Achieving Consistent Data Security across Hybrid IT

Read it ›

Hybrid IT is the new IT

The digital infrastructure that enterprises have known for decades is changing—radically.

Today’s business challenges pressure enterprises to be agile and flexible, to service customers in new markets faster, and to host workloads based on regulatory and geopolitical considerations. These factors are compelling enterprises to adopt the cloud across their entire business. 90% of apps and workloads that companies rely on are scheduled to be deployed to the public cloud, with the only exception of big data workloads, at 60%. But this does not mean the private data center is dead. In fact, 55% of corporations expect their use of private cloud to increase in the next two years. And no one expects mainframes to vanish anytime soon.

⌂ < >

90% of all apps and workloads are scheduled to be deployed to the public cloud[1]

55% of organizations see their use of private cloud increasing over the next two years[2]

The Transition to the Cloud is Changing How Companies Operate

A survey by the Ponemon institute has found that, on average, today's enterprises use 27 different *Software-as-a-Service* (SaaS), *Infrastructure-as-a-Service* (IaaS), or *Platform-as-a-Service* (PaaS) solutions to run their business. This includes essential business infrastructure solutions such as Microsoft Dynamics 365, Amazon Web Services, and Salesforce.

Enterprises are leveraging this infrastructure to deploy a majority of their custom applications to the cloud. The Cloud Security Alliance estimates that enterprises have an average of 464 custom applications, and over 50% of those are planned to be deployed to the public cloud by the end of 2018.

Enterprises use an average of **27** SaaS, PaaS, IaaS apps and services[3]

Enterprises have a majority of their **464** custom applications deployed to the cloud[4]

Cloud is the #1 target

for security spend increase by Chief Security Officers[5]

Shared technology

Data loss

Advanced persistent threats (APTs)

Insecure APIs

Denial of service (DoS)

System vulnerabilities

Insufficient identity, credential, and access management

Account hijacking

Data breaches

Malicious insiders

Abuse

Insufficient due diligence

But Security of the Cloud is the Number One Concern for Chief Security Officers

So it does not come as a surprise that a survey by CSO magazine pointed out that the cloud is the number one target for security spend increase by Chief Security Officers. The top threats in the cloud are very similar to the threats faced by an on-premises infrastructure. But it is the very nature of cloud services themselves that keep CSOs awake at night. The dissolution of the perimeter creates challenges that traditional system and perimeter IT security cannot cope with, leaving the modern hybrid enterprise vulnerable to advanced attacks and malicious insiders.

Top Data Security Challenges in the Cloud

The top security challenges in the cloud boil down to a few key features unique to cloud services: the essential lack of control over a third-party platform that will host key data about your customers and your business; the fact that enterprises are dealing with shared multi-tenant platforms where malware could spread between tenants; and the fact that data has to travel between multiple cloud platforms and your on-premises infrastructure. And on top of that is the increased focus on consumer privacy and data residency by regulators, which raises the stakes for any data breach.

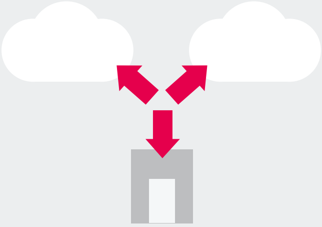
Platform Concerns

Lack of control over platform, and the need to rely on a third party for the privacy of your customers in the cloud.

Multi-tenancy

Malware could be introduced intentionally or unintentionally by one tenant and then spread to other tenants in the shared environment.

Gaps in Controls

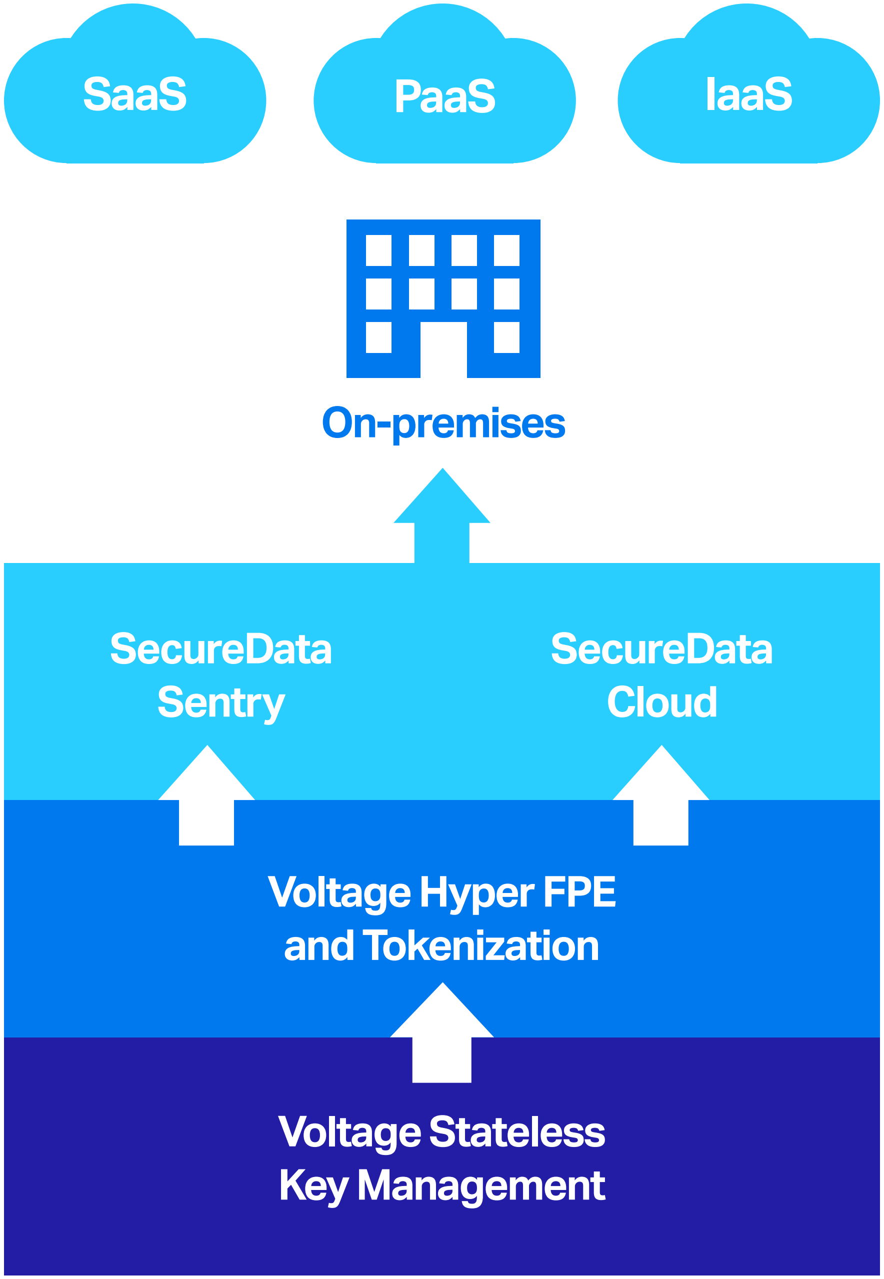


Data needs to be protected in transit between different clouds and between the cloud and your on-premises infrastructure.

Compliance Requirements

Stricter privacy and data residency legislation such as GDPR considerably raise penalties for data breaches.

Cloud customers need a data-centric approach for cloud data protection.


SaaS
PaaS
IaaS
On-premises
SecureData Sentry
SecureData Cloud
Voltage Hyper FPE and Tokenization
Voltage Stateless Key Management

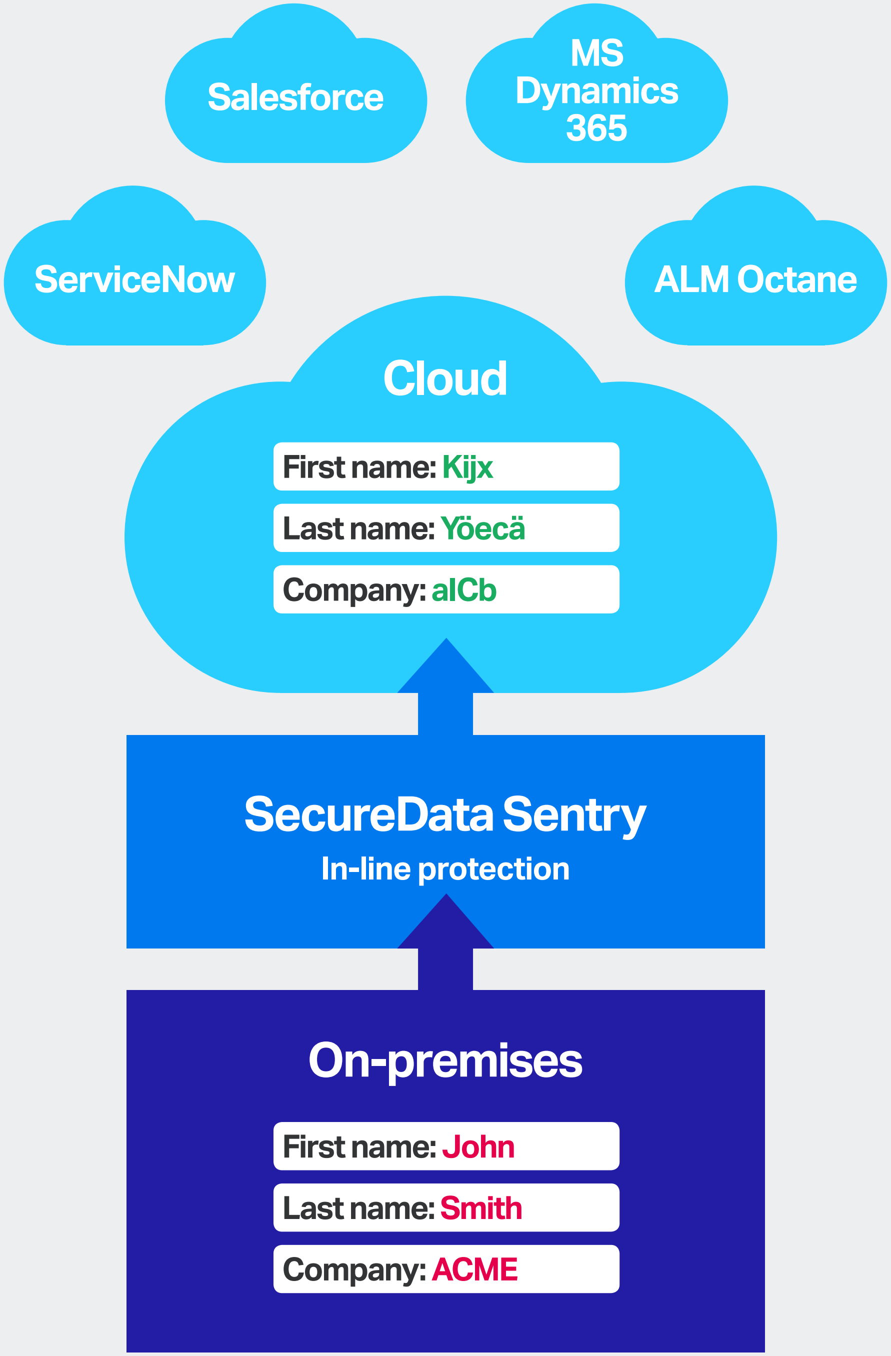
Voltage SecureData Provides Consistent Data Security across Hybrid IT

The sheer number of cloud services, the types of applications and usage, and the different security requirements and capabilities of different types of cloud require that enterprises adopt a flexible solution to secure data across hybrid IT. Voltage SecureData provides consistent data security across hybrid IT.

SecureData Sentry and SecureData Cloud provide flexible implementation options for enterprises to protect most third-party cloud platforms and customer workloads in the cloud. The underlying technologies, Voltage Hyper Format-Preserving Encryption (FPE) and Secure Stateless Tokenization, enable enterprises to embed security into the data, de-identifying sensitive personal information across cloud and on-premises systems. The breakthrough Stateless Key Management enables enterprises to maintain complete control over encryption keys while scaling to the needs of a global business.

Simplify Cloud Data Protection for XaaS with SecureData Sentry

SecureData Sentry simplifies cloud data protection for applications or services that can't be integrated with APIs—such as most SaaS applications. SecureData Sentry intercepts dataflows between on-premises databases and applications and cloud services. It applies protection to the sensitive data transparently, via proxy, intercepting data as it flows to the cloud. SecureData Sentry flexibility enables multiple cloud services to be protected, accelerating the time-to-value of your data-centric security investment.



Accelerate Your Transition to the Cloud with SecureData Cloud Platform-Agnostic Protection

SecureData Cloud offers a platform-agnostic approach to data protection, embedding data-centric security across hybrid IT and accelerating the speed of Dev Ops and the deployment of custom applications on hybrid systems. SecureData Cloud for AWS and SecureData Cloud for Azure provide a fully cloud-native solution where applications, data, and the security software appliance interoperate—on-premises or in the cloud—to enforce end-to-end data lifecycle protection. Voltage SecureData Cloud can support multi-cloud environments, hybrid cloud, and on-premises environments (such as z/OS, Linux, Windows, and Stratus VOS) through the Voltage SecureData product family.

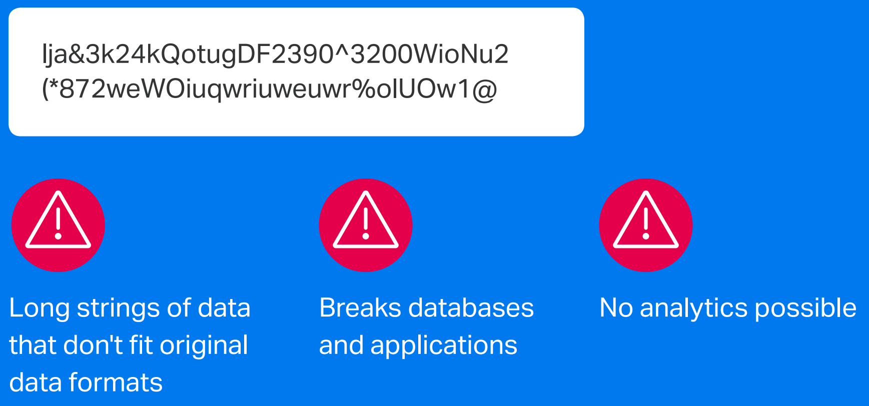
SecureData Cloud for AWS

SecureData Cloud for Azure

Use De-identified Data in the Cloud with Voltage Hyper Format-Preserving Encryption (FPE)

The underlying technology for Voltage SecureData with Hyper Format-Preserving Encryption (FPE) makes it easy and cost-effective for organizations to apply encryption. Hyper FPE enables businesses to de-identify sensitive personal data before uploading it to cloud platforms and applications. With Hyper FPE, even if a cloud platform experiences a security breach, the data is of no value to attackers because it is neutralized using encryption. However, because Hyper FPE maintains the format, meaning, logic, and context of the original data, the business can still use it for their business processes and analytics.

Traditional AES Encryption



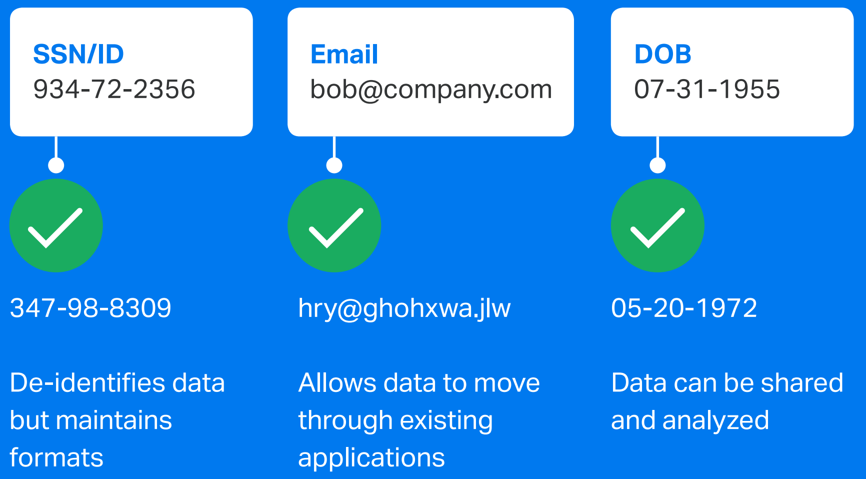
lja&3k24kQotugDF2390^3200WioNu2 (*872weWOiuqwriuweuwr%olUOw1@

Long strings of data that don't fit original data formats

Breaks databases and applications

No analytics possible

Hyper FPE Encryption



347-98-8309

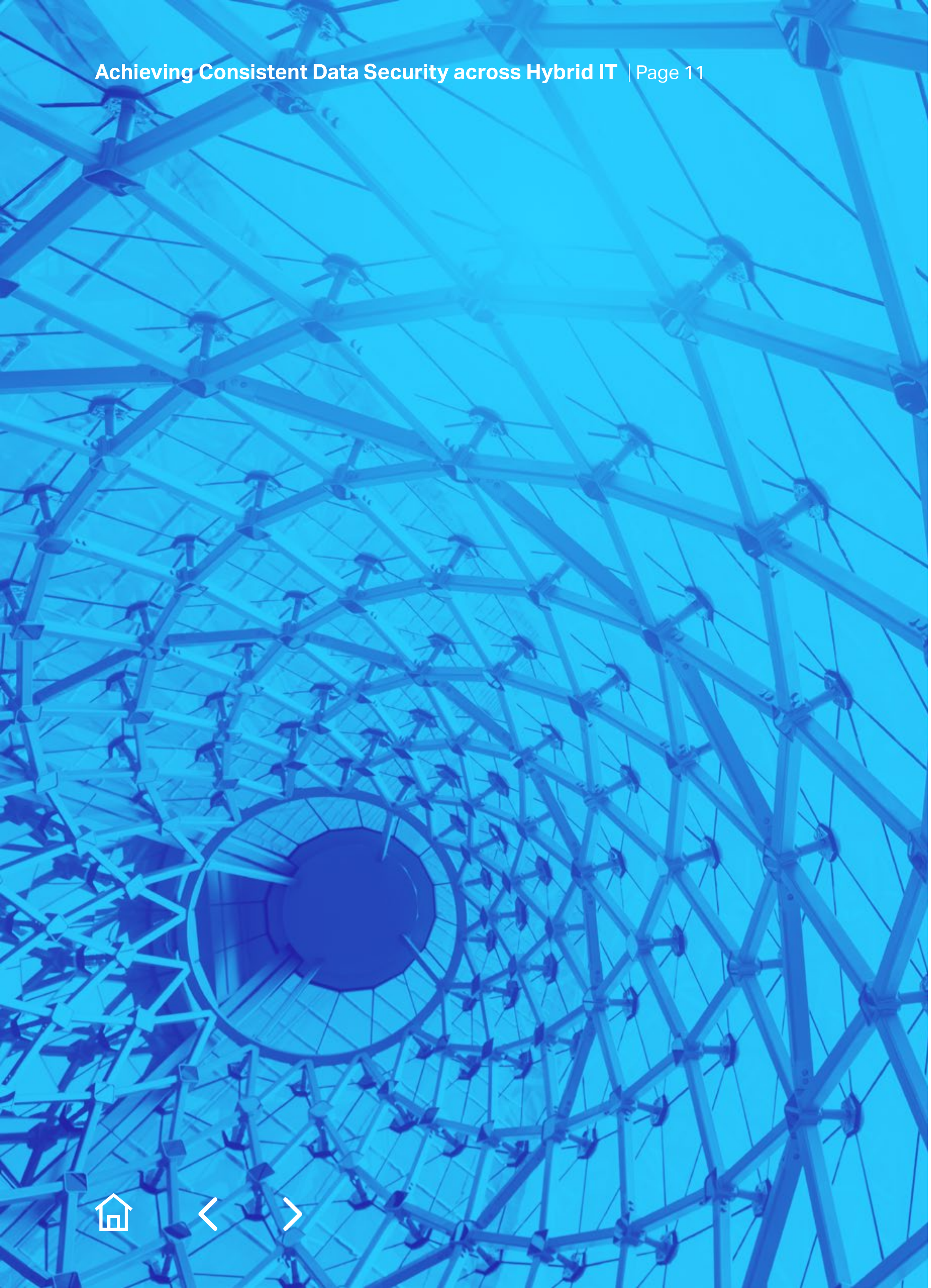
De-identifies data but maintains formats

hry@ghohxwa.jlw

Allows data to move through existing applications

05-20-1972

Data can be shared and analyzed



Scalability and Full Control over Encryption Keys with Voltage Stateless Key Management

Ultimately, the protection and usability of the encrypted data in the cloud relies on the ability of an enterprise to maintain control over encryption keys with a highly scalable key management solution. Voltage Stateless Key Management is the cornerstone of Voltage simplicity and scalability. Keys are derived dynamically as required by an application, with no key database to store, protect, and back up. Enterprises do not need to manually manage keys, certificates, or databases. This eliminates the hardware, software, and IT processes required to protect the database continuously or to back up keys from the site. Voltage Stateless Key Management enables low-cost, high-performance data protection that scales to protect the sensitive data of the largest financial services companies, telecoms, payment processors, and other global enterprises and government agencies.

Voltage SecureData: Consistent Data Security across Hybrid IT

By applying data-centric security, SecureData protects the data itself and addresses the main security challenges in the cloud. It mitigates the risk of cloud adoption across the spectrum of cloud services that enterprises operate, providing consistent data security for Hybrid IT.

Platform Agnostic

SecureData's platform-agnostic protection safeguards data on any PaaS, SaaS, or IaaS cloud service or application.

Neutralizes Threats

SecureData neutralizes data breaches and insider threats in a shared environment, making data unusable for attackers.

End-to-End Protection

End-to-end data-centric security technology embeds protection into the data and protects it across hybrid IT.

Easier Compliance

Encryption makes privacy compliance easier. If the data is breached, it will be de-identified and have no value to the attacker.

De-identified data provides end-to-end protection across hybrid environments, accelerating DevOps.

Use Case: Global Financial Services Company

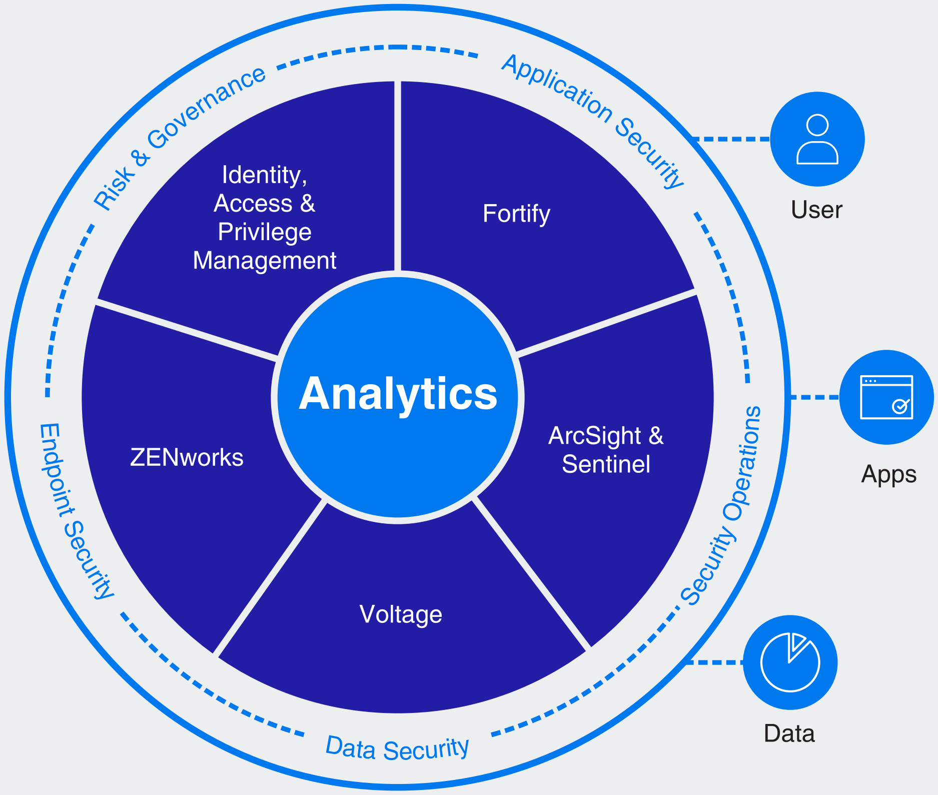
Business Need: A global financial services company was moving to a cloud-centric delivery of their business as SaaS and needed to protect data flowing into and residing in multiple clouds.

Challenge: The organization needed to protect data for over 100 million customers, with more than 40 different sensitive data types, and meet a third-party regulatory mandate for data security.

Their data resided in both Amazon Web Services (AWS) and Azure.

Solution and Business Outcomes: Voltage SecureData with Hyper FPE encrypted and tokenized all sensitive data in AWS and Azure, while maintaining on-premises policy enforcement, security operations, audit, and key management.

In a matter of weeks, they gained a unified architecture for streamlined compliance and risk control and met the requirements for third-party data protection mandates and audits.



At Micro Focus, we address our customers' biggest challenges across the full spectrum of hybrid IT.

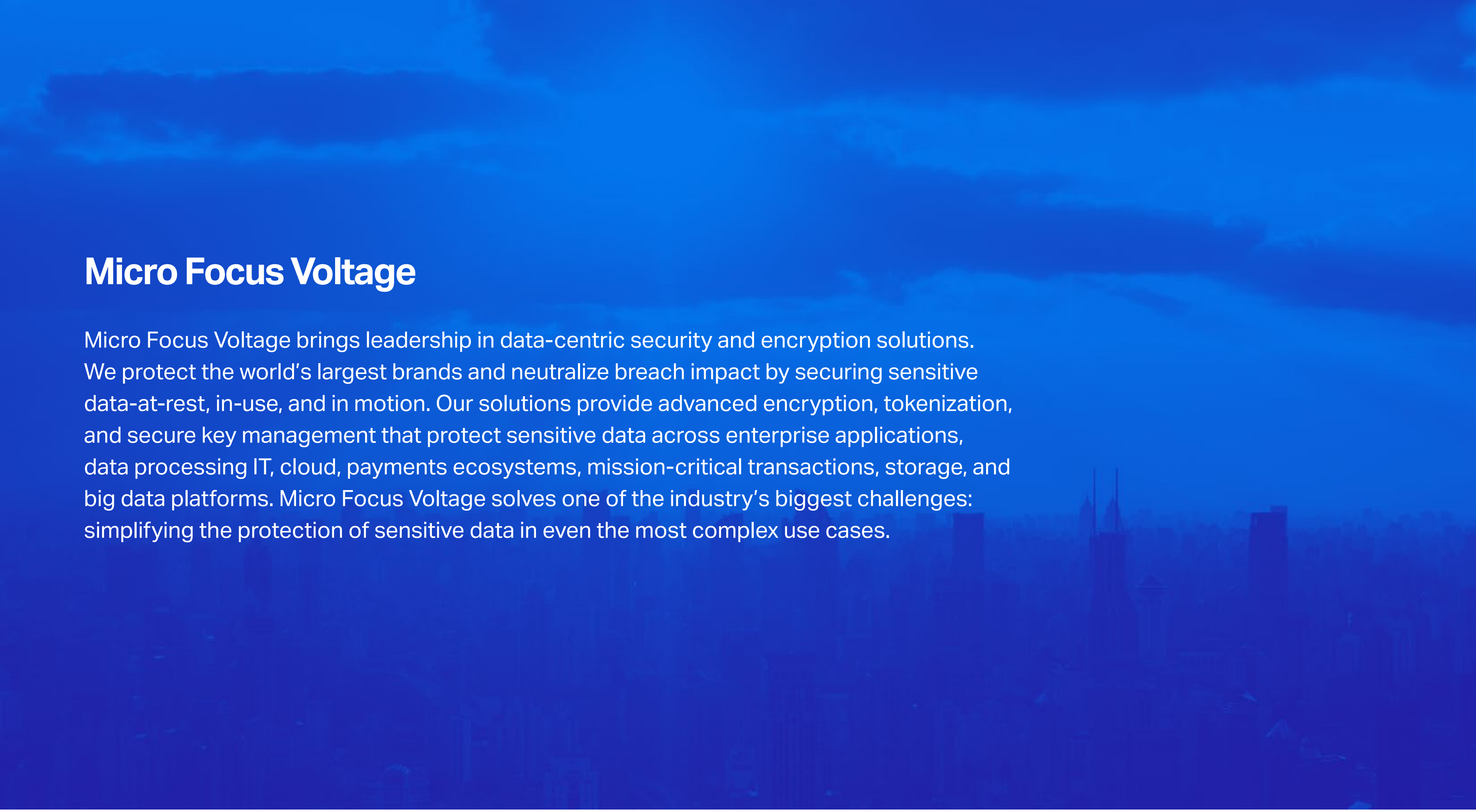
A transition to the cloud creates challenges that old security models can't simply address. Voltage SecureData is part of an industry-leading Micro Focus portfolio of security, risk and governance products and solutions. With Micro Focus, businesses can comprehensively manage and secure information; detect and respond to data breaches; and enforce identity and access controls; offering enterprises multi-layered information lifecycle protection across hybrid IT.

Learn more about how Micro Focus protects users, apps, and data—enabling companies to achieve a competitive edge.

For more information:

Cloud Data Security

Contact Us



Micro Focus Voltage

Micro Focus Voltage brings leadership in data-centric security and encryption solutions. We protect the world's largest brands and neutralize breach impact by securing sensitive data-at-rest, in-use, and in motion. Our solutions provide advanced encryption, tokenization, and secure key management that protect sensitive data across enterprise applications, data processing IT, cloud, payments ecosystems, mission-critical transactions, storage, and big data platforms. Micro Focus Voltage solves one of the industry's biggest challenges: simplifying the protection of sensitive data in even the most complex use cases.

Sources 1. Micro Focus Research, April 2018. Includes web & media, database, collaboration, infrastructure, business apps and Dev Ops, excludes big data workloads at 60%. 2. Market research by Micro Focus SUSE. 3. The 2018 Global Cloud Data Security Study, by Ponemon Institute LLC, 2018. 4. Custom Applications and IaaS Trends, Cloud Security Allliance, 2017. 5. 2017 Security Priorities, survey of Chief Security Officers, IDG, 2017

Warranty The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted rights legend Confidential computer software. Valid license from Micro Focus required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.