Calamu™

## DATA-FIRST SECURITY:

# SECURING DATA FROM THE INSIDE-OUT

Master Guide to Understanding Modern Data Threats and How to Protect Your Business Against Data Theft and Ransomware Attacks

# Contents



# Introduction

Today's businesses operate in a data-driven culture. When analyzed effectively, data helps companies find new solutions, guide informed decision-making, provide a pulse on relationships with customers, partners, and employees, and create resiliency that enables businesses to adapt to disruptions.

While data is not typically listed on a company balance sheet, it is considered a valuable corporate asset. So valuable, in fact, that data also makes organizations a target for cybercrime. Threat actors seek access to company data to exploit it for financial gain by selling it, holding it for ransom, or weaponizing it for extortion purposes with the threat of publishing on the dark web. And the cyber threat continues to increase as businesses accelerate adoption of interconnected platforms and cloud collaboration tools.

Today's businesses need solutions that will extend the capabilities of their security stack, eliminate the threat of exposure, and ensure business continuity daily and in the event of a breach. This guide explores how a data-first approach to security addresses today's biggest challenges.

Calamu™

# Understanding Data

### METEORIC RISE

The data produced and maintained by organizations is growing. IDC estimates that the compound annual growth rate (CAGR) of global data creation and replication is 23%.[1] By 2025, an estimated 175 zettabytes of data will exist around the world. Business is the biggest producer, managing around 50 terabytes at the SMB level[2] to upwards of 2.02 PB at the enterprise level.[3]

Corporate data can live in a variety of locations including internally managed servers and data centers, cloud repositories, third-party environments, edge and remote locations, and others. And data is produced from a variety of sources, not just from customer interactions or shared working files but also from the equipment businesses use such as smart IoT devices and from daily social media interactions. With the rapid growth of data produced daily, the challenges to businesses of all sizes are many, from storing and effectively analyzing data to complying with regulations. Yet chief among the modern challenges is securing the data. Today it is estimated that a business is breached every 11 seconds[4] with the goal to gain access to corporate data. To understand why, let us first understand the modern data environment by answering some common questions:

**23%**

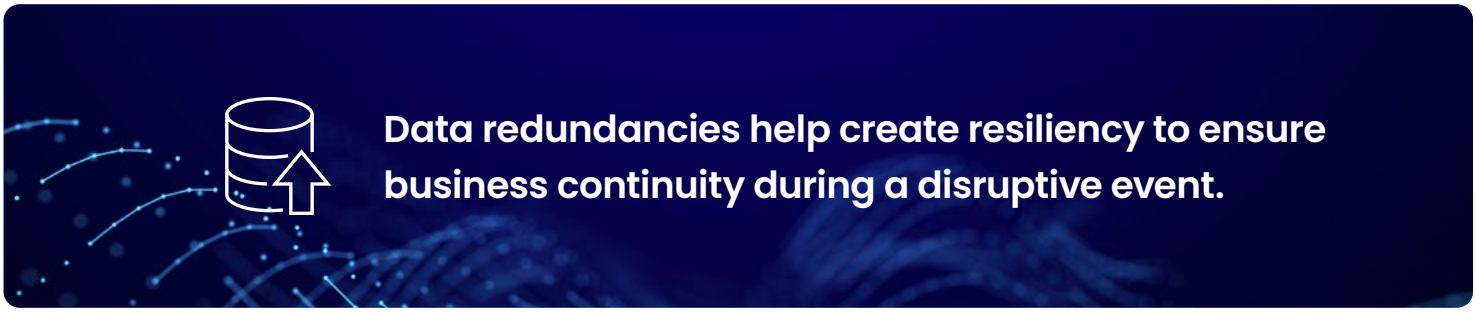
**The compound annual growth rate (CAGR) of global data creation and replication**

**175 Zettabytes**

**of data will exist around the world by 2025**

### 1. Why is data valuable to an organization and how is it being used?

Data is an extremely valuable asset to an organization. It helps businesses identify new opportunities to create revenue streams or find new solutions to increase operational efficiencies. It also helps businesses understand and keep a pulse on their interactions with the community of customers, prospects, employees, and partners. Data provides the backbone of how an organization differentiates itself to compete in the marketplace through research and the intellectual property it holds.

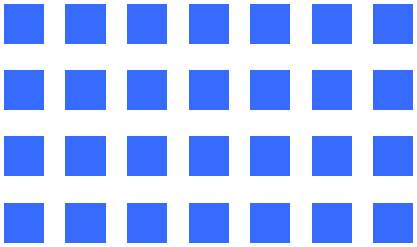



[1] IDC
[2] Smallbiztrends.com
[3] ZDNet
[4] Cybersecurity Ventures

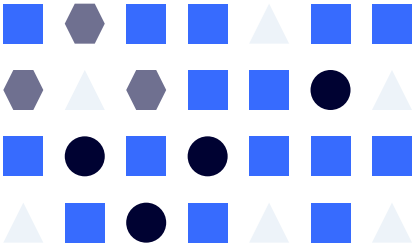
## 2. What types of data do businesses produce?

Data has three main classifications based on how it is organized:

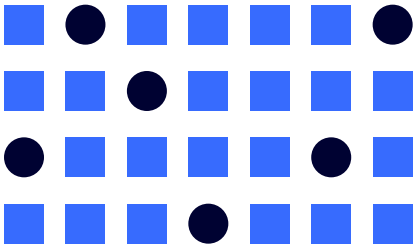
**STRUCTURED DATA**
Highly organized and easily searchable through a relational database such as the information that lives inside a customer relationship management (CRM) software.



**UNSTRUCTURED DATA**
"Everything else" - documents, spreadsheets, presentations, text files, mobile activity, social media posts, etc. This type of data cannot be analyzed or processed in a structured way.



**SEMI-STRUCTURED DATA**
Data that does not have a predefined data model but can still be categorized and searchable using metadata, such as tags.[5]



**Unstructured data accounts for over 80% of all enterprise data and 95% of businesses report prioritizing unstructured data management.**

Just as data is classified by its structure and type it is also defined by its movement. This state changes as organizations access and work with their data:

**DATA AT REST**
Data in storage that is not currently being accessed or transferred.

**DATA IN MOTION**
Data that is moving between locations or computer systems via email or file storage services.

**DATA IN USE**
Data that is being used and updated.

### What does having a "multi-cloud" strategy mean to you?

Let's agree that having SaaS products is not part of this definition, and the focus is on IaaS/PaaS public cloud providers. (eg GCP, AWS, Azure, Alibaba).

| | |
|---|---|
| 41% | You simply have more than one cloud provider configured and available for use with no specific workload-based strategy. |
| 26% | You are using a "best of breed" approach and running workloads where they most optimally run. |
| 20% | You are "cloud agnostic" and using the lowest common denominator (think container) with a focus on portability across two cloud providers. |
| 13% | You are running the same workload as active/active across two cloud providers. |

N=153 Technology Leaders | Powered by www.pulse.qa

[5] IBM

## 3. Where does data live?

Most data needs to remain accessible for employees to use and update on a regular basis. It also needs to be accessed by various departments that may be geographically dispersed. This is why so many businesses are turning to cloud storage and hybrid solutions. Microsoft estimates that only 27% of enterprise workloads remain in on-premises storage locations.[6] Not only are businesses moving toward cloud storage options, but they are also adopting a multi-cloud framework. A recent Flexera survey showed that 89% of respondents have a multi-cloud strategy.[7]

**89%**

**of respondents have a multi-cloud strategy**

[6] Microsoft
[7] Flexera

# Modern Data Challenges

### 1. SECURITY VERSUS ACCESSIBILITY

The rising complexity of data management brings with it many security challenges. Data—no matter its organizational structure, status, or location—needs to remain secure and within the confines of the organization's perimeter. Yet at the same time, data needs to remain accessible for daily usage to maintain business operations. The challenge to secure corporate data while keeping it readily available to employees has been magnified in recent years due to the shift to remote work environments.

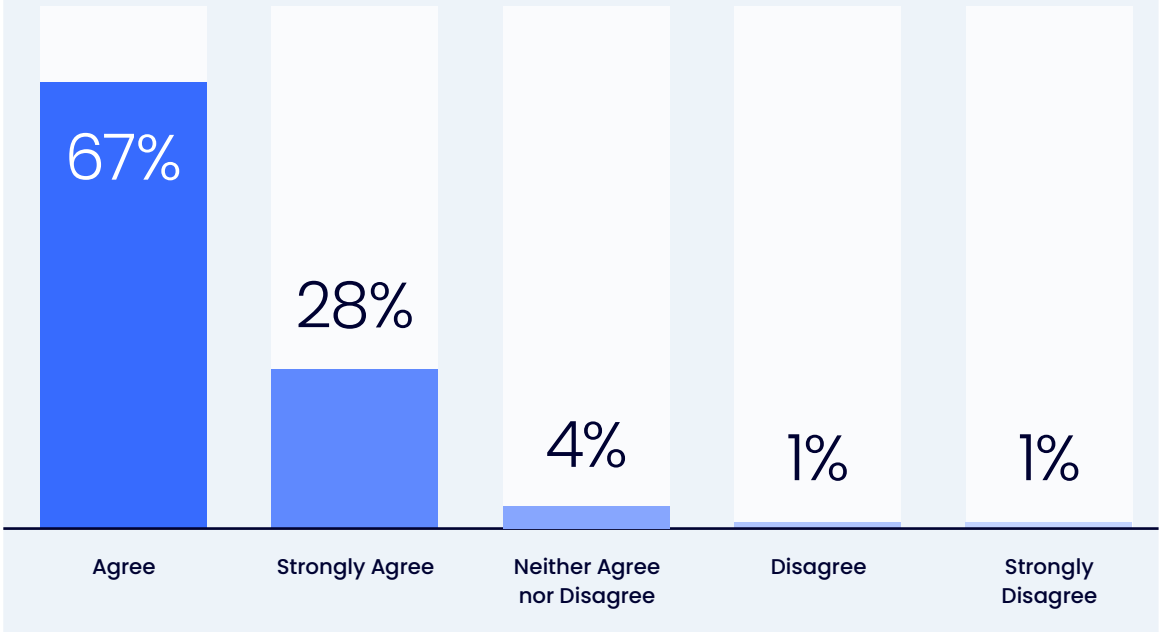
### 2. DATA ACCESSIBILITY AFTER A BREACH

The challenge of data accessibility does not just pertain to accessing files daily. Companies need to ensure business continuity in the event of a data breach or cyber incident by providing access to critical data.

### 3. CREATING A BACKUP...AND SECURING THE BACKUP

Data backups give companies a false sense of security. While a backup can be a lifeline for businesses to ensure continuity in the event of a breach or natural disaster; they are not, inherently, immune to ransomware themselves. In fact, data backups are becoming a primary target for ransomware and other attacks,[8] and 70% of businesses in a recent Calamu-sponsored survey agree that it is time to get prepared for attacks that target data backups. So, while companies need to adopt backup and recovery strategies, they also need to ensure the safety of those backups and test that safety regularly.

**Organizations should prepare for ransomware that targets backups.**




[8] SC Magazine

### 4. COMPLIANCE

Governments continue to impose compliance requirements on corporate data management, and non-compliant companies can face heavy sanctions. In addition, companies that experience a data breach may have duties to report the breach depending on their geographical location, and they may need to prove they followed proper security due diligence before and after an incident.

### 5. KEEPING AN AUDIT

To secure data, organizations need to know what they are securing. It is best practice for companies to create an audit and update it regularly including the amount of data, types of data, where it lives, and access rights to the most sensitive information. This audit will be important in the event of an outage or breach and should be standard practice as part of a recovery plan.

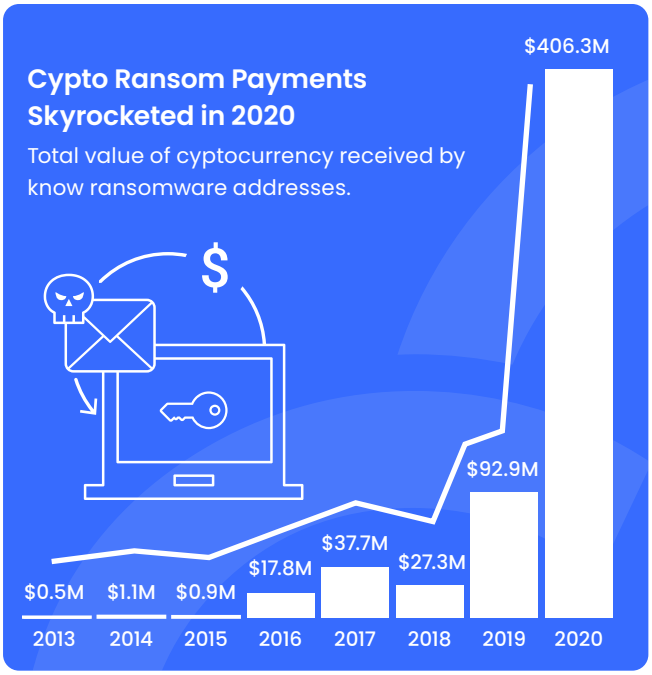
### 6. STAFF, BUDGET, AND RESOURCES

Of course, all the challenges listed above require resources, including staff to monitor and manage the data security and update the audit, as well as resources and budget to house the data and secure it properly. With the growing level of sophistication, many businesses, particularly SMBs, are turning to managed service providers for outsourced help.

# The Evolving Threat to Data

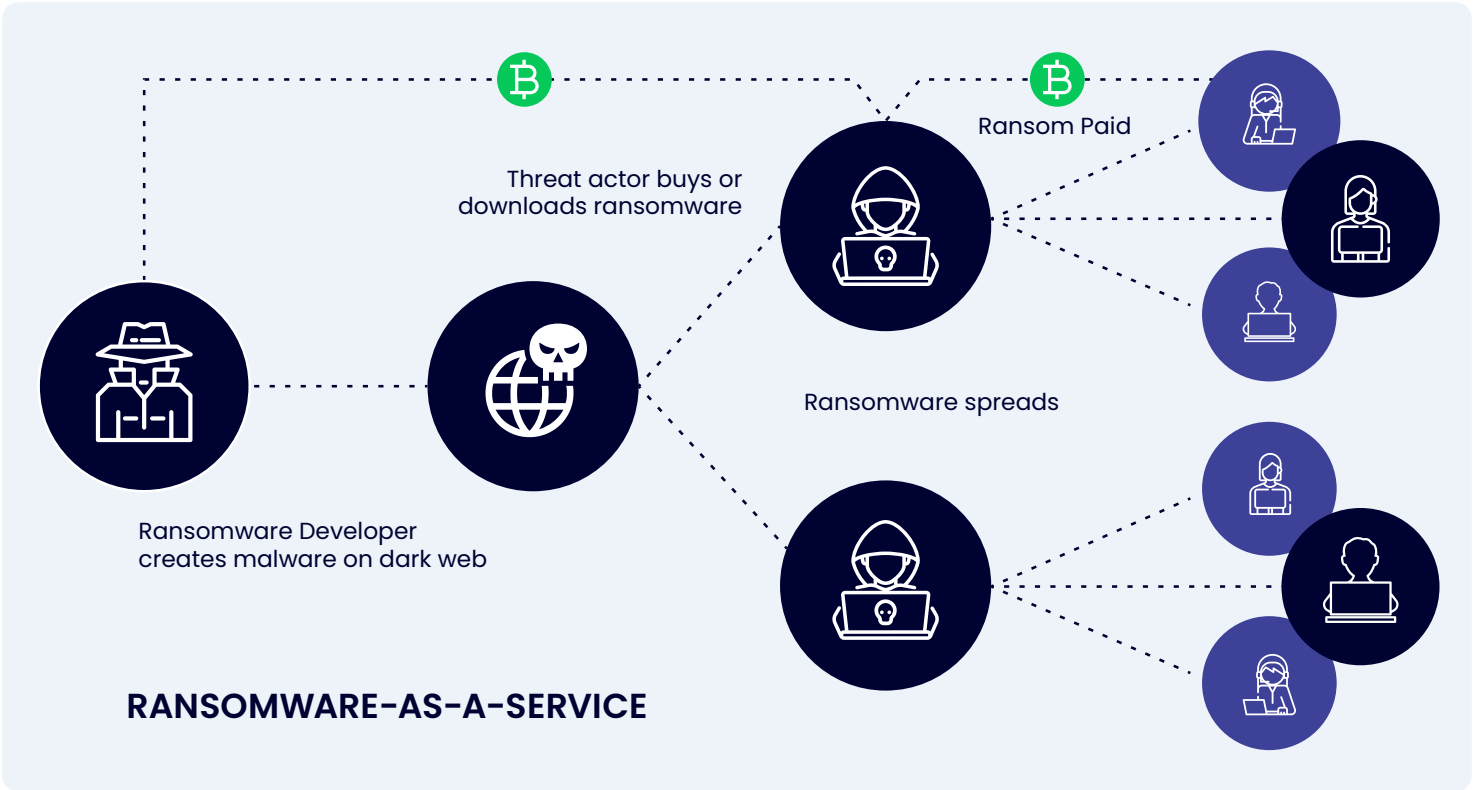
## The Turning Point for Ransomware

Ransomware saw a boon year in 2020 with ransom payments skyrocketing from $92.9M in 2019 to $406.3M by the end of 2020,[9] and this increase can be attributed to several factors:




First, the global pandemic forced businesses into remote working environments, many before they were fully prepared to do so. Misconfigured remote settings, particularly RDP (remote desktop protocol)[10] created new attack surfaces for threat actors. Misconfigured network settings are one of the leading causes of a data breach. This coupled with lax BYOD (Bring Your Own Device) policies and a loss of general control over the company network contributed to a rise in attacks.

Second, ransomware groups beefed up their business operations. Ransomware-as-a-service outsources the business operations of collecting payments and providing decryption keys to victims through a distributed affiliate network and botnets enable ease of deployment for that network. The affiliate model frees up the ransomware developer's bandwidth to focus on further refinement of their craft, including researching and exploiting vulnerabilities, devising methods for in-depth targeting, and writing more sophisticated attacks.




[9] Statista
[10] Dark Reading
[11] Checkpoint

Third, ransomware gangs flipped the script with multi-stage extortion attacks. In a basic ransomware attack, malware spreads through an organization's network and encrypts the files it can access. This type of attack is easily remedied by restoring data from backups. However, in a modern exfiltration attack, a copy of those files is first stolen, or exfiltrated, by the attacker prior to encryption, thereby increasing their leverage. Companies that choose not to pay the ransom risk having their stolen data published to the dark web. This tactic was first seen in late 2019[11] but proved to be highly effective, such that by 2022 data theft and extortion are reported in over 83% of ransomware cases.[12]

83%

of ransomware cases in 2022 were reported to use data theft and extortion to increase ransom leveage.

## DOUBLE EXTORTION EXPOSES A GAP IN THE TRADITIONAL SECURITY STACK

The changing ransomware threatscape exposed a gap in the traditional security stack. Security measures such as endpoint protection and firewalls are designed to build defenses around the organization's perimeter. Even next-generation products like XDR, MDR, and EDR[13] are built to detect potential threats with the goal to keep malware out. Meanwhile, backup solutions were designed for recovery efforts in the event of a disaster and were not inherently built for data theft detection or prevention. In this traditional model, a gap exists between the perimeter and the recovery—what happens when a breach occurs, and data is stolen?

Board rooms and governments around the world are discussing this question, yet often the discussion is around the legal and business implications of the breach, such as what and when to report the incident, cost-benefit of paying the ransom, when to activate public relations and critical response teams, and shortening downtime and recovery from the attack. Until recently there has been a gap in discussion surrounding how to mitigate the impact of the attack itself, or, better yet, eliminate it altogether.


[12] Venafi
[13] Crowdstrike

Calamu™

DATA-FIRST SECURITY:

# SECURING DATA FROM THE INSIDE-OUT

## Shift in Mindset:

## Do Not Just Recover from the Attack, Absorb It

A data-first security approach attempts to do just that, eliminate the impact of the breach. This new method for data security protects the data itself by transforming how it is stored, so that even if the perimeter defenses get breached and malware reaches the data for exfiltration, the company remains protected. This approach is not just a new technology process, it is a shift in mindset. Starting at the data level, rather than the perimeter, a data-first outlook assumes the eventuality of a breach. The goal is to turn ransomware and data breach attacks into meaningless non-events, and to do this we need to stop thinking in terms of merely handling the fallout post-breach but rather focusing on absorbing the attack itself.

Even if the data is stolen, companies that adopt a data-first security approach could carry on with ease, knowing that what was stolen is not usable to the attacker and thus removes double extortion from the ransomware toolkit.

Protecting data in this way would also solve the growing threat of attacks that specifically target data backups, mentioned in part two of this guide.

## BRIDGING THE GAP BETWEEN SECURITY AND ACCESSIBILITY

This shift starts with examining how we process data. At present, companies secure their data through a combination of perimeter defenses, detection and loss prevention, encryption, and access policies. Many companies house their most sensitive datasets—PII, intellectual property, trade secrets, etc.—in air-gapped, on-premises servers that have restricted, if any, access to the internet. The problem with this is two-fold: first, the data is not easily accessible or usable to the organization. Second, in the event of a breach, which can still happen even when the server is housed on-site under strict security,[14] the data remains in its complete state and thus readable and usable to threat actors should they reach it.

A data-first security process offers organizations immediate accessibility to even the most sensitive information while ensuring that the data remains unreadable to attackers during a breach. How? The process below outlines Calamu's approach to data-first security.

**1.**

### Secure the Data by Removing Its Value to Unauthorized Users

First the data itself runs through a multi-step process that compresses, encrypts, breaks them into fragmented pieces, and then re-encrypts those pieces using different keys. The technology that enables this process reads only the metadata and never the source data, eliminating the threat of a third-party failure point.

Next, the fragments are dispersed geographically across multiple cloud or local storage locations. The process of scattering the fragments ensures that no single location has all the fragments required to reconstitute the data (and that is assuming each fragment was decrypted against its own key before reassembly). Additionally, the fragments that comprise a data object or file are not all stored in the same repository (or even the same cloud provider), nor are they all stored in the same geographic region.

So, the data no longer exists to anyone but you, the rightful owner. No single cloud provider and no single geographic region has enough of the fragments to reconstitute the file.

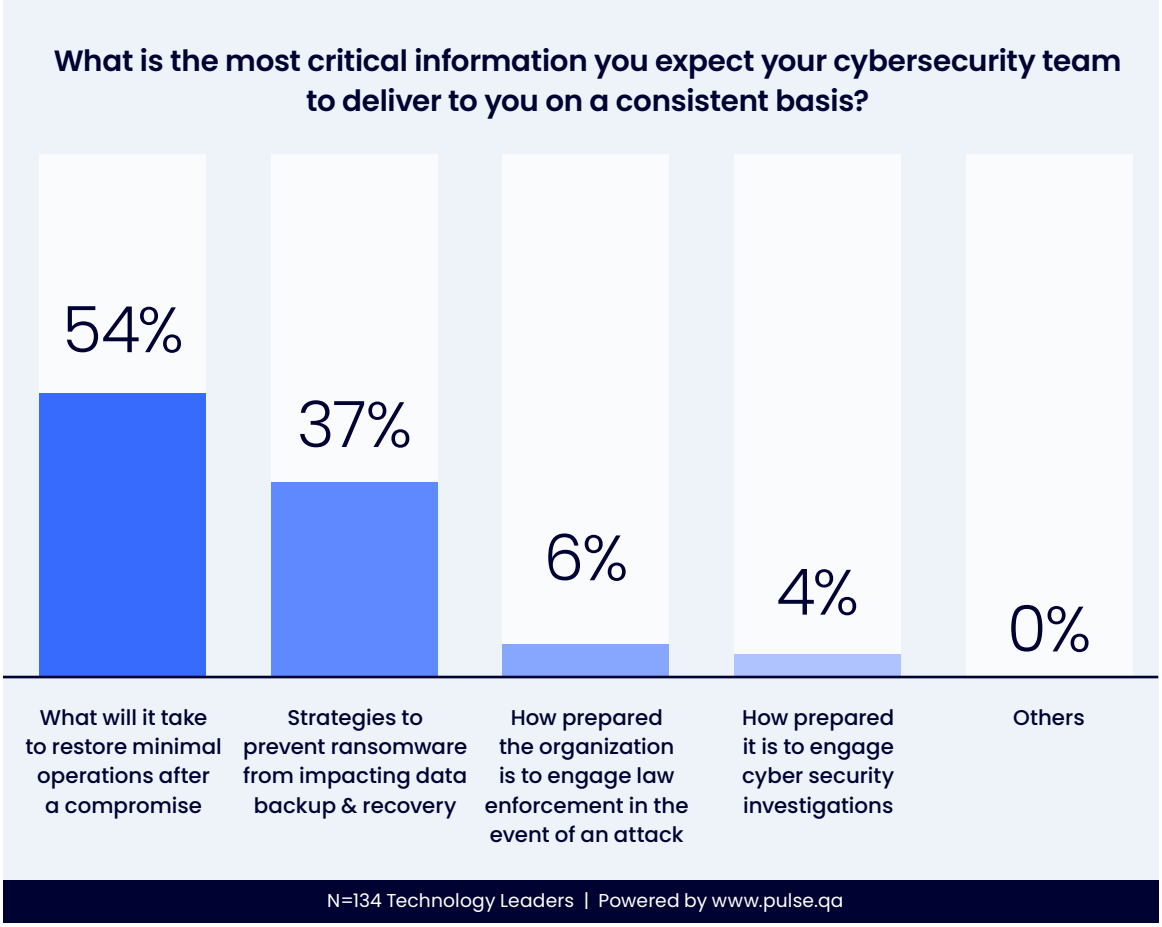
[14] Security Magazine

## 2.

### Ensure Accessibility and Performance through a Data Harbor

While the above-described process addresses the problem of securing the data, the next step is to address data accessibility. The result of this process is a virtual data harbor, a neutral environment that holds the keys to piecing the fragments back together instantaneously for an authorized user to work on before scattering the encrypted fragments back to their disparate locations. The fragments in a data harbor are immutable—meaning changes to the source data are versioned and fragments cannot be removed outside of the file versioning system itself. Therefore, stolen credentials are useless for attempts to encrypt and destroy data. However, data accessibility means nothing without speed of access.

The architecture of a data harbor was engineered with performance in mind. Tests show that it is nearly 2X faster in most cases using a 100MB file size compared to a direct cloud upload or download.[15]




[15] Calamu

## 3.

### Absorb the Attack and Eliminate Downtime

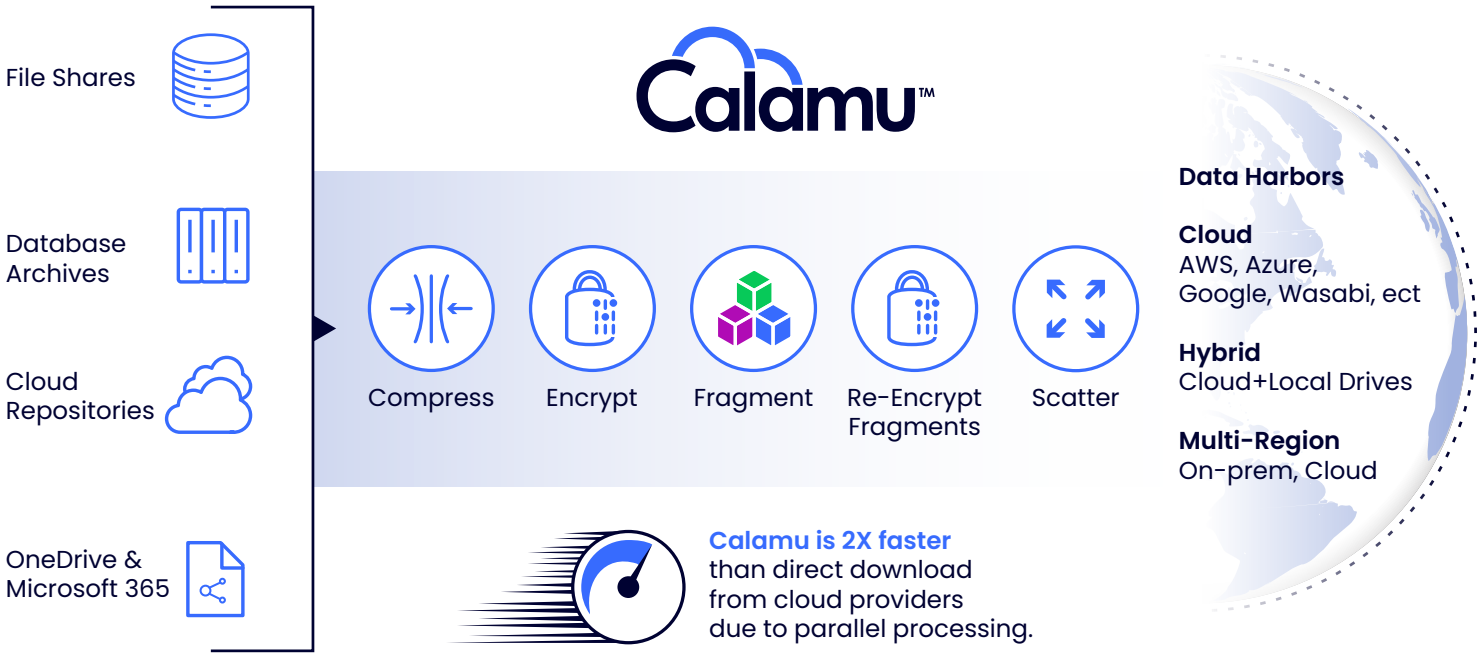
A recent Calamu survey showed that the most critical information business leaders expect to hear from their cybersecurity teams on a consistent basis is what it will take to restore minimal operations after a compromise. The traditional perimeter security model is focused on recovery efforts and shortening downtime after a breach. A data-first security approach goes one step further to eliminate the downtime.

The data harbor is built to detect an event as it occurs and self-heal instantaneously. Should an errant process, bad actor, or stolen service credentials offer unauthorized access where a fragment is modified or removed, the location immediately becomes quarantined, and the data harbor rebalances to new secure storage locations. This means that even if a breach occurs, the attack is absorbed by self-healing, and business operations can continue without downtime.

› Click here for more information on the data process and data harbor.

[15] Calamu

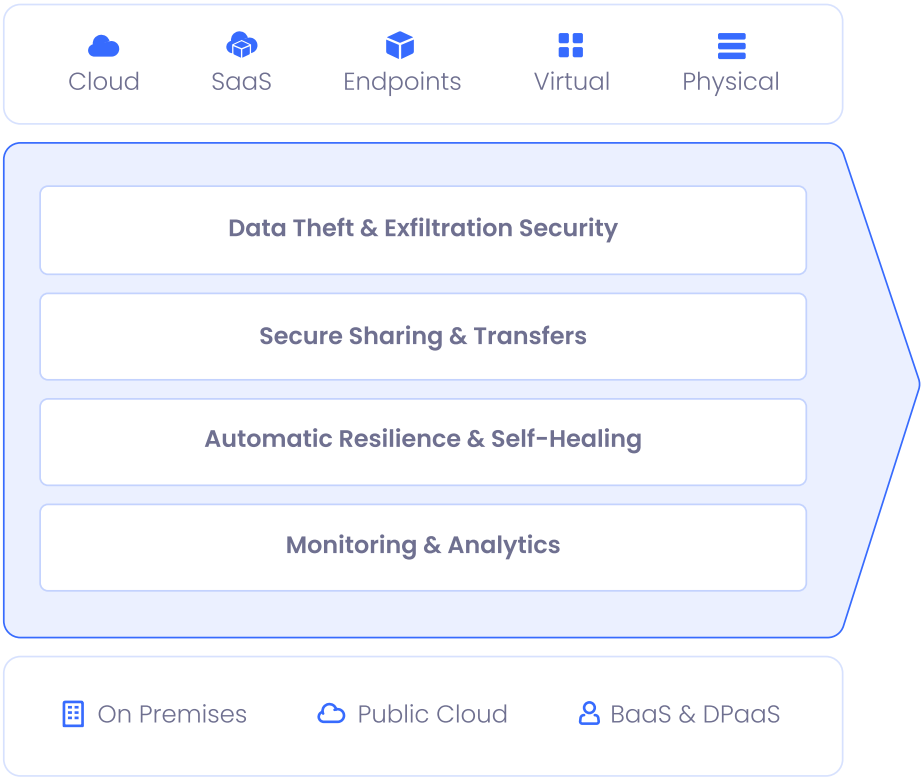
# The Calamu Process

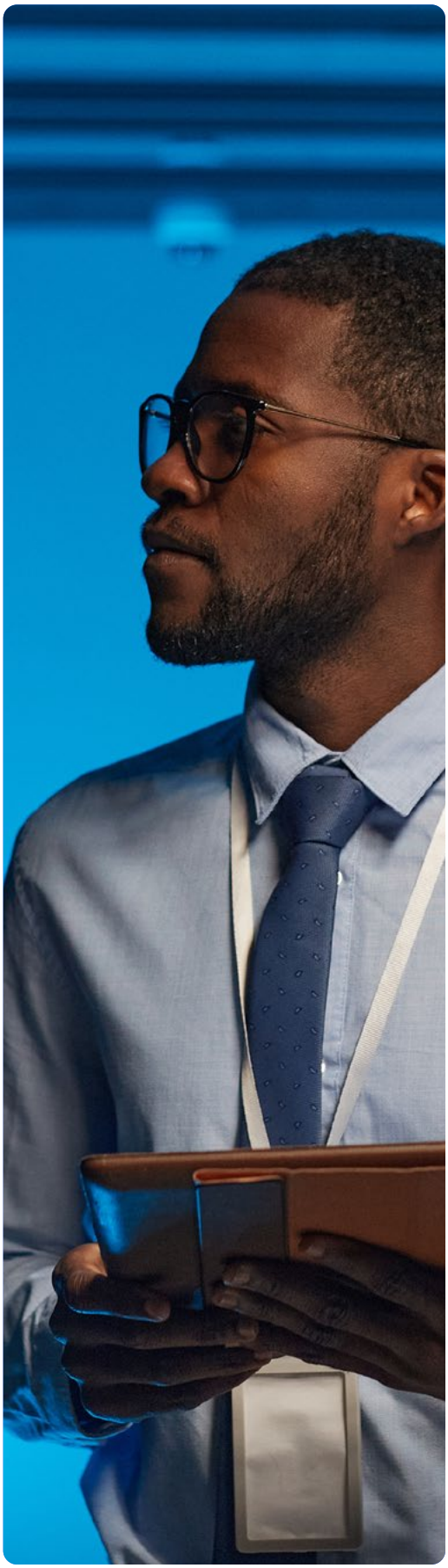



> Most organizations implement a layered, outside-in approach that includes VPNs, browser isolation, multi-factor authentication, and firewalls, yet their data can still be exposed. We offer an inside-out approach, fragmenting and encrypting files at the source and dispersing them across multiple cloud locations. Any compromised data is relegated to useless Digital Sludge.™
>
> **SIMON YELSKY**
> **VICE PRESIDENT OF PRODUCT AT CALAMU**

# Fill the Exfiltration Gap and Increase Efficiency

Double extortion and data theft exposed a gap in the security stack that a data-first solution described above is intended to fill. Yet, as security best practices state, a layered approach is always best, so it is recommended to have a data-first solution working alongside existing security defenses and recovery plans. A data-first security solution sits as a foundational layer in-between traditional security defenses, file management, and back up services.



**Adding this layer to a security plan offers:**

- Unprecedented security against data theft and exfiltration to guard against multi-faceted ransomware extortion attacks
- Secure file sharing and transfers
- Automatic breach detection and self-healing that absorbs the attack and eliminates downtime
- Granular details and control over data storage and access for increased efficiency

# Building Resilience

Recent global shifts in the way businesses operate and interface with data have introduced the need to think beyond security and recovery and start building cyber resiliency plans. The National Institute of Standards and Technology (NIST) defines cyber resiliency as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[16] From the global demand for remote working environments, to the massive shift in labor forces, and the onslaught of the current ransomware explosion, businesses need to stay agile and adapt quickly to change agents, and a data-first security approach can help achieve new levels of resiliency.

Within the NIST cyber resilience framework, five objectives are outlined: prevent, prepare, continue, constrain, and transform. [17] **A data-first security approach provides solutions to each of these objectives:**

**Prevent** - a data-first security approach focuses less on securing the perimeter and instead ensures data protection at the data level to prevent unauthorized users from extracting value from the data in the event of a breach. Preventing valuable data from theft means that even if security defenses fail, businesses stay protected.

**Prepare** - companies that prepare for the eventuality of a breach versus a fallback plan, should one occur, are better suited to recover. A data-first security approach assumes that an attack will happen and secures the data itself against theft and exposure to absorb the attack rather than simply recover from it. In addition, the access management levels that the technology provides gives the organization a full view of their data profile and full control over where data is housed and how it is used. This level of information is powerful for building and updating a data audit that is recommended for preparation. (See Ten Steps to Protect Against Today's Threats)

**Continue** - a key pillar of resiliency is the ability to continue operations during and after an attack. The traditional perimeter security outlook focuses these efforts toward reducing downtime and enacting recovery efforts. A data-first security approach, by contrast, focuses on absorbing the attack and eliminating downtime altogether. Built-in intelligence predicts when a breach is occurring and automatically self-heals the system to keep operations running. The goal is to turn ransomware attacks into meaningless non-events.

**Constrain** - effective resiliency plans focus on how to constrain the exploit and limit further damage which aligns with a data-first security approach. Through encrypting, fragmenting, re-encrypting, and scattering across multiple geographically separated locations, data sets are never fully accessible from one single location or one single decryption key. An attack on one storage location constrains the threat to that location only and data redundancies instantaneously work to recover file fragments from other locations to eliminate downtime. When an attack happens, the single most important asset is time—time to investigate, solve the problem, and secure the system. The ability to absorb and make data accessible through an attack gives the time advantage back to the business.

**Transform** - companies need to learn from cyberattacks and make changes to their operations, which requires knowledge of how the attack occurred. A data-first security approach offers granular data-level details on the incident to empower SecOps teams to learn and adjust.

> **"When an attack happens, the single most important asset is time."**

[16] NIST
[17] Developing Cyber-Resilient Systems; A Systems Security Engineering Approach

# Ten Steps to Protect Against Today's Threats

Changing a security approach or building one from the ground up can be a daunting task for many businesses. Even adding in one extra security layer or switching an existing security vendor for another takes many considerations.

**The following steps are guidelines recommended by Calamu Founder & CEO, Paul Lewis, to get started.**

**About Paul Lewis:**

Paul Lewis is a serial entrepreneur and cyber expert, having founded and led global organizations in the fields of Cybersecurity, Data Forensics, Digital Information Security, and Compliance Technology. Lewis is a contributor to the NIST Cybersecurity Practice Guide, and has advised the SEC, FBI, Department of Homeland Security, and the United States Department of Justice on emerging trends in cyber and information security. Lewis has been granted numerous patents to advance data privacy and protection, and is a court-appointed expert in data security and incident response.

**1.**

### Mindset

Shifting the mindset is important. Understanding that a cyberattack on the organization is likely is an important jumping off point. Instead of preparing to reduce the impact should an event occur, companies that understand the eventuality of an attack can look to eliminate consequences by preparing, using the data-first security approach.

**2.**

### Build a Framework

Existing frameworks around access management such as zero trust[18] and continuity plans such as the NIST cyber resilience framework are intended to help organizations approach their security plans. Develop a plan that works for your organization.

**3.**

### Audit

Take an audit of the type of data you have, how it is being used, and where it lives. Understanding the amount of data that needs to be stored and secured, and then classifying it in terms of level of sensitivity will help build out a strategy.

**4.**

### Research Innovative Solutions

The cyber security market is growing and evolving. Talk to your security reseller and research potential new solutions that will address your specific needs. Demo and test drive them to ensure they will work within your environment.

[18] NCCOE

5.

### Secure, Backup, and Create Redundancies

Secure your data with the best possible security solutions you have. Create backups and redundancies of that data. Securing data may take multiple layers including perimeter defenses and data-level solutions. A data-first solution will secure your data and create redundancies in a singular process.

6.

### Roll Out Cybersecurity Training for Employees

Even with the best defenses in place, it is recommended that all employees take regular cybersecurity awareness training and stay up to date on how the latest threats are evolving.

7.

### Update and Patch Software and Equipment Regularly

Build a plan for managing software and equipment to ensure proper care, patching, and updating occurs on a regular basis.

8.

### Review Settings

Network misconfiguration and unsecure RDP are leading causes of breaches. Review your policies and settings closely or partner with a vendor who can perform a cyber readiness audit.

9.

### Review Company Policies

Develop and review your company policies around BYOD, password hygiene particularly for mobile devices, application usage, and others.

10.

### Monitor, Analyze, and Refine

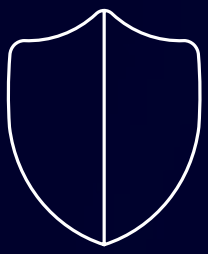
Plan for regular monitoring of system health and alert responses for cyber incidents. Study your network activity and data and refine your plan to adapt to changes.

Calamu™

# Take the next step in your data-first security journey.

**Schedule a demo today to see Calamu Protect in action and how data remains impenetrable during an attack.**

www.calamu.com/get-started



## About Calamu

Calamu was founded by experts in cybersecurity and data privacy with the mission of making the cyber world a safer place. The company is pioneering the use of data-first technology to automatically mitigate the impact of a ransomware attack or data breach, whether data is stored in the cloud or on-premises. The Calamu platform enables businesses to maintain complete ownership of their data, preventing unauthorized access and dramatically simplifying regulatory requirements around data privacy and protection.

**For more information on Calamu visit www.calamu.com.**



Calamu™