Big Data Protection with Data-Centric Security

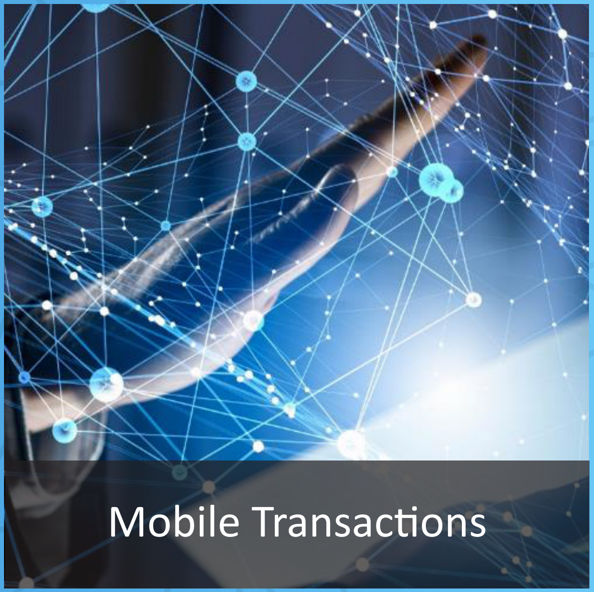
Protect privacy and unleash the power of data

Today we live in a different world of data everywhere…

The world is radically changing with data at the center of new value creation for businesses. Smart connected devices are everywhere — from connected cars, to all manner of IoT devices — including billions of mobile devices carrying sensitive data in the hands of users across the globe. All of these connected devices feed massive volumes of sensitive data into data lakes and warehouses, enabling enterprises to gather intelligent insights about customers, operations and competitors through analytics. Big data drives the modern enterprise, enabling the business user and data analysts to identify and understand data outliers, variations from baseline, interesting data clusters and more. But broadly enabling data access carries risks. How safe is your data in light of today's modern threat landscape?

Connected Cars

Smart Infrastructure



Mobile Transactions

… driving the modern enterprise

Sensitive data explosion – type and scale

A breach is the ultimate nightmare of corporate executives

Personal Data

Among the massive volumes of data captured by enterprises is sensitive information that, if stolen, results in harmful consequences to consumers affected and the business breached. In the age of big data, this risk exposure is exponentially more dangerous. With enterprises capturing personal information, intellectual property, health information, and more new classes of sensitive data than ever before, information in a data lake can form toxic combinations that reveal identity. Even data not apparently sensitive at face value could be combined with other disparate pieces of data to reveal personally identifiable information—and if stolen, be used for fraud and trigger penalties due to privacy legislation.

HEALTH DATA >

Insurance

- Claims
- Payments
- Coverage

Personal

- Tracking devices
- Activity records
- Genetic code

Patient

- Prescriptions
- Diagnosis
- Device logs
- Measurement

IDENTITY >

Demographic

- Age
- Sex
- Address
- Profession

Identifiers

- Name
- User-names
- e-Mail addresses
- Phone numbers
- Nick names
- SIM
- Device IDs
- IP addresses
- Bluetooth IDs
- SSID
- IMEI

Interests

- Shares
- Likes
- Favorites
- Preferences

Big data trends

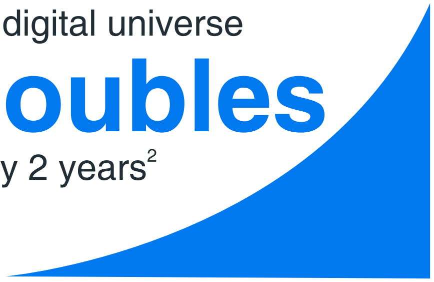
20B

Devices connected to the Internet by 2020[1]

The digital universe

Doubles

every 2 years[2]



The big data at the heart of the modern enterprise is growing massively each day. From the estimated 8.4 billion connected devices in use today, Gartner expects that we will reach 20 billion by 2020. Through these devices, leveraging new high speed networks, users are generating so much digital content that the entire digital universe is doubling every 2 years.

[1] "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", Gartner, Feb. 2017

[2] The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, IDC

Big data challenges

Big data is the

#1 target

for spend increase for Chief Security Officers[3]

1 in 2

Employees that request big data access are denied[4]

At the same time, big data is becoming a major priority for Chief Security Officers (CSOs). In a recent IDG survey, CSOs voted "Big Data" the number 1 target for increased security expenditures to prevent data breaches. But the increased security scrutiny is also having unintended consequences. Forrester reported that 1 of every 2 employees that request access to big data are denied for security reasons, hurting a company's ability to gain competitive insights from the data.

[3] 2017 Security Priorities, survey of Chief Security Officers, IDG, 2017

[4] Open Your Analytics Architecture To Keep Up With The Speed Of Business, Forrester and HPE, Aug. 2016

Across industries, organizations are leveraging big data to find opportunities for customer value creation

Financial Services

A global financial services firm imports massive data sets into data lakes from multiple sources for analysis to improve marketing to customers, find opportunities for monetization and improve fraud detection.

Manufacturing

A top car manufacturer collects sensor data from millions of connected cars—including GPS location—globally to identify defects and improve product offerings by analyzing vast data in real time, in a Hadoop data lake.

Telecommunications

A large European telecom provider created a data lake with a 180-node Hadoop cluster to analyze massive data sets, from millions of mobile subscribers in multiple countries, for insight into operations, performance, fraud detection and monetization opportunities.

Sensitive data and Hadoop insecurity constrain access to data lakes

Two common challenges keep enterprises from using big data to its full potential. The first is that among the petabytes of data collected into data lakes is highly sensitive personal information subject to GDPR and other privacy legislation. The second is that Hadoop is an inherently untrusted platform, highly distributed, with a rapidly changing open source community, and no way of deleting data. When combined, these 2 factors raise exposure risk and force enterprises to constrain access to data lakes to only a few trusted analysts.

Traditional IT security can’t protect big data

As data flows throughout the enterprise from the edge of the network where it is created, through thousands of applications and systems, all the way to storage in the cloud or on-premises systems, data must be protected, at-rest, in-motion and in-use. But traditional system and perimeter IT security can’t achieve this except for in silos, leaving security gaps in the modern hybrid enterprise.

Data has to be protected from the edge and in the cloud

Security Risk!

Traditional on-premise security controls can’t be extended to the hybrid cloud or protect data streaming from IoT devices

Data protection has to scale with Hadoop

Security Risk!

Traditional system-based security can’t scale at the speed of big data growth for most organizations

Data has to be protected during analytics

Security Risk!

Traditional data-storage security can’t protect data when it is being used by applications or being analyzed

Data has to be protected at 3rd parties

Security Risk!

Traditional embedded system security can’t properly protect data being shared outside the organization.

A new approach is needed that scales with the growth of big data!

Voltage SecureData – data-centric protection for big data

Protection for data everywhere it goes

✓

SecureData Cloud provides security in the cloud across Hybrid IT systems. NiFi integration enables IoT protection from the edge.

Protection that scales with Hadoop

✓

SecureData for Hadoop and IoT delivers protection that scales with the growth of Hadoop nodes, data volumes and data types.

Protection enabling data usability for analytics

✓

Data protected by Voltage Hyper FPE preserves usability for analytic insights and supporting business processes.

Protection for sharing data with 3rd parties

✓

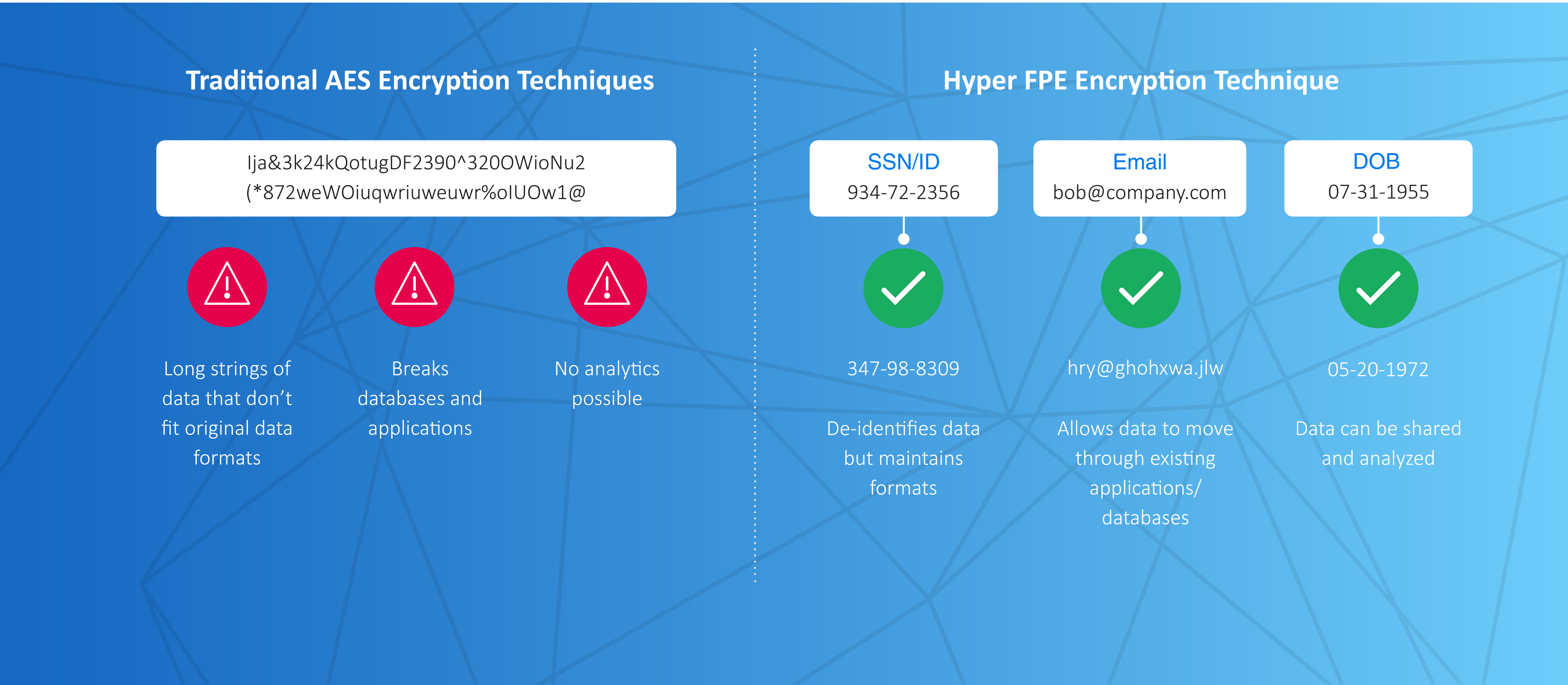
SecureData granular policy controls allow many users to access protected data and only a few to expose sensitive data, if required.

Voltage SecureData – embed security into the data itself

That means data is always protected, in motion, in-use or at-rest, and security policy travels with the data. What's more, Voltage Hyper Format Preserving Encryption, and Tokenization preserve the usability of data for analytics, applications, and business processes

Voltage Hyper FPE – protect privacy and unleash the power of data

Voltage 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 without extensively revamping existing IT infrastructure. It improves privacy protection and lowers the cost of achieving strong data protection. With Hyper FPE, even if an application or system experiences a security breach, the data is worthless to attackers because it's neutralized using encryption. However, because the substitute data types maintain the format, meaning, logic and context of the original data, analysts can use it to identify patterns, and run queries while encrypted. Hyper FPE also allows data to remain mobile so it can be moved between systems and around the globe while remaining protected, without breaking applications, database schema or business processes.



Traditional AES Encryption Techniques

Ija&3k24kQotugDF2390^320OWioNu2
(*872weWOiuqwriuweuwr%oIUOw1@

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

⚠ Breaks databases and applications

⚠ No analytics possible

Hyper FPE Encryption Technique

SSN/ID
934-72-2356

✓ 347-98-8309

De-identifies data but maintains formats

Email
bob@company.com

✓ hry@ghohxwa.jlw

Allows data to move through existing applications/ databases

DOB
07-31-1955

✓ 05-20-1972

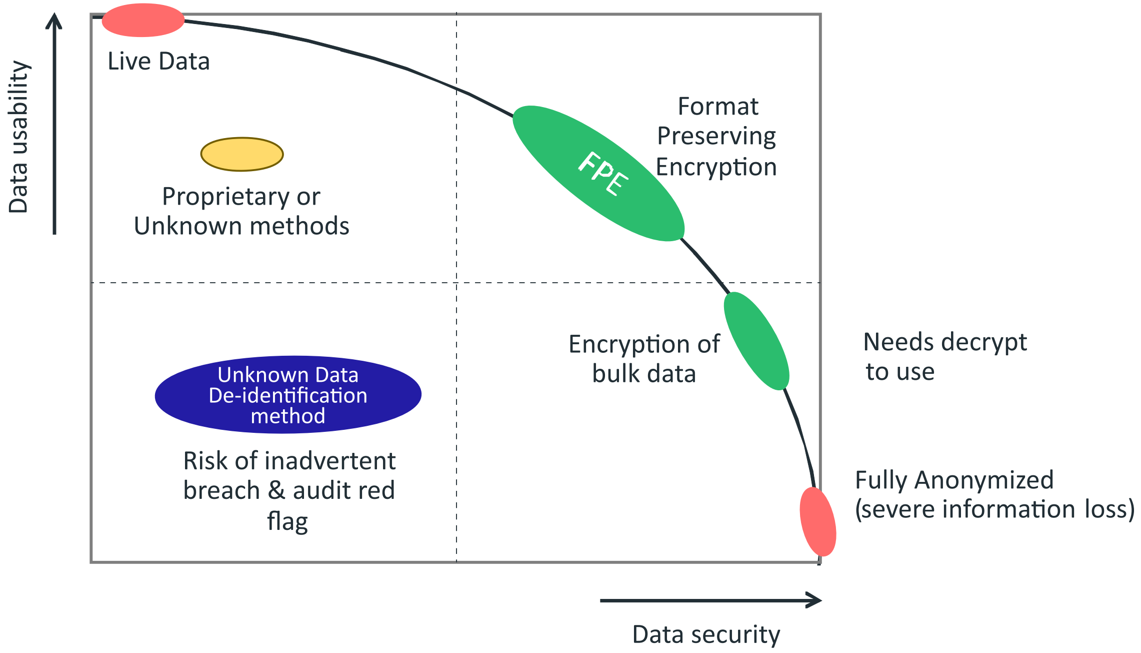
Data can be shared and analyzed

Voltage Hyper FPE optimizes protection and usability

Many technologies can be used for data protection, but only Voltage Hyper Format Preserving Encryption optimizes the balance between protection and usability for the needs of big data applications. For example:

- Bulk volume encryption provides strong security for data-at-rest, but data has to be decrypted and exposed for use.
- Full anonymization ensures security of data, but destroys data usability in the process.
- Proprietary, non-standard methods of protection may claim to retain data usability, but are essentially risky and uproven because of the lack of formal peer review from third-party validation.

Only NIST-recommended and FIPS-validated FPE from Voltage can offer strong, peer-reviewed security that also maintains data usability in its protected form. SecureData customers state they can run over 90% of their analytics on data protected by Voltage Hyper FPE without decryption that creates risk exposure.


Data usability
Live Data
Proprietary or Unknown methods
FPE
Format Preserving Encryption
Unknown Data De-identification method
Risk of inadvertent breach & audit red flag
Encryption of bulk data
Needs decrypt to use
Fully Anonymized (severe information loss)
Data security

“SecureData customers state they can run over 90% of their analytics on data protected by Voltage Hyper FPE without decryption ”

Not all FPE technologies are created equal

Voltage SecureData with Hyper FPE

Voltage SecureData with Hyper Format Preserving Encryption (FPE) can encrypt virtually unlimited data types. Hyper FPE technology delivers a proven method of protecting data that enables global enterprises to take full advantage of a breakthrough NIST-recommended encryption technology and delivers best-of-breed capabilities, including:

Hyper performance

Accelerated encryption for hyper performance—up to 170 percent faster than previous FPE technology—supporting high-volume needs of next-generation big data, cloud, and IoT scenarios.

Hyper flexibility

Encryption of virtually unlimited data types, including IDs, VINs, bank accounts, and classified data types that need encryption. Preserves format, relationships, context, meaning, and fit for use in advanced big data and hybrid IT environments and legacy systems.

Hyper usability

Gives data scientists, analysts and developers wide access to de-identified data, powering big data, cloud, and IoT initiatives, while using granular policy management control to limit access to highly sensitive data.

NIST, FIPS and Common Criteria

FPE has a formal proof of security with the NIST FF1 AES – SP800-38G recommendation and SecureData is the world's first FIPS and Common Criteria-validated FPE product—delivering a proven method of protecting data.

Voltage SecureData with Hyper Secure Stateless Tokenization (SST) offers an enhanced, patented approach to tokenization that maximizes speed, scalability, security, and manageability of the tokenization process, effectively doubling the existing "high octane" SST tokenization performance.

Voltage SecureData is fully integrated with Atalla HSM, a FIPS 140-2 Level 3 validated hardware appliance, offering organizations greater physical and logical data protection. Atalla HSM stores and manages root keys, with centralized configuration and security policy enforcement.

Global financial services firm – Hadoop and data warehouse

Business Need

- A global financial services firm needed to import massive data sets into data lakes from multiple sources for analysis to improve marketing to customers, find opportunities for monetization and improve fraud detection.
- This exposure places a massive volume of sensitive data at risk in a single data lake.

Challenge

- The firm needed a solution to protect data in multiple data warehouses and big data platforms, such as Hadoop, while enabling analytics.

Solution and Business Outcomes

- SecureData with Hyper FPE and SST protect PII and PCI data before Hadoop ingestion and throughout data warehouses, enabling data analysis in protected form without putting sensitive data at risk.
- Enabled wide expansion of live protected data access by BI tools for real-time analysis, ultimately achieving detailed ROI on IT investments, and dramatic PCI scope and compliance cost reduction.

Customer Use Case

Top car manufacturer – data lake, IoT and cloud

Business Need

- A top car manufacturer collects sensor data from millions of connected cars globally, including GPS location data, to find defects and improve product offering by analyzing vast data volumes in real time in a Hadoop data lake.

Challenge

- The data lake became “radioactive” with sensitive information – only 4 users were allowed access to information, running limited analytics, due to risk exposure.

Solution and Business Outcomes

- Voltage Securedata de-identified sensitive data from sensors or company systems, and integrated with Teradata warehouses and Hadoop, for end-to-end protection—anywhere data may travel.

- Enabled open access to de-identified data for hundreds of data scientists and analysts, while only a few have access to source sensitive data if absolutely required.

Customer Use Case

Large European telco – data lake, pseudonymization and GDPR

Business Need

- A large European telecom provider created a data lake with a 180-node Hadoop cluster in 2 data centers to analyze massive data sets, from millions of mobile subscribers in multiple countries.
- Looking for insights into operations, performance, fraud detection and monetization opportunities.

Challenge

- How to protect sensitive personal data including CDRs, location, IMEI, and other subscriber information in order to comply with data residency laws and GDPR.

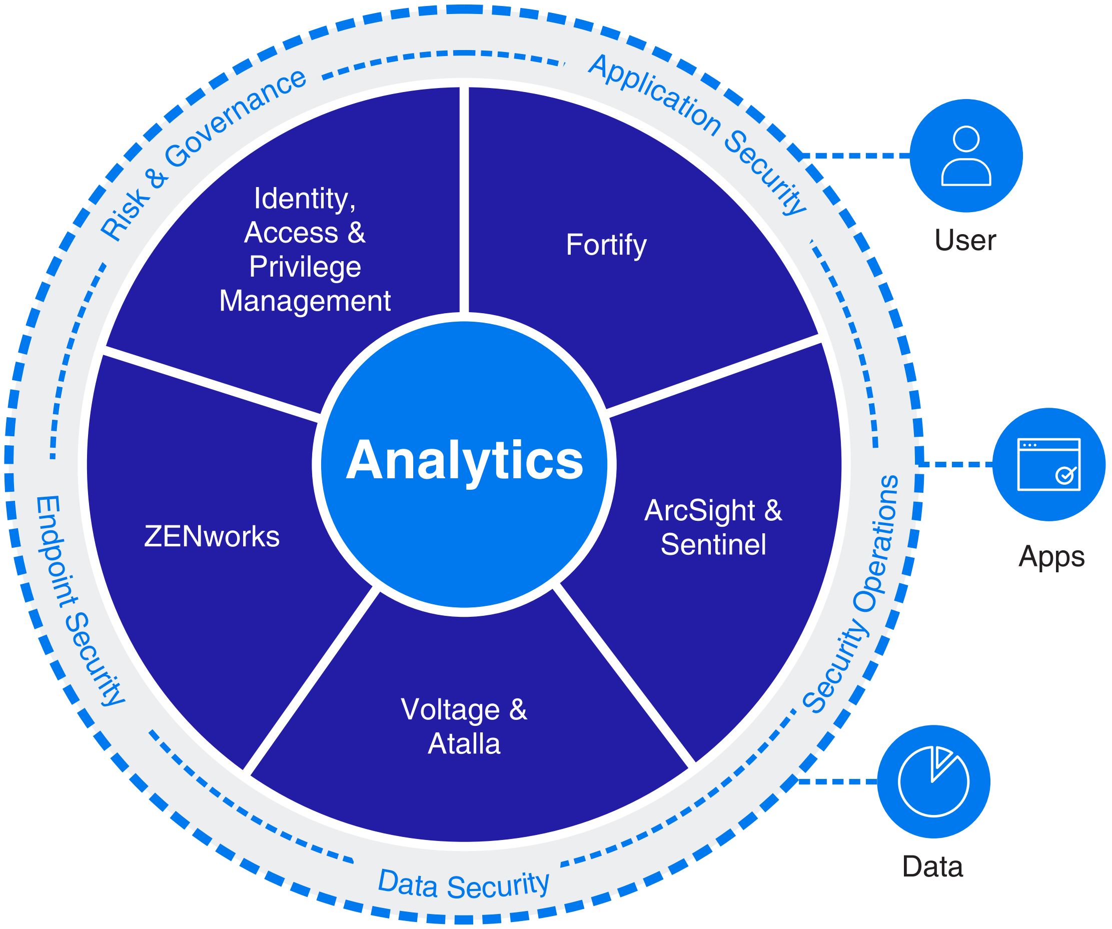
Solution and Business Outcomes

- Voltage SecureData pseudonymized personal information before uploading to Hadoop clusters, handling approximately 11 billion records daily.
- Enabled the analysis of data in protected form while complying with privacy mandates.
- Allowed for the expanded use and access of data across the enterprise leading to customer service optimization, improved fraud detection, scaled network analysis, and opened the door to finding new revenue streams.

Customer Use Case

Micro Focus:

A leading security and data governance portfolio to ensure safe analytics for the enterprise



Big data analytics underpins today's enterprise value creation and operational efficiencies, but it also creates new risks that old security models can't always address. Voltage SecureData is part of a broad security portfolio that incorporates identity management, application security, event monitoring, endpoint protection and information governance, that—when combined—offer multi-layered information lifecycle protection for the most critical data assets of an enterprise.

Learn more about how Micro Focus protects users, apps, and data—allowing companies to achieve competitive edge—while protecting their most sensitive data!

For more information:

Big data security

Voltage SecureData

Micro Focus Data Security

Micro Focus Data Security brings leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise, 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 Data Security solves one of the industry's biggest challenges: simplifying the protection of sensitive data in even the most complex use cases.

MICRO FOCUS®

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.

Copyright notice

335-000026-001