risk, increased compliance obligations, and higher IT costs by holding on to redundant, outdated data. A deep insight and knowledge of their information is needed to minimize their data to support compliance, decrease storage costs, mitigate risk, and increase IT efficiency.

Application Retirement
Retiring legacy applications is a key goal of IT modernization. However, the cost and risk of managing and retiring application data is a growing concern for many organizations, especially when complying with stringent data protection frameworks and leveraging IT modernization projects.

B2C Payment Security
In today's strict regulatory environment, it is critical to protect payment data anywhere it moves, or resides, and however it is used. Payment data should be secured at all points of the purchasing process, in storage and in use in applications.

Critical challenges resulting from exponential data growth in organizations worldwide as of 2019



www.statista.com/statistics/1010737/worldwide-data-exponential-growth-challenges

How we Help

To keep pace with IT modernization initiatives, organizations need to quickly determine what data needs to be kept, what data holds value, and what data does not. Saving revenue on storage and license renewals, our solution reduces corporate risk by identifying information to be retained, deleted, or acted upon. With Micro Focus Voltage, businesses can reduce the cost of ownership of application infrastructure, increase business productivity, mitigate heightened compliance risks, and automate the secure migration or retirement of data.

Our framework reduces the risk of data breach and liability exposure while complying with the Payment Card Industry Data Security Standard (PCI DSS and PCI P2PE) and data privacy laws. We give you control over end-to-end payment security, independent of the payment or service provider solution, boosting consumer trust and brand value.

> **"The archiving of obsolete data reduced the footprints of our application environments in some cases by as much as 50%. This resulted in an increase in application performance – and of course a reduction in capital expenditures – on processing and storage infrastructure."**
>
> **SENIOR DEVOPS ENGINEER**
> **Automotive Finance Company**

Stories and Solutions

The Problem

This large financial business unit had never implemented an archiving or data management strategy, and the security team were under pressure from increasing regulations, risk, and growing costs. They were deeply entrenched with a separate system for data management, with a lack of experience in data lifecycle management holding them back. The organization had a huge risk footprint due to the amount of legacy data being stored and had not deleted or archived financial data since their inception in the late 70s.

How Did We Add Value?

Having no previous relationship with the client, we placed emphasis on the legal aspect of the problem. We identified that what mattered most to the legal team was the reduction of risk and volume of data, and the organization of the data. By focusing our discussions on this and the importance of data management for audits and litigation, as well as ensuring that we offered more than their existing data management system, we were able to get buy-in from the legal team.

The Solution

We identified the goals of the different stakeholders in the organization and presented a strategy that brought legal and IT together through our experience in archiving, governance, and data lifecycle management. We determined business unit requirements for data retention, applied retention to structured records, extracted and migrated records to a secure repository, and put in place an enterprise-wide electronic archival solution.

The Outcome

By establishing enterprise data lifecycle management practices across the region, we were able to meet both legal and IT needs. This reduced the organization's data footprint by as much as 50%, building the foundation to support data privacy regulations such as the CCPA. So far, we have archived and purged more than 8.2 million structured records and data from more than 1,000 database tables, establishing a strong data management and governance approach that reduces risk, streamlines processes, and delivers financial benefits and return back to the business.

The Art of Data Privacy and Protection—

Protecting data through the entire lifecycle is a precise art form, with experienced 'security artists' understanding the need for expert support and the right tools and processes.

At the center of any great art you find people, and it is the same with data protection. These people are staff, partners and customers; the ones buying the products, making the business more productive, and helping to drive competitive differentiation. It is these "data subjects" whose personal information must be protected.

Artists understand the skill of editing their work. Data security experts must know how to edit the exponential amount of data they collect. They should understand complex data privacy regulations and delete all data that isn't needed in order to comply.

Any great work of art goes through multiple revisions. So, too, data must be managed and secured through its entire lifecycle to maximize business value, preserve data integrity, meet regulatory requirements, and reduce risk. For too long the approach taken by many organizations has been siloed and incomplete, exposing them to reputational and financial risk.

As artists do, security professionals need to master the right tools, technologies, and processes for the job. As with any art form, the first step is to choose a subject and composition—that is, to establish the right framework for your business.

> **"Voltage is the one-stop shop for all our data security use cases. It complies with all current data privacy regulations, integrates superbly into our environment, and has matured our data protection approach and processes."**
>
> SENIOR PROGRAM MANAGING ARCHITECT
> Leading business processing organization

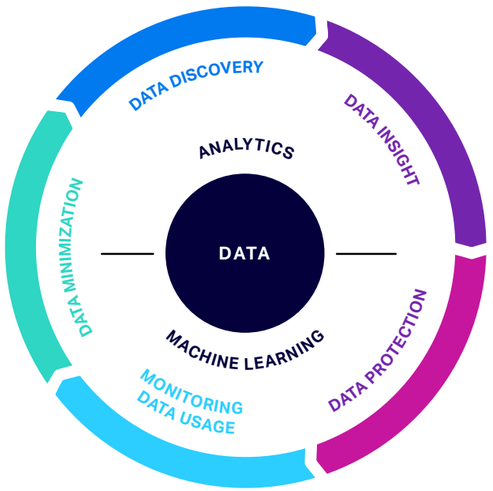
The Art of Data Privacy and Protection—

Many data protection offerings are little more than point solutions that offer neither the scope, vision, nor cross-silo analytics needed to address company-wide challenges of cloud adoption, IT modernization, and regulatory pressure.

Organisations must implement a unified framework to deliver insight and control where they need it most, and across the entire data lifecycle.

Micro Focus data protection allows you to manage your structured and unstructured data throughout its lifecycle by supporting your data privacy and protection through our proactive cyber resilience framework, evolving with you as your business changes and grows.

The Voltage data privacy and protection framework enhances your intelligence and cyber resilience, protecting against advanced threats at scale. By identifying, tracing, and learning from cyber threats, we empower businesses to oversee and secure structured and unstructured data, building a resilient culture that grows with the enterprise.



The Voltage data privacy and protection framework ▲

Our data privacy and protection framework allows you to:

Discover

We discover sensitive data across 39+ countries, analyzing and remediating data in-place without moving before taking action on this data. We utilize AI in our context-aware discovery process, maximizing the depth and breath of PII detection.

Insight

Our context-aware analysis, underpinned by AI, significantly reduces false positives and increases efficiency. Visualisation and rich analytics help to show organizations the potential value their data has, to then apply various data lifecycle policies based on content, age, relevancy and risk.

Protect

Our patented, format-preserving encryption protects structured data in place, eliminating the need to quarantine data, enabling data security in use and in motion. We automate the tagging and protection of sensitive data based on risk and context, ensuring that sensitive data is protected from unauthorized access and that information sharing is secure when files are open within an enterprise.

Monitor

We prioritize accuracy and speed when discovering files and their associated permissions, identifying security vulnerabilities to remediate and ensuring only authorized access to application data. As well as our flexible policy enforcement, we offer near real-time insight into data usage and operations across your entire network, making the enforcement of these policies easier.

Minimize

By minimizing data and managing the entire lifecycle, businesses can make faster, informed decisions around data disposition, identifying redundant, trivial data to take action on and monitoring and auditing all actions in the process.

With this framework, customers have the springboard they need to drive innovation-fuelled growth. We understand that this is a continual process because data – and its associated risks – changes over its lifecycle, which is why we strive to assist organizations during every step of the data journey.

How data privacy and protection improves cyber resilience

Cyber resilience is the ability of an organization to enable business acceleration by preparing for, responding to, and recovering from cyber threats.

A cyber-resilient organization is able to easily adapt to threats, adversities, and challenges, whether they're known or unknown.

An effective cyber resiliency strategy will incorporate multiple components, including:

- **Artificial intelligence and machine learning**
- **Data security**
- **Application security**
- **Identity and access management**
- **Security operations**

A comprehensive cyber resilience strategy requires the integration of data privacy and protection throughout the entire lifecycle.

This way, organizations can protect their business, detect changes in the risk landscape, and evolve their capabilities. Analyzing existing data, both structured and unstructured, gives businesses valuable insights that help with achieving regulatory compliance and therefore cyber resiliency.

For more information visit – **https://www.microfocus.com/en-us/cyberresilient**

Data as Art—

We're a world consumed by data. This data informs and controls us every single day, but we rarely see it. If we replace the numbers with dots, lines and shapes, but retain the complexity and connectivity, we can represent this vast language in engaging visual ways. Data is the paint on our canvas, the ink on our pages, and the pixels on our screens.

Contact us at **www.microfocus.com.**

About Micro Focus

Micro Focus develop integrated cybersecurity solutions to enhance data intelligence and cyber resilience, protecting against cyber threats at scale. Our solutions enable customers to oversee and secure structured and unstructured data, managing identities and access throughout the organization. We empower businesses by using AI and connected insights to structure a resilient culture and to adapt to changing needs.