virtru

How to Create a Sustainable Cybersecurity Strategy

How a Data-Centric Approach Can Increase Agility and Strengthen Breach Preparedness

Contents

02 Introduction

04 What does it mean to be data-centric?

06 Why pursue a data-centric strategy?

08 How to get started

09 Conclusion

Contact Virtru

Introduction

As organizations embrace digital transformation, businesses are collecting, processing and storing larger quantities of data than ever before.

Accordingly, effective, sustainable commercial growth must now be underpinned by comprehensive and multi-cloud-capable data governance – an imperative set in stone by legal frameworks, such as the California Consumer Protection Act (CCPA) in the US, and the EU's General Data Protection Regulation (GDPR).

Good data governance is an enabler of trust – an equally critical factor: teams, internal and external customers rely on businesses to provide an environment that facilitates engagement without compromising on security. This compels firms of all sizes to consider how their systems can be improved to mitigate risk of data breach and respond effectively to evolving cyber threats.

To begin, leaders must recognize data protection and cybersecurity as primary drivers for successful business in this data-driven age.

"If you reorient your organization, with data positioned as the most sensitive asset, you'll make different decisions about how you implement your cybersecurity program," says Rob McDonald, Executive Vice President of Platform at global leader in data privacy and protection, Virtru.

Within a culture that champions data welfare, tools and technologies can enable intelligent data handling on a granular level. Only then can businesses build a sustainable IT infrastructure that works in an increasingly complex digital environment—remaining competitive, legally compliant, cyber-secure, and respectful to the data owners that these organizations are stewards for.

"If you reorient your organization, with data positioned as the most sensitive asset, you'll make different decisions about how you implement your cybersecurity program."

What does it mean to be data-centric?

Traditionally, business security has come through a perimeter defense strategy, comprising a range of entities from basic firewall protection, through to end-to-end network security that wrap around the business network.

This 'cookie jar' structure was designed to stop malicious attacks or potentially infected data from getting into the IT infrastructure. However, the single layer of defense meant that, should the perimeter become breached, then everything inside potentially becomes compromised.

This, the popular choice over recent decades, simply isn't fit for purpose in a digital era defined by multi-cloud and distributed environments that have accelerated cybersecurity complexity. However, if organizations protect data at the object level—securing each individual file, email or other data asset with its own layer of encryption—the perimeter isn't such a critical vulnerability. Each data object remains protected, everywhere it travels—and if the perimeter is breached, each data object inside remains protected with its own layer of security.

As businesses get to grips with what's at stake, we are witnessing an undeniable shift towards a safer, more future-proof mindset that can deal with cyberattacks of increasing sophistication.

"The cybercriminals and systems involved are so sophisticated that it's impossible to stay protected with the perimeter approach. In the last two years, we've seen a significant uptick in the switch to data-centric strategy," says Rob.

The data-centric approach

Instead of prioritizing security controls for hardware and IT infrastructure, a data-centric approach focuses on safeguarding data where it is stored and processed.

From this position, the business is able to leverage that data, make more intelligent decisions and drive greater value through every facet of the firm. The eventual result is a healthy, sustained data environment that can save money and drive productivity.

When applied to data protection strategy, being data-centric involves making decisions about your overall information security and information management posture by using the data itself as the north star to guide your approach.As such, the degree to which you value your data will inform how your security and training programs develop.

From a technical point of view, being data-centric opens up an opportunity to re-examine technology vendors through a new lens:

Which vendors will partner with you to drive your business forward with this framework? Will they equip your employees with the combination of flexibility and security needed to foster innovation? Which vendors will you trust to protect your organization's most vital data and uphold data integrity? At the end of the day, it's up to you to determine what capabilities you truly value to support the future of your organization.

Ultimately, a company needs to ensure that whenever data is used, technical controls are in place to monitor requests, govern access, and control levels of protection at all times.

> ***"There's both a strategic and a technical aspect to becoming data-centric. Some organizations will do one better than the other, but both aspects are interrelated and both are essential as part of a holistic data-centric program," says Rob.***

Zero Trust within a data-centric environment

In practice, Zero Trust understands that when an exchange of information takes place, trust does not play a part in the movement of data from one juncture to the next. In place of trust comes the guarantee that data integrity and data security will be upheld at all times, because all traffic is validated.

A Zero Trust approach to security, therefore, begins with the assumption that a data breach will happen. Security levels then depend on the context of the data being protected, its value, and the compliance controls surrounding that data, allowing for appropriate local and technical protection to be implemented.
Zero Trust is especially decisive as a protection culture because of the sheer number of facets within a modern business, each of which has a stake in data privacy—from people, documents and network switches, to firewalls and computers. If one person conducts a data exchange, that data may travel through five or six different entities: for example, from a device, through a network to another network, through a cloud vendor, and beyond.

Through authorization and authentication enabled by a data-centric approach, businesses can develop cybersecurity in a way that engenders Zero Trust effectively at every stage in the data journey.

As detailed by the National Security Agency, key principles of Zero Trust are as follows:

- "Never trust, always verify: Treat every user, device, application/workload, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies."
- "Assume breach – Consciously operate and defend resources with the assumption that an adversary already has presence within the environment. Deny by default and heavily scrutinize all users, devices, data flows, and requests for access. Log, inspect, and continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity."
- "Verify explicitly – Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources."

Why pursue a data-centric strategy?

A data-centric approach is more relevant than ever.

A marked increase in cyberattacks brought on by the pandemic is just one of a number of driving forces behind the need for stronger cybersecurity today.

Compliance with evolving data law, the obligation to optimize data governance, and the need to exploit big data and tech trends such as AI, also help to explain why the data-centric security market is forecast to reach $7.3 billion by 2025.

A data-centric approach allows businesses to reduce cyber threats and overcome barriers to growth created by more traditional approaches to security, suggests a Capgemini and Forrester study titled Making Your Business Cyber-Resilient In 2021.

Below, we take a look at some of the key business benefits a firm can expect to unlock by following a data-centric strategy.

Empower employees, unleash productivity and collaboration

Through data-centricity, the data itself is protected, removing the inherent concerns surrounding working from home and other growing working trends. Improved cyber-resilience means employees can share data with confidence, pushing up productivity and encouraging faster, more coherent working behaviors throughout teams and with partners.

“Through building collaboration and innovation, the data-centric approach is becoming decisive in a company’s ability to attract and retain talent,” says Rob. “When employees are empowered to collaborate more freely, they can innovate much more effectively, as well as bring new products to market faster, creating a more positive and, ultimately, successful work environment.”

Cost savings

The data itself is the most sensitive element that perimeter-based solutions are engineered to protect. However, a data-centric approach cuts out the middleperson to implement a more pragmatic, robust take on cybersecurity that can adapt to an ever-changing threat landscape.

Embracing data-centric models also delivers value because they improve application, tool and device visibility across a business.

Data-centric security adapts to context, forging a smarter allocation of resources that promises financial savings in the long term. On the other hand, failure to re-architect your IT cybersecurity environment by adjusting to a data-centric approach will bring greater financial burden as protection needs evolve and become increasingly nuanced.

“By investing in data-centricity, you’re creating a more sustainable strategy in terms of protecting your data. You’re doing something that will transcend the coming changes in technology because the common denominator will always be the data itself.”

Protect data as it travels through the supply chain

Organizational data has typically been protected in very segmented ways, with application encryption, database encryption, and other technologies contributing to an approach for which a number of different groups within an organization are responsible.

The data-centric approach ensures appropriate, top-level protection for data, whether it is in storage, being processed or travelling through supply chains. This guarantees the best protection for your business and its partners. For greater protection, companies can tag their data in a way that supports access governance in accordance with users’ roles and credentials, known as attribute-based access control (ABAC). Governing data in this way assures that data is accessed on a “need to know” basis.

Future-proof your tech stack

“By investing in data-centricity, you’re creating a more sustainable strategy in terms of protecting your data. You’re doing something that will transcend the coming changes in technology because the common denominator will always be the data itself,” says Rob.

In the same way, a business that embraces data-centricity can expect to stand up stronger in the face of cyber threats as they evolve. This dynamic, robust posture offers a far better ROI as your business grows. Over time, as more data-centric investments are adopted, the future-proofing of the technical stack will have a measurable reduction in total cost of ownership.

“A lot of CSOs are rethinking their technical spend as they realize their stack isn’t as effective as they had hoped,” says Rob.

Data-centric culture and associated efficiencies will also become a positive differentiator. Forward-thinking companies have the chance to demonstrate data governance proficiency, enhance trust and boost their following.

“Data-centric adaptation itself becomes a competitive edge,” Rob adds.

How to get started

“Taking a whole new approach to protecting data can seem daunting and the danger is that people simply fall back into what they’re comfortable with, which are existing solutions,” says Rob.

The journey begins by knowing what data you have, where it lives and how to access it.

> Checklist for a data audit

Your business may have data assets residing in multiple locations, through different software, apps, servers and programs. Make a list of the data assets you have and who within your company has access to them—including third parties.

If you are not able to speak to individual employees, then discuss with team leaders or department heads about what data individuals use and have access to. Ask where this data is located, how much of it workers actually need to do their jobs and what problems they may encounter with that data.

> Prioritize data protection needs across the data life cycle

Determine the role each type of data plays in your organization. Ask what purpose the data serves, then decide whether it needs to be held elsewhere to improve organizational alignment.

“It’s so important to just step back and simply look at what does or doesn’t work. Once you have that rationale, you can begin to get others to buy into the importance of what you’re trying to achieve,” underlines Rob.

Prioritization of the data is key here. For example, an online retail store would attach importance to email addresses and mailing addresses, while a direct marketing firm might solely prioritize mailing addresses. Furthermore, different departments within an organization may have different interpretations of the same data: What the marketing department considers sensitive may differ from what finance or sales views as sensitive. Having cross-functional input into this process ensures that data is treated with necessary care and serves all areas of the organization. Once data has been mapped, think about the value it brings to key players and how it drives profit. You may find that your business has been storing customer dates of birth for ten years, when there’s really no need. Such storage simply pushes up costs, soaks up resources and increases risk.

Delete old, unused or non-compliant data wherever possible, then consider where greater or fewer protection measures are needed according to your business mission. This will allow you to strategize storage, discovery and cybersecurity more effectively.

> Select partners who can help you implement and grow your strategy over time

The next step is to implement policies across the business, through systems, networks, applications and products.

“The priority here is to give the right tools to your staff and partner ecosystems to get the job done. An inventory of tools and environments will be required to fulfil the value promised to customers, partners and other users,” says Rob.

When the right policies are in place, a business can go to market to try to find the best security solutions according to needs, looking at vendors that are taking the zero-trust approach.

Encryption or tokenization should be used to protect the data, but a solution should also allow access to deprotected data based on pre-established user rights that allow access to sensitive information on a need-to-know basis.

Finally, consider which regulatory environment you will be aligning to – whether that’s NIST, or a similar body that will continuously contribute Zero Trust frameworks and security models to which you subscribe.

“We’re seeing more vendors than ever adopting Zero Trust standards and protocols. There’s nothing more accelerating than that from a legacy application perspective, because an adoption path is being created. CISOs are seeing that they can actually do this,” says Rob.

Conclusion

“Data-centric concepts and standards have never been more important,” Rob reminds.

When a business understands that data protection is top of the cybersecurity agenda, it can begin to move away from the antiquated cultures and mechanisms that only serve to increase corporate risk in the digital era.

By embracing a data-centric strategy, data becomes managed in a sensitive, granular way, making it far easier to navigate ever-present cyber threats.

In a more intelligent, sustainable IT environment that pays for itself over time, cybersecurity strategy actually nourishes innovation and drives healthy business growth.

About Virtru: Your Partner in Implementing a Data-Centric Strategy

Virtru is a global leader in data protection and privacy, equipping enterprises with flexible, end-to-end data encryption solutions that protect emails, files, databases, video, and more.

Virtru’s tools are easy to use and integrate seamlessly with Gmail, Outlook, Google Workspace, as well as enterprise apps such as Salesforce, SAP, and Zendesk. Additionally, with features that include access controls, key management, DLP rules, and persistent audit, organizations are able to meet privacy and compliance requirements like GDPR, HIPAA, ITAR, and CJIS.

To see how you can take full control of your organization’s data, everywhere it’s shared, contact Virtru to start the conversation today.

Contact Virtru