REPORT

Enterprise Supernova: The Data Dispersion Cloud Adoption and Risk Report

This report is brought to you courtesy of Ingram Micro.

REPORT

McAfee

Enterprise Supernova: The Data Dispersion Cloud Adoption and Risk Report

Table of Contents

REPORT

Enterprise Supernova: The Data Dispersion Cloud Adoption and Risk Report

The stars in our universe are fueled by nuclear energy at their core. Over time, that fuel burns out, causing the star to cool. A supernova occurs at the end of a star's life, when the core has cooled to the point where the external force of gravity is stronger than its internal fuel source can handle, ultimately causing a massive explosion of its matter into the universe.

Modern enterprises are fueled by data. The force of the cloud has been like gravity in a supernova, causing data to explode outward and disperse forever. No longer constrained by the network, the free flow of data to cloud service providers and a wide range of devices fragments visibility and control for enterprise security.

While most data outside of the network resides in cloud services sanctioned by IT, thousands of other cloud services are used ad hoc, without vetting. Collaboration within the cloud bypasses any remaining network controls. Sensitive data accessed by unmanaged personal devices disappears indefinitely.

Security and risk management professionals are left with a patchwork of controls at the device, network, and cloud—with significant gaps in visibility to their data. Living with these gaps and the patchwork of security born out of the network is an open invitation to breach attempts and noncompliance.

Breaking this paradigm requires a thorough understanding of where data goes today and how risk has changed with the rapid advancement of cloud adoption. In this paper, we'll evaluate a combination of survey results from 1,000 enterprises in 11 countries and an investigation into anonymized events from 30 million enterprise cloud users to provide you with a holistic view of modern data dispersion, so you can learn and adapt your own security practice.

Key Findings

- **"Shadow IT" and the greater web expand risk infinitely:** Fifty-two percent of companies use cloud services that have had user data stolen in a breach.
- **Unmanaged personal devices are black holes:** One in four companies have had their sensitive data downloaded from the cloud to an unmanaged personal device, where they can't see or control what happens to the data.
- **A new era of data protection is on the horizon:** Only 31% of companies have consistent data protection across their devices, networks, and cloud services.
- **Intercloud travel opens new paths to risk:** Nearly one in 10 files shared in the cloud with sensitive data use a link open to the public, an increase of 111% year over year.
- **Dispersion outpaces IT:** More than 40,000 data loss incidents are likely missed every month by companies who don't monitor their cloud services.

The Aftermath of Data Dispersion

Like discovering new planets and stars in the sky, we are constantly discovering new locations in the cloud where enterprise data travels. Services like Microsoft Office 365 are as clear as the sun. Thousands of others are used ad hoc, some representing new forms of productivity to eventually become sanctioned by IT. In our survey, companies told us they typically sanction 41 cloud services, 33% more than a year ago.

Cloud services have replaced many business-critical applications formerly run as on-premises software, driving a migration of sensitive data. Seventy-nine percent of companies told us they store sensitive data in the public cloud.

From our investigation into real-world cloud event data, we can see that 26% of files in the cloud contain sensitive data, an increase of 23% year over year.

Files in the Cloud with Sensitive Data

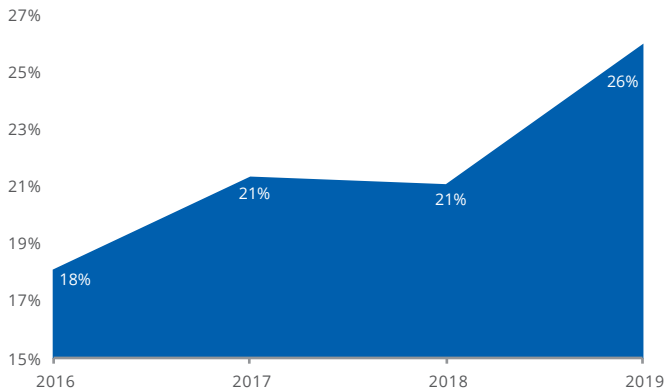

Figure 1. Anonymized cloud event data showing percentage of files in the cloud with sensitive data.

Nearly one in 10 files shared in the cloud with sensitive data use a link open to the public, an increase of 111% year over year.

Twenty-six percent of files in the cloud contain sensitive data, an increase of 23% year over year.

As security professionals, we're tasked with protecting our organization's assets, now widely dispersed in the cloud. Still, one in five companies say they lack visibility into what data is in their cloud applications.

The edge of our IT universe is now an amorphous ecosystem of cloud services that has no defined perimeter to act as a boundary. In this model, security must move closer to the data, as that is our only certain point of reference. It starts with visibility into data from the device, through the web, into and throughout cloud services. Methods of control are familiar, yet find new life in a cloud context.

Stopping a data breach in the cloud is first priority. Data loss prevention (DLP) technology that runs in the cloud is new to many but effective for services sanctioned by IT. From our real-world event data, we can see the prevalence of data loss incidents for companies running DLP in the cloud, covering millions of cloud users. On average, enterprise companies running DLP in Software-as-a-Service (SaaS) see 45,737 incidents every month. Yet only 37% of companies we surveyed told us they currently run DLP in the cloud. Every company tailors what they consider to be sensitive data and what qualifies as an incident. However, for the 63% not running DLP in the cloud, there is likely unseen risk.

Intercloud Travel

Our future may be interstellar, but our data is already intercloud by design. Collaboration facilitates the transfer of data within and between cloud services, creating a new contextual challenge for data protection. Forty-nine percent of files that enter a cloud service are eventually shared, whether to a colleague, business partner, or the whole world. Risk comes from sensitive data reaching an undesired location, in many cases, unintentionally.

In Box, for example, you might share a presentation with upcoming product plans and pricing to a colleague—which is helpful when the file size exceeds your email limit. Twelve percent of files shared in the cloud contain sensitive data such as this, an increase of 57% year over year.

Files Shared in the Cloud with Sensitive Data

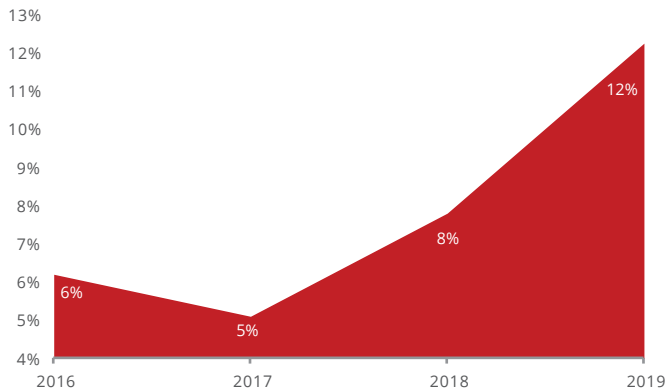

Figure 2. Anonymized cloud event data showing percentage of files shared in the cloud with sensitive data.

One in five companies say they lack visibility into what data is in their cloud applications.

On average, enterprise companies running DLP in SaaS see 45,737 incidents every month.

A common mistake—yet a feature by design—is creating a link with public access when sharing sensitive data from a cloud service like Box. The recipient of your strategy presentation may not be aware of its sensitivity and forward on to external business partners, customers, or prospects. When the link is public, all of them have access, and sensitive data is exposed without recourse. Nearly one in 10 files shared in the cloud with sensitive data have public access, an increase of 111% year over year.

Files Shared in the Cloud with Sensitive Data Using a Public Access Link

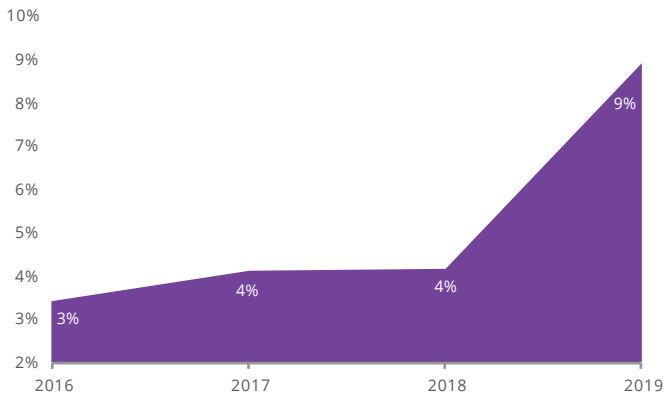

Figure 3. Anonymized cloud event data showing percentage of files shared in the cloud with sensitive data using a public access link.

Data shared from a cloud service like Box to another cloud user or any external party is not visible to network controls. Again, our protection strategy must be closer to the data and must control its motion within the cloud. Only 34% of companies told us they could control collaboration settings for their cloud services, including sharing permissions like the use of public access links.

Unmanaged Personal Devices Are Black Holes

The remnant of a supernova is a black hole, nearly undetectable and carrying inescapable gravitational force. As we've broken free from the constraints of the network and dispersed data to the cloud, our devices remain, some visible and controlled by IT and many more personally owned and invisible. Data can and will enter the black hole of an unmanaged personal device, as many cloud services can be accessed with credentials alone. This again is often by design. For example, working in a sales position can require frequent travel, and access to data in services like Salesforce from anywhere. A personal smartphone can login, view, and download customer data and then move that data anywhere else freely. Seventy-nine percent of companies allow access to the cloud by personal devices, varying by sector.

Nearly one in 10 files shared in the cloud with sensitive data have public access, an increase of 111% year over year.

Only 34% of companies can control collaboration settings for their cloud services.

Who Allows Access to the Cloud from Personal Devices?

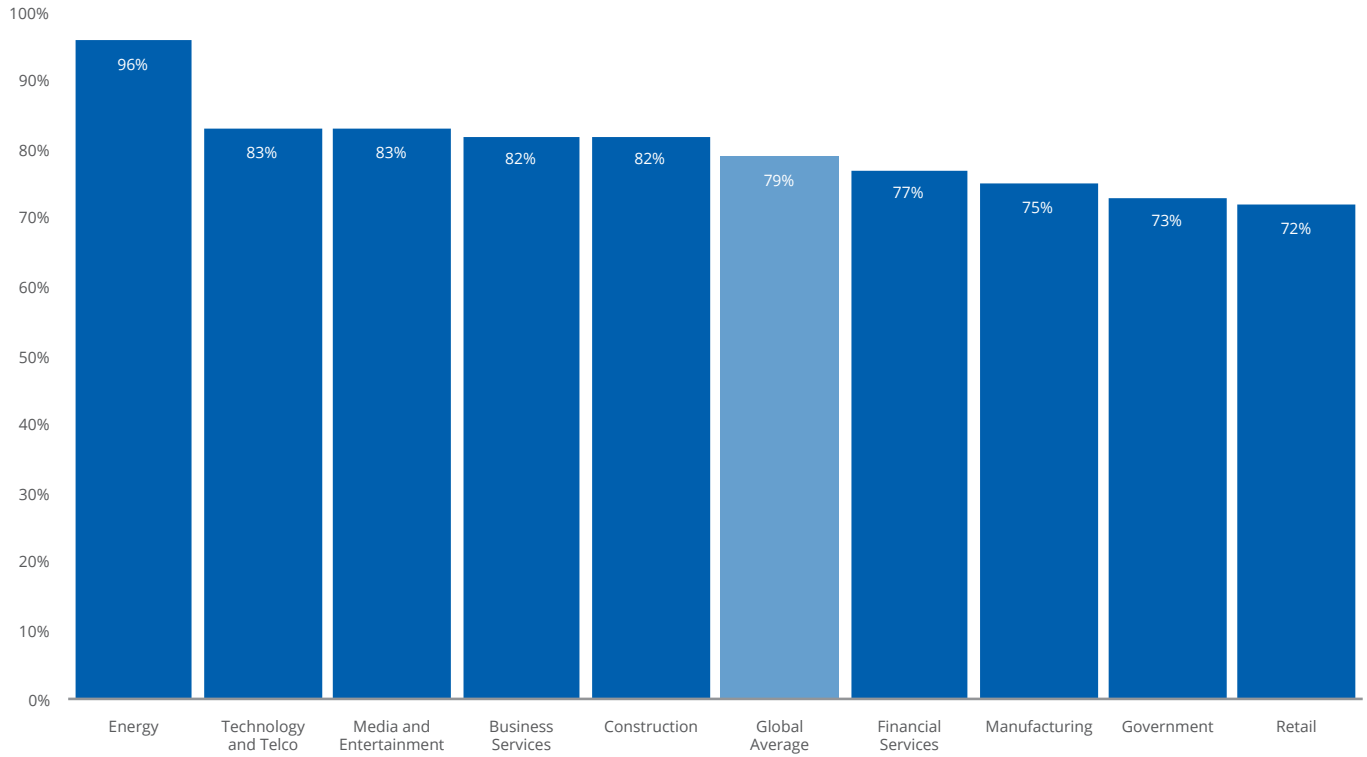

Figure 4. Survey data showing results by industry from the question "Does your organization allow access to data from employee-owned, personal devices in any of the following cloud services (SaaS, PaaS, or IaaS)?"

79% of companies allow access to the cloud by personal devices.

Any sensitive data that reaches an unmanaged personal device is a data loss event. Customer records. Financial plans. Product roadmaps. An employee may find a multitude of justifiable business rationales for accessing this data, but it is lost forever. One in four companies report having their sensitive data leaked to unmanaged personal devices.

Who Has Had Sensitive Cloud Data Leaked to an Unmanaged Personal Device?

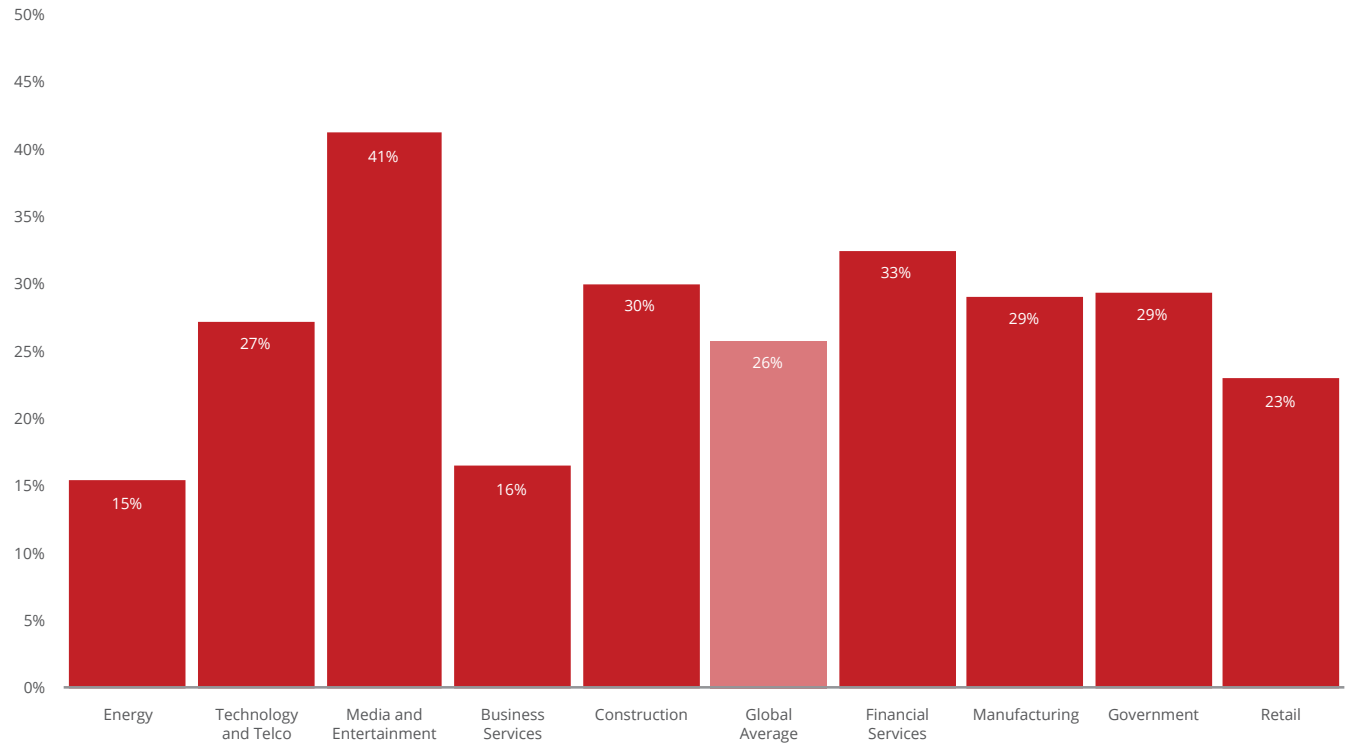

Figure 5. Survey data showing results from the question "Has your organization experienced any of the below issues when it comes to using SaaS?" Showing results by industry for "Sensitive data download to an unmanaged personal device."

Our data-centric model for security hedges against these data loss incidents ever happening. Yet only 41% of companies tell us they can control personal device access to their data in the cloud.

One in four companies report having their sensitive data leaked to unmanaged personal devices.

Who Can Control Access to Cloud Data for Personal Devices?

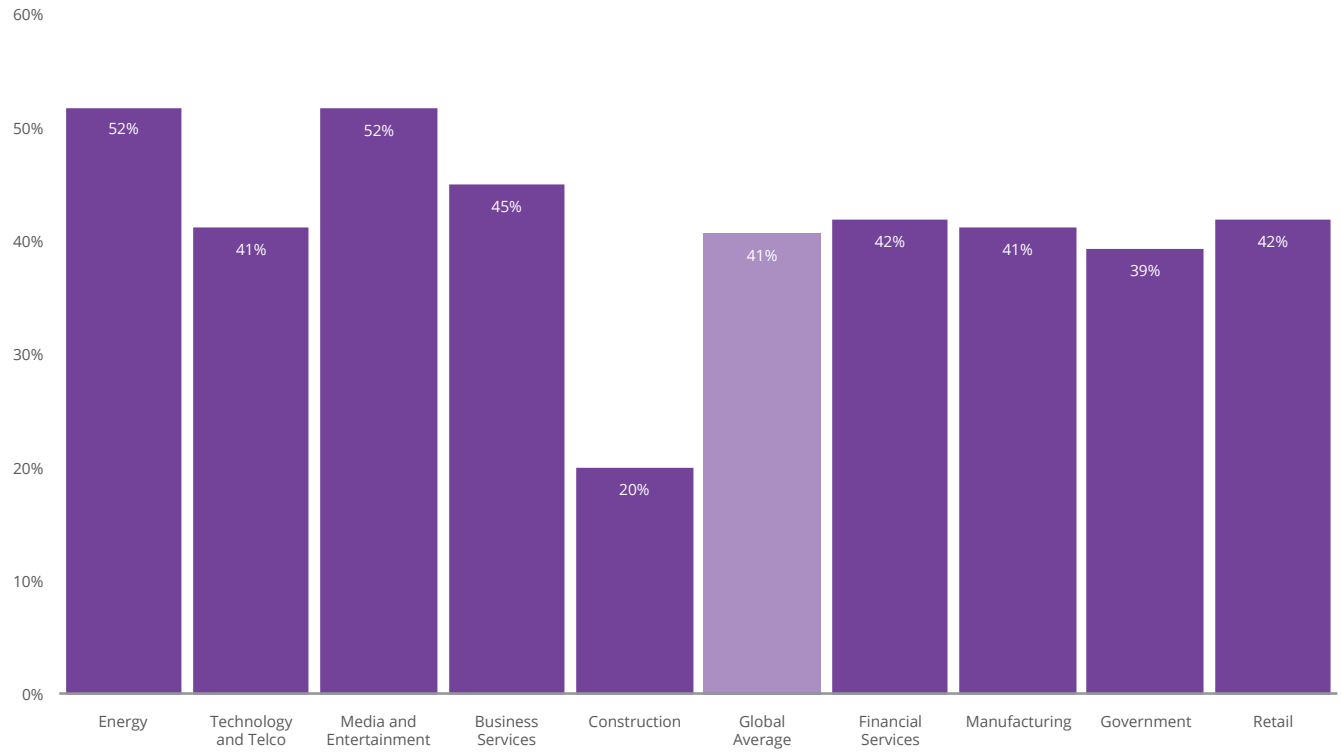

Figure 6. Survey data showing results from the question "Can your organization's current cloud security solution(s) conduct any of the following in the cloud?" Showing results by industry for "Control access to cloud data for personal devices."

Only 41% of companies can control personal device access to their data in the cloud.

Some industries are struggling with this problem, while others are much further ahead. For example, despite an above-average likelihood that media and entertainment companies can control personal device access to data in the cloud, they rank the highest for data loss incidents. The energy sector, which has long required technology access in dispersed remote locations, is both mature in its ability to control personal device access and the least likely to experience data loss incidents. The same cannot be said for the average company in construction, which has an inverse relationship between control and incidents. Construction firms are less likely to control personal device access and more likely to experience data loss incidents.

Navigating around these black holes requires direction from the source of the data. Contextual access can be enforced at the cloud service itself, assessing the device type to only allow devices IT can control, and blocking the rest.

Infinite Expansion: "Shadow IT" and the Greater Web

While an average of 41 cloud services are sanctioned at most enterprise companies, there are thousands more being used ad hoc, some for a single task and others more regularly, but under the radar and waiting to be the next sanctioned app. The universe of cloud apps is expanding infinitely. IT has the benefit of direct control over the services they sanction, managing risk to data with full cloud context. With "Shadow IT," the diversity of services is unpredictable. Some have application programming interfaces (APIs) that allow them to become fully controlled sanctioned services, and others do not. The risk profile of each cloud provider is just as variable. Let's look at a few examples.

Ninety-one percent of cloud services do not encrypt data at rest. That means your data is not protected if the cloud provider is breached. Sensitive data needs to be classified and blocked before entering the cloud service to mitigate risk or block access to the service altogether.

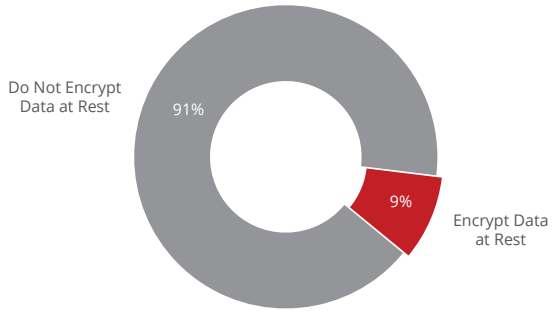

Figure 7. Cloud registry assessment showing the percentage of cloud applications that encrypt customer data at rest.

Next, 87% of cloud services do not delete data upon account termination. That means your data could live with the cloud provider in perpetuity, with complete uncertainty as to what they'll do with it in the future. The same strategy applies. Control what goes in the cloud or block these services outright.

91% of cloud services do not encrypt data at rest.

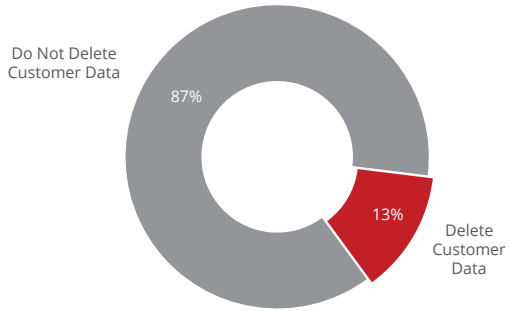

Figure 8. Cloud registry assessment showing the percentage of cloud applications that delete customer data after account termination.

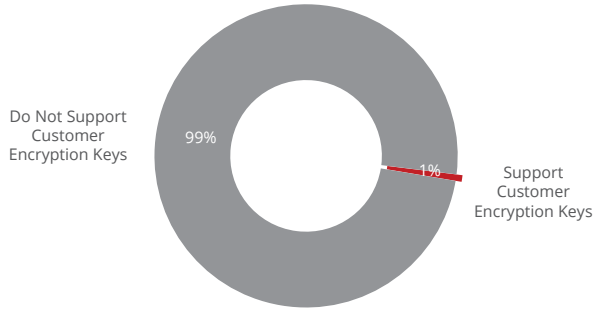

Figure 9. Cloud registry assessment showing the percentage of cloud applications that support data encryption with customer-owned encryption keys.

At this point, you might reach the conclusion that, if you were able to use your own encryption keys, you could allow access to these services and still protect your data. Unfortunately, less than 1% of cloud services allow encryption with customer-managed keys. Business critical apps like Salesforce do support customer-managed keys, however, so you can still control your own encryption for some critical data types. We hope more cloud service providers move in this direction. Until then, choose apps that support bring your own key (BYOK) when you can, and make sure your other apps encrypt data at rest.

The next area of risk is access control, specifically the ability to harden access with multifactor authentication (MFA), such as SMS, tokens, and other methods. Only 22% of cloud services support MFA. This was 19% one year ago, so the industry is moving in the right direction but not rapidly. MFA is still the best risk mitigation tool against credential theft and should be part of your protection strategy for critical apps where it is supported.

Less than 1% of cloud services allow encryption with customer-managed keys.

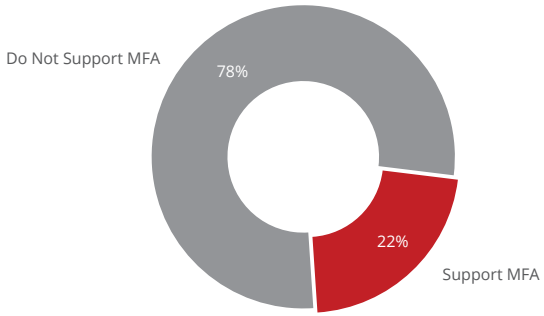

Figure 10. Cloud registry assessment showing the percentage of cloud applications that support multi-factor authentication.

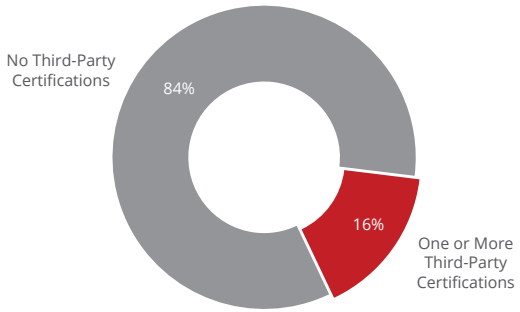

Figure 11. Cloud registry assessment showing the percentage of cloud applications with at least one third-party certification, for example: HIPPA, PCS, SOC2, SOC3, ISO27017, ISO27018, FEDRamp, or others.

Lastly, for companies that are subject to strict regulation, it is important to determine whether cloud providers have the compliance certifications you need to even consider using them. We found in our assessment that only 16% of cloud services have one or more third-party certification, such as HIPAA, PCI, SOC2, SOC3, ISO27017, ISO27018, or FedRAMP. This is an indicator of how seriously some cloud providers take their security practice and a required point of investigation for many organizations.

The notion of risk here is clear, but consensus varies within many organizations. C-Level IT leaders see the risk of "Shadow IT," while manager-level decision makers are less likely to report risk to their data from unsanctioned applications.

Only 16% of cloud services have one or more third-party certification, such as HIPAA, PCI, SOC2, SOC3, ISO27017, ISO27018, or FedRAMP.

Do You Believe Shadow IT Impairs Your Ability to Keep Data Secure?

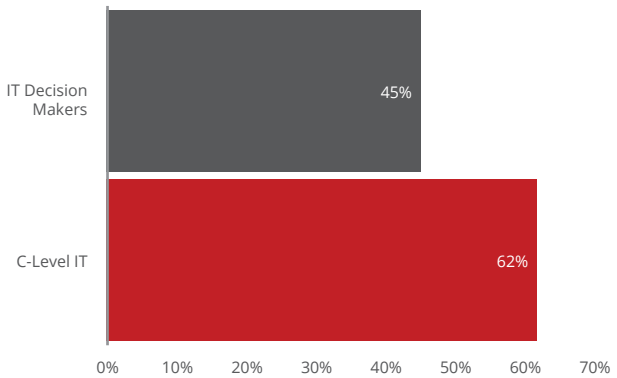

Figure 12. Survey data showing results from the question "Does Shadow IT impair your organization's ability to keep data secure?" by aggregate role.

While we've uncovered in past research that only 10% of sensitive data lives in "Shadow IT,"[1] the risk factors associated with many of these services can still lead to data loss events. In an investigation into our real-world cloud event data, we found that 52% of companies use cloud services that have had user data stolen in a breach. Usernames and passwords are a common data type in these breaches, compounding risk when the same credential combinations are used across multiple services. In a similar investigation, Microsoft found that, in their own active accounts, 44 million users were currently using credentials that had been stolen in the past and leaked to the public.[2]

Despite the risk and general knowledge of the vast expanse of unsanctioned cloud services, only 34% of companies say they can discover and remediate "Shadow IT." The continuous expanse of "Shadow IT" can and should be a part of every data protection strategy. The control point is out from the device and through the internet to a cloud destination. Data protection can be implemented at these stages through analysis of data leaving the device and control over web traffic to the cloud.

The Next Horizon for Data Protection

The data-centric model for security we've discussed allows us to adapt to the dispersion of data into the cloud. Most companies understand it is their responsibility to protect data in the cloud, reinforced by every major cloud provider from AWS to Microsoft and others as a shared responsibility that their customers agree to uphold. This is not universally understood within most organizations. Again, C-Level leaders in IT are the most likely to understand that it is their responsibility to secure data in the cloud. Ninety-three percent of CISOs get this.

52% of companies use cloud services that have had user data stolen in a breach.

Who Is Responsible for Securing Data in the Cloud?

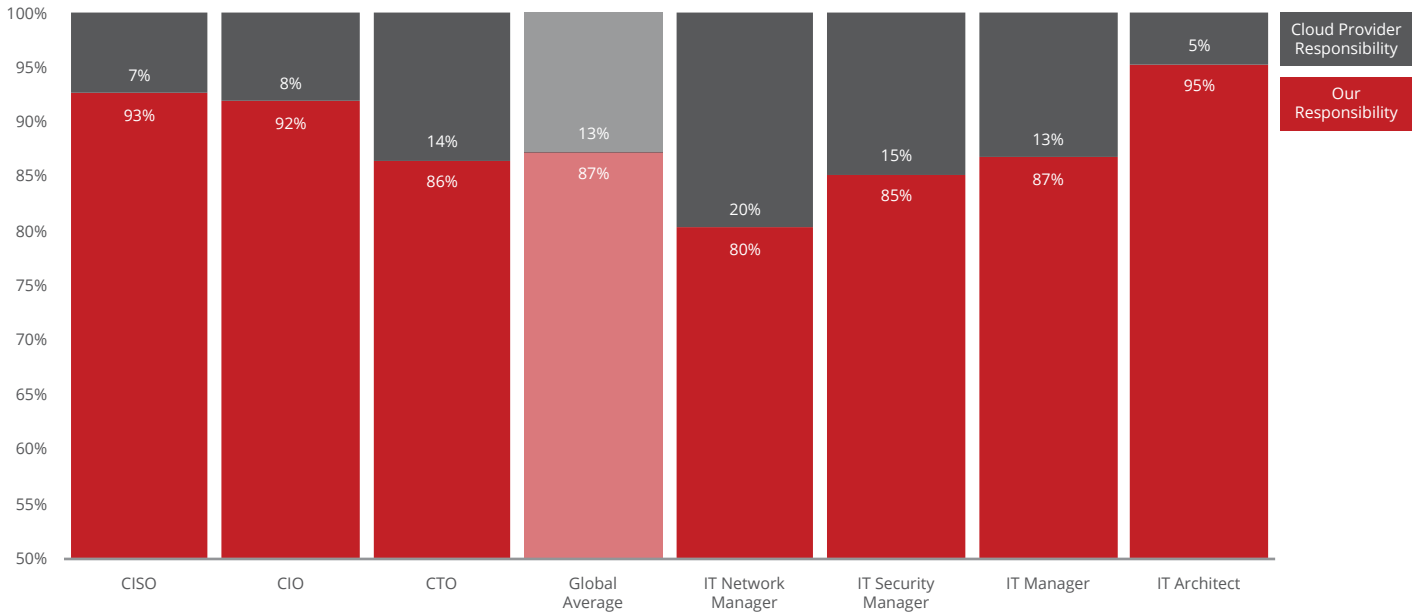

Figure 13. Survey data showing results from the question "Who is responsible for securing the data held in cloud services for your organization?" by role.

30% of companies lack the staff with skills to secure SaaS applications.

Many roles outside of the C suite are less clear on the delineation. One in five network security managers think cloud providers are responsible for securing their organization's data. Cloud providers do not implement controls for what data can live in the cloud, who can access it, and where it can go. If a network security manager is responsible for allowing access to cloud services through their network, they may not be considering their full responsibility to protect that data in motion.

In our survey, 30% of companies told us that they lacked the staff with skills to secure their SaaS applications, 33% more than a year ago. Both technology and training are likely being outpaced by the rapid expansion of cloud adoption.

Ninety-seven percent of companies told us they use some form of cloud security technology, whether native controls that a cloud provider offers or third-party tools. Forty-one percent said those tools could manage

all types of cloud services, whether SaaS, Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), or private cloud together. Every company uses multiple SaaS providers, and, as we've discussed in prior research, 92% are multicloud for IaaS.[3] Only 31% said their cloud security tools could enforce the same DLP policies at their devices, network, and cloud services.

The next horizon for data protection starts with the device and follows data through the network to a new cloud edge. Based on our analysis in this study, reaching this horizon will require:

1. **Cloud context:** Data protection must understand the creation and flow of data within the cloud, through collaboration and inter-cloud sharing.
2. **Device context:** IT needs the ability to understand whether it is a personal device or one which they control accessing sensitive data. Data loss to personal, unmanaged devices cannot be remediated.
3. **Web context:** The continuous expanse of cloud services is impossible to predict, requiring rules that manage access through web before reaching an unknown cloud destination.
4. **Unified visibility and control:** Each context in this new horizon complements the next, sharing information across devices, the web, and the cloud. Together they deliver a complete perspective for managing risk to data.

Recommendations

The force of the cloud is unstoppable, and the dispersion of data creates new opportunities for both growth and risk. Security that draws closer to data—creating a spectrum of controls from the device, through the web, and to a new cloud edge—provides the opportunity to break the paradigm of network-centric protection. We recommend the following steps to break this paradigm at your own organization:

1. **Evaluate your data protection strategy for devices and the cloud:** Consider the difference between a disparate set of technologies at each control point and the advantages of merging them for a single set of policies, workflows, and results.
2. **Investigate the breadth and risk of "Shadow IT":** Determine your scope of cloud use, with a focus on high-risk services. Then, move to enabling your approved services and restricting access to those which might put data at risk.
3. **Plan for the future of unified security for your data:** Context about devices improves security of data in the cloud, and context about the risk of cloud services improves access policy through the web. Many more efficiencies apply, while some are yet to be discovered. These control points are merging to deliver the future of data security.

Only 31% of companies said their cloud security tools could enforce the same DLP policies at their devices, network, and cloud services.

Learn More

For more information on cloud security technology, please visit the following links:

- Cloud Access Security Broker (CASB) solutions
- Device Data Loss Prevention (DLP) solutions
- Secure Web Gateway (SWG) solutions
- Unified Cloud Edge technology

Ready to begin? Contact McAfee for a personalized assessment of cloud usage in your organization.

Methodology

To bring you these findings, we surveyed 1,000 IT professionals in 11 countries selected to represent a diverse set of industries and organization sizes. These results were used in comparison to aggregated, anonymized cloud usage data for more than 30 million McAfee® MVISION Cloud users worldwide who collectively generate billions of unique transactions and policy events in the cloud each day. Both of the data sets represent companies across all major industries, including financial services, healthcare, public sector, education, retail, technology, manufacturing, energy, utilities, legal, real estate, transportation, and business services. Data about cloud provider security was derived from an over 260-point assessment of more than 30,000 cloud services in the MVISION Cloud registry.

1. https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-adoption-risk-report-business-growth-edition.html
2. https://www.zdnet.com/article/44-million-microsoft-users-reused-passwords-in-the-first-three-months-of-2019/
3. https://cloudsecurity.mcafee.com/cloud/en-us/forms/white-papers/wp-cloud-adoption-risk-report-iaas.html

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com