Why Data is the New Edge

SECLORE™

Introduction

Collaboration drives modern business. Whether working with partners, vendors, or remote employees spread around the world, your focus is on making the collaboration touchpoints as seamless and secure as possible. But, while eliminating costly collaboration friction across boundaries, you must do so without risking the privacy and integrity of your business data. Data protection is more important than ever, but traditional methods are no longer sufficient. You can't go backwards; you can't close the barn doors. Instead, you need to think differently about data protection without encumbering collaboration.

In this white paper, we will explore why the flow of data fueling modern business has effectively made the traditional edge of your network—the datacenter perimeter—obsolete. How data itself has become the new edge and why now is the time to rethink data protection for your business. We will also offer practical solutions for protecting your data in this new environment. By understanding the changing nature of data protection and taking action to adapt, your business can continue to collaborate and innovate without risking the security of your data.

The Data Protection Catch-22

Data is the lifeblood of any organization. It is the driving force behind nearly every business decision and action, and it is vital for the successful operation of any company. However, in order to make the most of this valuable asset, organizations must engage with a wide variety of collaborators, both inside and outside of the traditional boundaries of the business.

The rise of the cloud and the globalization of work has only accelerated this trend. Organizations are now expected to seamlessly share and access data with a wide range of "trusted" parties. Unfortunately, this free flow of data comes with its own set of challenges and complications.

Organizations must protect their digital assets—such as intellectual property, customer data, and go-to-market plans—to safeguard their competitive advantages. Furthermore, every business faces a host of regulations and mandates that require stringent control over access to data. Lastly, in order to stay agile and responsive to changing market dynamics, organizations must be able to quickly and effectively react to new cyber threats and business challenges.

This situation creates a data protection “Catch-22". On the one hand, they must eliminate friction in the flow of data in order to remain collaborative, competitive, and successful. On the other hand, they must implement safeguards to protect against potential risks and unintended data exposure. Finding the right balance between these two competing priorities is a daunting task, and one that many organizations struggle with daily.

The reality is that, even with the best intentions and efforts, organizations can no longer completely control their data. The genie is out of the bottle and trying to put it back is simply not feasible. Implementing overly restrictive controls on the flow of data can have the opposite of the desired effect, as users will always find ways around these restrictions if it means they can get their job done.

The key is to strike the right balance between removing friction and providing safeguards. By carefully evaluating the risks and rewards of different data sharing strategies and implementing the right processes to protect against potential threats, organizations can continue to reap the benefits of a free flow of data without exposing themselves to unnecessary risks.

How Did We Get Here?

Over the course of human history, data has always been central to business success. From the earliest days of commerce, when trade was primarily conducted with physical goods, data was collected and used to make decisions and drive actions. However, the way data is created and shared has changed significantly over time.

Business Data Across the Ages

In the “stone age” of data, data was physical, and paper based. Distribution was limited by the literal boundaries of the world. Filing cabinets and locked doors were the primary means of keeping data safe and secure. The effort required to collaborate was non-trivial and the speed at which it could be transmitted beyond a data owner’s control was slow due to its physical nature.

In its “industrial age”, data traveled on the backs of other mediums—such as faxes and as email attachments—but this was still a cumbersome and slow process. Distribution was point-to-point and often required specialized hardware (like a fax machine). The scale and ease of collaboration may have increased, but limitations remained. This friction gave many a false sense of control.

The onset of the internet age made data more portable and easier to share. The growth of new cloud services enabled business collaborators to access and share data from practically anywhere in the world. However, platforms like Dropbox and OneDrive also introduced their own challenges and complications requiring workarounds. Different systems and formats have made it difficult to seamlessly collaborate and share data.

Now, we are entering the age of data enlightenment, where data is the medium itself. With advancements in cloud file formats and related technologies, data can flow more freely, and collaboration can happen in real-time. However, with this new freedom comes with the real risk that the right data can easily end up in the wrong hands. Or worse, the vital business data is no longer easy (if not impossible) to safeguard.

Whether we like it or not, our data is on the move. And while this may be a daunting prospect for some, it is ultimately a good thing. As data becomes easier to share and access, businesses will be better equipped to make the most of this valuable resource.

By embracing this new reality and finding the right processes to protect their data, organizations can position themselves for success in an increasingly data-driven world.

Striking the Right Balance Between Control and Collaboration

The criticality of and risks associated with data collaboration are clearly not a new phenomena for business success. What has changed is the sheer scale and blast radius. It's the escalating risks and demands that requires that we think differently about how to protect and control this valuable asset.

The reality is that we can no longer rely on the traditional boundaries of networks and devices to keep our data safe. The rise of the cloud has effectively eviscerated these borders, and businesses must always assume that their data is at risk of exposure, whether malicious or accidental.

Shortcomings of Common Data Safeguards

Data encryption has long been seen as a proven means for protecting vital data, but it is increasingly clear that this approach alone has limitations. Encryption can be incredibly complicated for the average knowledge worker. Even the smallest mistake can have disastrous consequences. For example, if encryption keys are misplaced or forgotten, the data could be lost forever. On its own, encryption is a blunt instrument that often adds unnecessary hurdles to the flow of data.

Reactive controls, such as data loss prevention (DLP) and cloud access security brokers (CASB), can also be useful for protecting data. However, these tools are often cumbersome to deployment, too slow to be effective, and can do little to protect data that has already been shared outside of an organization's immediate control.

Given these shortcomings, we need to change the way we think about data protection.

Data is the New Edge

As we have seen, the traditional approaches to data protection are no longer sufficient to keep our valuable data assets safe and secure. The rise of cloud computing, the proliferation of devices, and the increasing importance of effortless collaboration have all combined to create a new set of challenges and complications when it comes to data protection.

Rather than relying on reactive controls and complicated encryption schemes, businesses must shift to a proactive data protection approach.

Instead, organizations need to implement processes and tools that:

- Enforce appropriate business use
- Uncover unauthorized or unapproved use
- Maintain security controls even after data has been shared
- Revoke access when conditions change

The answer to these problems is to move the protection and control of data to the data itself. By adopting this approach, organizations can create an effective boundary around their data that carries and maintains usage policies and security controls. This new boundary can travel with data wherever it goes and is agnostic to the medium through which data is shared (such as email or file shares) and the location where it is stored (whether on-premises, in the cloud, or with a third-party). It also compliments other security controls and policy enforcement for defense-in-depth.

Just like devices and applications are embracing a zero-trust security model, the same methodology can be applied to data. This means that organizations can trust but also always verify who has access to their data and apply fine-grain and dynamic policies to ensure that only authorized users can access the data. Furthermore, organizations can confidently revoke access rights when no longer needed or if circumstances change—regardless of where the data is located—eliminating the common challenges of “all or nothing” access.

By embracing this perspective, organizations can gain significant business benefits.They can protect against threats, achieve regulatory compliance, and remove collaboration friction without fear.

As an added benefit, organizations can accelerate their digital transformation efforts without leaving anyone (employees, partners, or customers) behind, confident in the knowledge that their data is safe and secure, no matter where it is located or who has access to it.

Achieve Data-Centric Security

Data will continue to be the increasingly valuable lifeblood of any organization. In order to protect this valuable asset, organizations must think differently about data protection. Rather than relying on the traditional boundaries of networks and devices, organizations must move the protection and control to the data itself. By embracing data as the new edge, organizations can create a boundary around their data that carries and maintains usage policies and security controls.

Seclore is the world leader in data-centric security and has helped over 1,000 companies across a wide range of the most sensitive industries (financial services, manufacturing, public sector, telecom, etc.) successfully transition to this new model. By implementing new concepts pioneered by Seclore, these companies have protected their data, achieved regulatory compliance, and eased collaboration friction without fear.

If you're ready to start now and take steps to make your data security independent of your infrastructure security, contact our team for more information.

SECLORE™

About Seclore

Protecting the world's sensitive data wherever it goes. Seclore protects and controls digital assets to help enterprises close their data security gap to prevent data theft and achieve compliance. Our data-centric approach to security ensures that only authorized individuals have access to sensitive digital assets, inside and outside of their organization. Enterprises can set automated policies and enable users to control and revoke who has access, what access they have, and for how long. Learn why leading enterprises like American Express and Applied Materials choose Seclore to protect and control their digital assets without sacrificing seamless collaboration and data sharing.

Visit **www.seclore.com** for more information.

5201 Great America Parkway
Suite 440
Santa Clara, CA 95054