



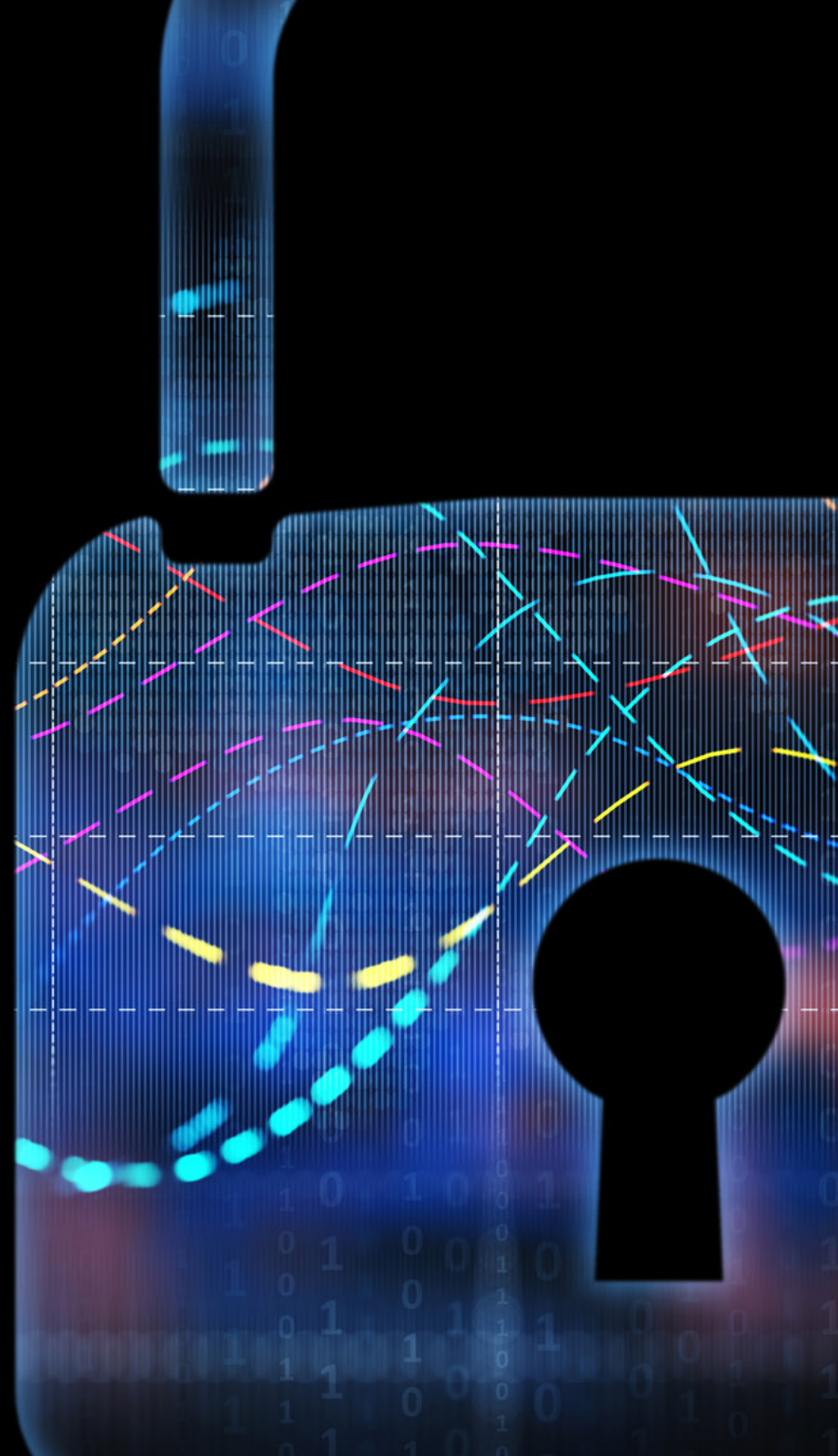
Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

TRENDS IN CLOUD DATA SECURITY

The Data Perimeter of Hybrid Clouds

JANUARY 2019



Research Objectives

The broad adoption of public cloud services and knowledge worker mobility have created the need to employ purposeful controls to secure data assets both within and outside of the network perimeter in an increasingly hybrid cloud world. The strategic imperative to secure the data perimeter is driving demand for a range of data security controls including DLP, encryption, UEBA, and rights management, as well as those provided natively by CSPs and those packaged as features in CASBs and CWPPs, resulting in market fragmentation and buyer confusion.

In order to get more insight into these trends, ESG surveyed 392 IT and cybersecurity professionals at organizations in North America (U.S. and Canada) responsible for evaluating and purchasing hybrid cloud security technology products and services.



GOALS OF THIS STUDY

- Examine the impact of cloud, mobility, and regulations on data security priorities.
- Gain insight into top data security challenges and the rate of data loss from the cloud.
- Determine the degree of separation between unified approaches for cloud and on-premises data assets.
- Understand data security spending intentions and priorities.

Survey participants represented a wide range of industries including manufacturing, financial services, health care, communications and media, retail, government, and business services. For more details, please see the *Research Methodology and Respondent Demographics* sections of this report.

Executive Summary

KEY RESEARCH FINDINGS

- » **1. Data is shifting to public cloud ahead of organizational readiness to secure it.** Organizations are increasingly storing data—a significant amount of which is considered “sensitive”—in public clouds. However, initiatives to secure that data lag similar on-premises efforts, with significant amounts of sensitive data not being sufficiently secured.
- » **2. Shadow IT and data discovery top list of cloud security challenges.** Not surprisingly, the concerns and challenges associated with securing cloud-resident data included a combination of technology, people, and process—with the biggest challenge being employees signing up for cloud applications and services without IT approval or oversight.
- » **3. Data loss associated with public cloud services is common, due to a multitude of causes.** The increased use of both sanctioned and unsanctioned cloud-based applications, in combination with security programs for the cloud that are often less mature than existing on-premise initiatives, has led to a significant loss of corporate data. Top contributors to data loss included violations of security policy, the lack of effective access controls, and the implications of employees using their own devices.
- » **4. Organizations are making investments across multiple data security disciplines.** Organizations identified numerous improvements required to secure sensitive assets regardless of location. And 40% of respondents expect cybersecurity spending to increase substantially.
- » **5. Cloud and on-premises data security are currently handled by different teams, but most organizations strive for unified function.** The ability to gain greater operational efficiencies by unifying security policies across on-premises and cloud-resident data, regulatory compliance, and fears about data loss are primary investment drivers.
- » **6. Cloud security architects have emerged with broad responsibilities and influence, but IT is still the buyer.** The cloud security architect has emerged as a new role with broad responsibilities and influence over the security of cloud-resident data. And IT, security operations, the network security group, development operations, and line of business/application owners are often involved in purchase decisions for security products and services. However, it is IT that continues to be the primary economic buyer.

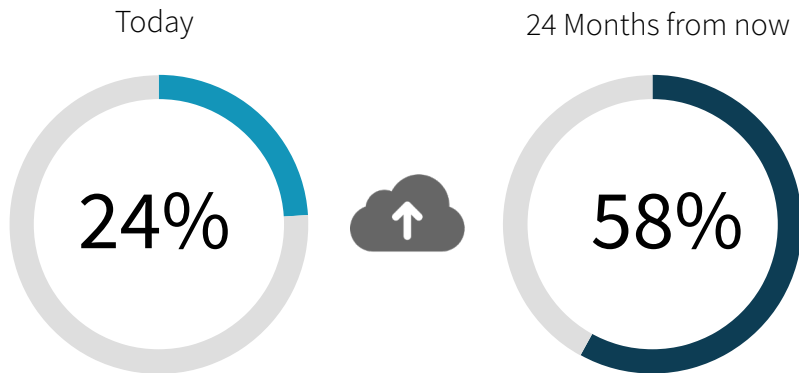
**DATA IS SHIFTING TO
PUBLIC CLOUDS AHEAD OF
ORGANIZATIONAL READINESS
TO SECURE IT.**



Data Is Moving to Public Cloud Services, including Sensitive Data

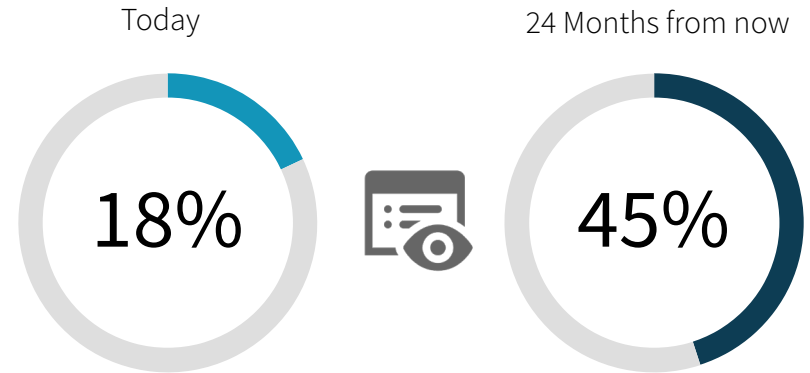
Almost one-quarter (24%) of respondents said that more than 40% of their corporate data resides on public cloud services today. This is expected to more than double to 58% of organizations within 24 months.

» Respondents with more than 40% of company data in public cloud



Nearly one in five (18%) respondents said that more than 40% of their corporate data that resides on public cloud services today is sensitive. This is expected to more than double to 45% of organizations within 24 months.

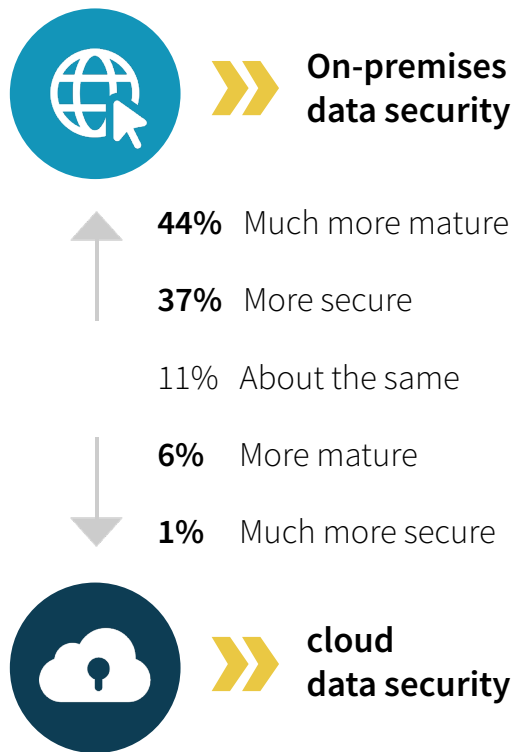
» More than 40% of public cloud-resident data is sensitive



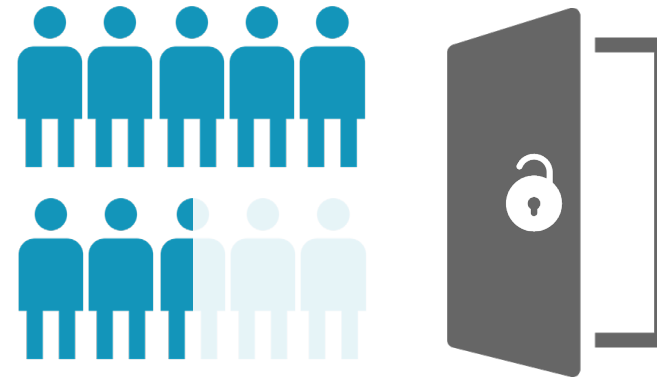
At least 75% of respondents with sensitive cloud-resident data say it is stored across several public cloud environments.

Public Cloud Security Not Keeping Pace with Requirements

Forty-four percent of respondents said that their on-premises data security is much more mature than their data security for public cloud services.



Not surprisingly, three-quarters of respondents believe that at least 20% of their public cloud data is insufficiently secured.



» **3/4**
of respondents say more than
20% of their public cloud data is
insufficiently secured

SHADOW IT AND DATA DISCOVERY TOP LIST OF CLOUD SECURITY CHALLENGES



Cloud Data Security Challenges



» **35%**

of respondents indicated that one of their biggest challenges for the security of data in the cloud is employees signing up for cloud applications and services without IT approval or oversight (i.e., shadow IT).

Another 30% of respondents said that discovering and classifying personally identifiable information (PII) to address data privacy concerns and comply with regulatory requirements is their biggest challenge.

» OTHER SIGNIFICANT CLOUD DATA SECURITY CHALLENGES



2.

Discovering and classifying personally identifiable information



3.

General organizational knowledge of cybersecurity threats



4.

Trusting employees to follow their organization's data usage policies



5.

Detecting data breaches in real time

Cloud Data Security Concerns

Given some of the top cloud data security challenges, it's not surprising that only 39% of respondents are completely confident in their organization's abilities to discover and classify all its public cloud-resident sensitive data.



ONLY 39%

of respondents are completely confident in their organization's abilities to discover and classify all its public cloud-resident sensitive data.

This lukewarm confidence manifests itself in the fact that 87% of respondents stated that concerns around data security have adversely impacted usage of public cloud services to some extent.



25%

Yes, concerns around data security have prevented our adoption of some public cloud services



62%

Yes, concerns around data security have slowed our adoption of public cloud services



13%

No, concerns around data security has not affected our use of public cloud services

An aerial night photograph of a city skyline, likely Dubai, featuring several illuminated skyscrapers and a highway with light trails from traffic. The text is overlaid on the left side of the image.

**DATA LOSS ASSOCIATED
WITH PUBLIC CLOUD
SERVICES IS COMMON,
DUE TO A MULTITUDE
OF CAUSES**

Organizations Are Losing Data



50%

of respondents know their organization has lost cloud-resident data

However, cloud-resident data loss is not limited to one public cloud service model, as companies report data loss across software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS) solutions.



PERCENTAGE OF ORGANIZATIONS REPORTING DATA LOSS



35%

SaaS



28%

IaaS/PaaS



13%

SaaS+IaaS/PaaS

Contributors to Cloud-based Data Loss

The top contributors to cloud-based data loss were policy violations, access controls/credentials, and use of personal devices.

» POLICY VIOLATIONS:



Sensitive data uploaded to IT-led cloud services, **33%**



Use of unsanctioned cloud services, **25%**



Exposure from data misclassification, **25%**

» ACCESS CONTROLS/ CREDENTIALS:



Misuse of access/permission controls, **32%**



Misconfigured object storage, **29%**



Stolen employee credentials, **26%**

» BYOD:



Data exposure from personal devices, **32%**



Data exposure from mobile devices, **25%**

The background is a composite image. On the left, a dense cityscape (likely Hong Kong) is visible, with numerous skyscrapers and buildings packed along a coastline. The water in the foreground is a deep blue-green. In the upper left, a large commercial airplane is flying towards the right. On the right side, a person in a dark suit is seen from behind, standing in a high-rise office window, looking out over the city. The window reflects the sky and clouds. The overall tone is professional and modern.

**ORGANIZATIONS ARE MAKING
INVESTMENTS ACROSS MULTIPLE
DATA SECURITY DISCIPLINES**

Highest Data Security Priorities

Given its inclusion among the most common cloud data security challenges, it makes sense that discovery and classification of sensitive data (regardless of location) tops the list of cloud security priorities (35%). Other common areas of focus include actively monitoring user access to sensitive data (35%) and the need to build a cloud security strategy that can be used to secure data across both public and private clouds (34%).

» TOP FIVE RESPONSES

**35%**

Improve discovery and classification of sensitive data to meet regulatory requirements

**35%**

Actively monitor user access to our most sensitive data

**34%**

Build a cloud security strategy that can be used to secure data assets across heterogeneous public and private cloud environments

**32%**

Increase visibility into when folders, directories and shares are breached

**32%**

Extend our current security technologies to protect cloud-resident data

Data Security Spending Increase

The vast majority (83%) of organizations expect to increase spending on data security technology over the next 12 months, and four out of ten expect this increase to be substantial.

In terms of cloud data security investments, planned technology acquisitions are consistent with organizations' stated needs for the next 12 months. Specifically, cloud workload protection platforms, data discovery and classification, DLP for cloud, and data encryption are the tools likeliest to receive funding.



» TOP FOUR RESPONSES



34%

Cloud workload protection platform



33%

Data discovery and classification




33%

Data loss prevention



33%

Data encryption provided by our cloud service provider



**CLOUD AND ON-PREMISES
DATA SECURITY ARE
CURRENTLY HANDLED BY
DIFFERENT TEAMS, BUT MOST
ORGANIZATIONS STRIVE FOR
UNIFIED FUNCTION.**

Top Business Drivers for Third-party Cloud Data Security Tools

Currently, nearly half (46%) of organizations leverage third-party security controls for their cloud-resident data.



» 46%

of organizations leverage
third-party security controls
for their cloud-resident data.

What are the top business drivers behind usage of third-party cloud data security technologies? The unification of security policies across on-premises and cloud-resident data (via centralized management) is an investment driver for 38% of respondents.

» TOP FOUR RESPONSES



38%

Gaining greater operational efficiencies by unifying policies across our own data center and cloud-resident data assets via centralized management



34%

Assuring regulatory compliance/passing external audits



32%

The sheer number of assets that are cloud resident



31%

Fears about security incidents, including data loss, our organization may experience in the future

Other common factors include regulatory compliance and passing external audits, the amount of cloud-based data, and fears of future security incidents, including data loss.

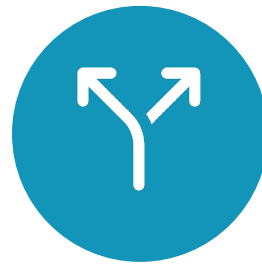
Separate On-premises and Public Cloud Data Security Teams

A majority (86%) of organizations currently maintain separate teams for data security policies, processes, and technology, though 61% plan to merge functions in the future.



61%

Yes, we currently have different teams responsible for securing the on-premises and public cloud-resident portions of our hybrid cloud infrastructure, but we plan to merge these responsibilities in the future



25%

Yes, we currently have different teams responsible for securing the on-premises and public cloud-resident portions of our hybrid cloud infrastructure, and we have no plans to merge these responsibilities



14%

No, we currently have centralized and unified security responsibility across all aspects of our hybrid cloud environment

The background features a dark, textured sky with large, billowing white and grey clouds at the bottom. Overlaid on this is a complex, dense web of thin, golden-yellow lines that swirl and curve across the upper portion of the image, creating a sense of dynamic movement and digital connectivity.

**CLOUD SECURITY ARCHITECTS
HAVE EMERGED WITH BROAD
RESPONSIBILITIES AND
INFLUENCE, BUT IT IS STILL
THE BUYER.**

Cloud Security Architects

Nearly two-thirds (60%) of organizations say they have a cloud security architect in place, with another 23% actively hiring or establishing this position within 12-24 months.

» **60%**

of organizations say they have a cloud security architect in place



» **21%**

Yes, and this position(s) has been in place for at least a year

» **39%**

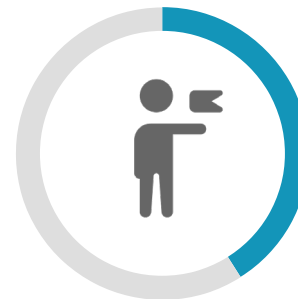
Yes, and this position(s) was recently established (i.e., within the last 12 months)

More than three-quarters (79%) of these organizations said their CSA does/will report to a C-level executive, and 41% report that these individuals define (or will define) policies for cloud-resident data.



» **79%**

of these organizations said their CSA does/will report to a C-level executive



» **41%**

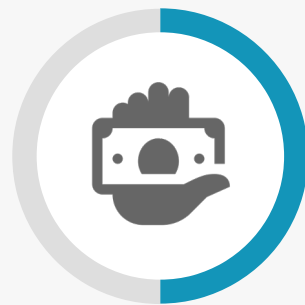
report that these individuals define (or will define) policies for cloud-resident data.

Cloud Data Security a Team Initiative

Fifty-eight percent of respondents said their security team was directly involved in creating their organization's cloud data security policies, along with IT operations and networking groups.



When it comes to purchasing, 61% of respondents said IT typically makes the purchase decisions, with SecOps, network security, and DevOps as key influencers.

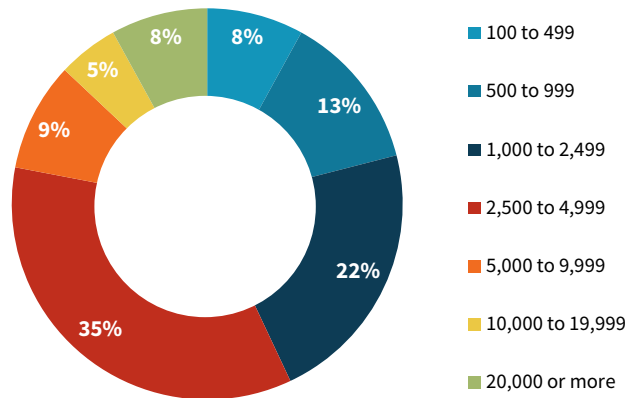


61%

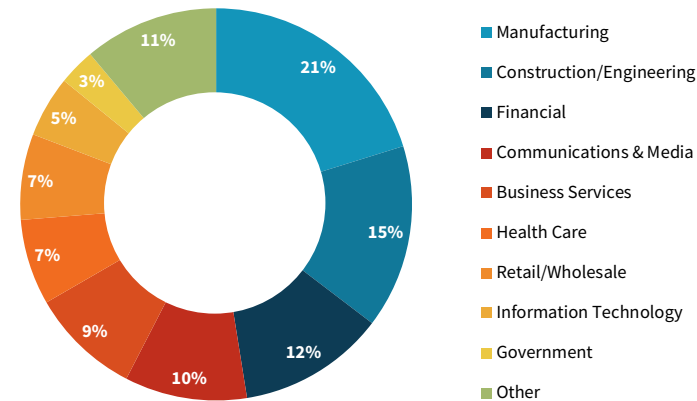
of respondents said IT typically makes the purchase decisions, with SecOps, network security, and DevOps as key influencers.

Research Demographics and Research Methodology

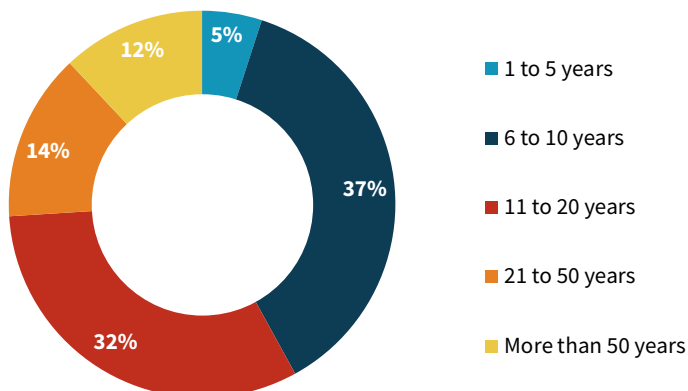
Respondents by Number of Employees Worldwide



Respondents by Industry



Respondents by Age of Organization



To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between August 16, 2018 and September 6, 2018. To qualify for this survey, respondents were required to be IT or cybersecurity professionals personally responsible for evaluating and purchasing hybrid cloud security technology products and services. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 392 IT and cybersecurity professionals.



Micro Focus Voltage enables the world's leading brands to neutralize data breach impact for data at rest, in motion and in use by de-identifying sensitive information.

Micro Focus® Voltage data security solutions enable advanced format-preserving encryption, secure stateless tokenization, and stateless key management to protect enterprise applications, data processing infrastructure, hybrid IT/cloud, payment ecosystems, mission-critical systems, storage, and big data/IoT analytics platforms. Voltage data security solutions solve the industry's biggest challenge by simplifying data protection across complex legacy and modern IT, enabling organizations worldwide to comply with privacy mandates with confidence and trust, while driving digital transformation for value creation.

LEARN MORE

ABOUT ESG

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.





All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.