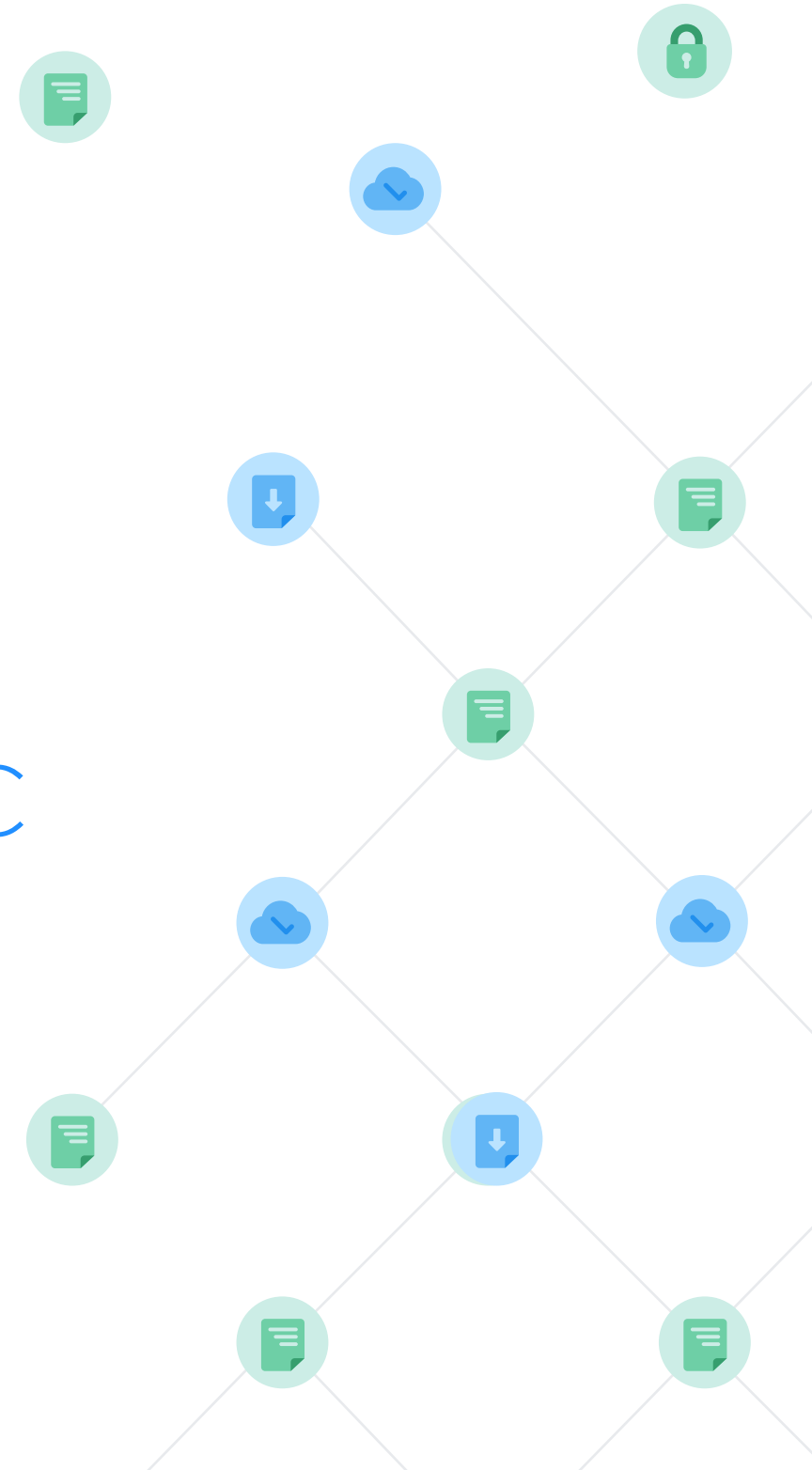
VERA

HOW TO SAFELY ENABLE CLOUD COLLABORATION WITH DATA-CENTRIC SECURITY



INTRODUCTION

Organizations are transforming the way work gets done to be faster, more efficient, and more collaborative. Critical data and files can live anywhere, be accessed from any location and from virtually any device. Likewise, these assets often need to be shared across a wide range of users and collaborators, both inside and outside the enterprise. However, while this “data everywhere” philosophy is great for efficiency, it’s devastating to traditional security models.

Traditional perimeter security obviously fails to protect data that is outside the network perimeter, especially when both the user and the data travel beyond the perimeter. But the problem goes beyond simply trying to extend the perimeter to the cloud. Data, files, and emails are mobile. They can be copied, forwarded, and saved to USBs. As a result, each user that accesses a resource is a potential source of data leakage or a breach, and that user may not be within the perimeter or even in the same organization. When there are many paths to the data, and the data itself is portable, a one-time allow/deny decision at the network or application level simply doesn’t cut it.

Vera delivers a new approach that adheres security to the data itself. Instead of trying to manage the countless avenues that a user could take to access the data, Vera secures data at rest, in flight, and in use, while remaining completely transparent and frictionless to the user. This approach allows users and organizations to collaborate and work intuitively, while allowing security to ensure that assets and intellectual property remain protected and under company control. In this paper, we will dive into the details of how organizations can safely adopt new cloud-based collaborative workflows that both empowers users and keeps the organization safe.

Friends, Foes and Accidents

Enterprise data can be lost in a wide variety of ways, and it is not always the cliched “hacker in a hoodie” who is behind it. While cyber attacks are ever-present and continue to grow in sophistication, some of the largest breaches of the past few years have been due to data that was exposed by insecure third parties or simple mistakes from internal staff.

Regardless of how the data is lost, the costs of a breach are staggering. Reporting requirements, fines, brand damage, and legal costs are just a few of the negative consequences of a breach, and a 2018 analysis by the Ponemon Institute found the average cost of a breach to be $3.82 Million. Looking at the problem globally, the numbers get truly staggering. The recent Hiscox Cyber Readiness Report estimated the global cost of cybercrime at $450 Billion and research firm Cyber Ventures projects the cost to rise to $6 Trillion by 2021. The problem certainly isn’t going away, and if not managed properly, collaborative applications can be an avenue for data loss.

3.62 MILLION

Current estimated global cost of cybercrime

2 TRILLION

By 2020 the estimated global cost of cybercrime

User Accidents

This concept gets even more powerful when we start to look at the other common sources of breaches and data loss. While cybercrime gets the headlines, recent data suggests that this is not even the largest part of the equation. As organizations become more interconnected and work more collaboratively, data is increasingly being disclosed accidentally.

Clear evidence for this can be found at The Privacy Rights Clearinghouse, which maintains an open searchable database of publicly disclosed breaches including how they occurred. While this resource doesn't include all breaches, it does collect information about breaches where disclosure is required by law such as breaches related to PCI, HIPAA, GDPR, and GLBA just to name a few.

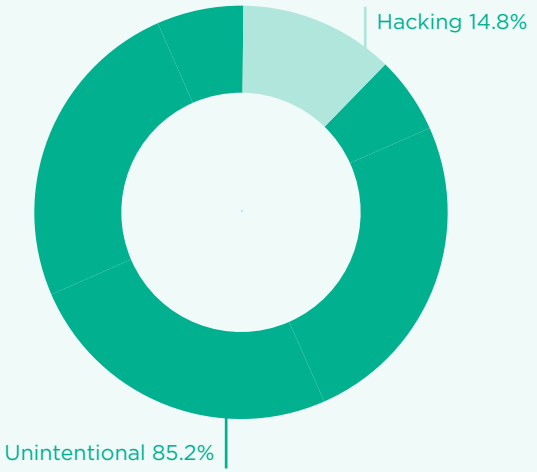
A simple analysis shows that in 2017 over 5 times as many records were disclosed due to accidental causes (1,735,088,147 records) compared to hacking (301,889,038 records). This trend has continued into 2018. Between January and August of 2018, unintentional disclosures have accounted for 623,152,797 records compared to 190,465,130 due to hacking.

So the obvious question becomes, "where are all these unintentional breaches coming from?" In many cases it can boil down to simple human error. Email is a common and easily recognized source of accidental disclosure. A user can accidentally send to the wrong "Brian" or reply all to a large email chain. Furthermore, email is easily forwarded, which further magnifies the chances for a mistake.

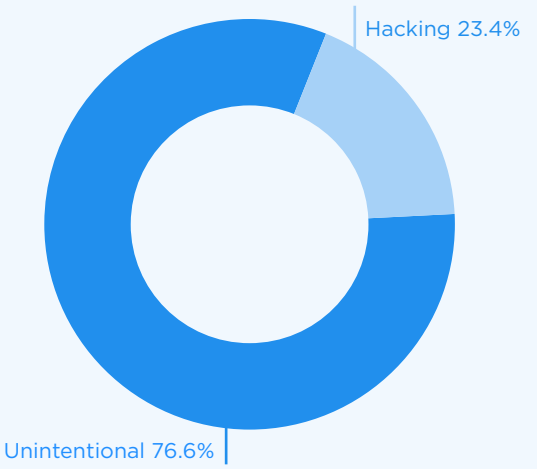
And while email is a traditional source of data loss, content collaboration tools that connect users and teams both inside and outside an organization are having an impact as well. Most organizations are well aware of tools such as Dropbox and Sharepoint for sharing files and collaborating on projects. However, these are just the tip of the data-sharing iceberg with a wide variety of tools such as Slack, messaging apps, Google Drive, and many more allowing users to share data and files through their browsers.

IN 2017 ACCIDENTS ACCOUNTED FOR 5X MORE BREACHED RECORDS THAN HACKING

2017 DISCLOSED RECORDS



2018 DISCLOSED RECORDS (JAN - AUG)



Source: Privacy Rights Clearinghouse

Directly stealing files from their compromised machine

Simply ask the victim directly for information or credentials

Using the victim's identity to access and steal internal files and data.

Threats

While it can be easy to focus on the price tag of a breach, we also need to understand how and why they are happening. The most intuitive answer is to look at the threat landscape including the attackers, malware, and underground economy that survives on the value of stolen data. Modern attackers have become highly adept at compromising individual users and either directly stealing files from their compromised machine or using the victim's identity to access and steal internal files and data.

In other cases, attackers can skip the exploits and hacking tools altogether, and instead simply ask the victim directly for information or credentials. Social engineering remains one of the most successful attack vectors for hackers, and it is incredibly difficult for traditional security controls to stop a user who is willingly handing over data to an attacker.

However, regardless of whether the data is stolen by hacking or guile, the attacker is banking on a common assumption: if he can get to the data, then he wins.

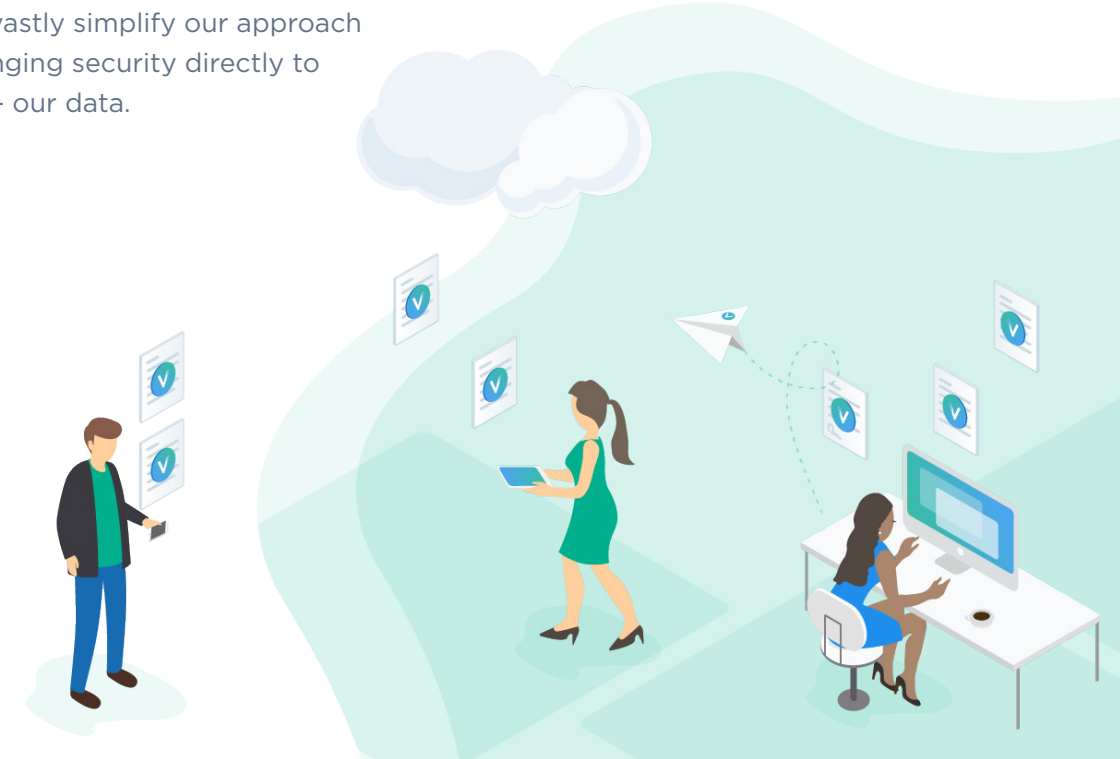
In a data-centric security model this does not have to be true. When security policy follows the data itself, access to the data can be pulled back even after the data has been compromised in an attack.

Partner Ecosystem

In many cases, the critical mistake can occur outside the organization entirely. As businesses become more interconnected, data and files naturally move back and forth across organizational boundaries. While you may take the utmost care with your data, it is almost impossible to fully control the ways that everyone else in your ecosystem behaves. In fact, this has quickly become one of the most notorious sources of damaging data breaches.

Verizon, well-known in the security industry for the Verizon Data Breach Investigation Report, recently themselves suffered a breach of 6 million user records. In this case data was exposed due to the data being insecurely handled by a 3rd party customer service agency that Verizon did business with. Likewise, Dunn and Bradstreet recently suffered a breach of 33 million records, when a partner leaked a file containing contact information for business and government personnel. The file in question was part of the marketing list that the company would rent to marketing firms, and one of those firms leaked the file to the outside.

Once again, it is virtually impossible to completely control and manage everything that our users and partners do. The more we share data, the more likely we are to have that data exposed, whether through honest mistakes or outright negligence. But while mistakes are inevitable, we do have the opportunity to undo the damage of those mistakes. Data-centric security can prevent the disclosure of data to unintended parties (such as preventing partners from passing your data to other parties), and if data is leaked, we can pull that data back so that it can't be used. As we will see in the following sections, we can vastly simplify our approach to security by bringing security directly to the item of value - our data.



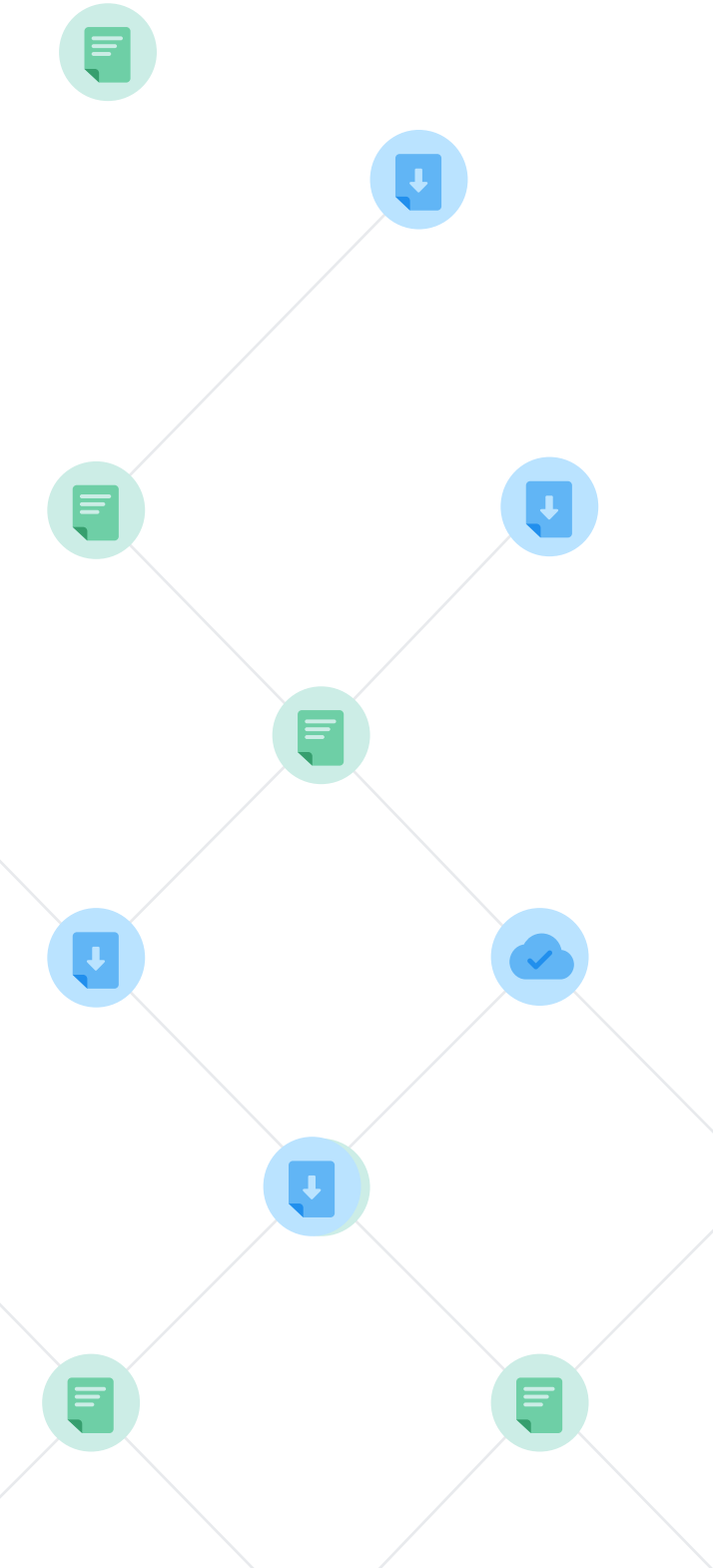
SECURITY IN THE AGE OF COLLABORATION

Collaboration is rapidly redefining how organizations get work done. Far from being a “nice to have”, collaboration tools have quickly become front line tools for working with data. What began with tools like Box and Dropbox has spread to applications of all types. Some of these applications could be sanctioned at the corporate level, used in an ad-hoc way by teams (e.g. Slack, messaging apps), or even simply by an end-user’s personal favorite application (personal Gmail or Google Drive). And while organizations will always try to drive adherence to the sanctioned corporate tools, users tend to gravitate to their personal favorite apps or what they see as the most convenient in the moment.

Secure Enablement

And while collaboration can pose a challenge to security, avoiding it entirely is simply not an option for most modern organizations. Content collaboration is growing fast, and is making adopters more agile and efficient. Recent analysis from IDC observes that a convergence of content collaboration and social engagement is enabling “new approaches to growing business, creating a new generation of engagement-centric efficiencies that benefit every part of the enterprise”. The collaboration market itself is growing rapidly with industry analysts predicting the Enterprise Content Collaboration market to more than quadruple in size by 2025. Likewise, Gartner predicts that by 2022, 50% of enterprises will be using content collaboration platforms.

When a new technology stands to make the organization more productive and more competitive, the security team can’t afford to be the “Department of No”. This not only pits the security team against the needs of the organization, it also simply fails more often than not. In the past, some security teams hoped to limit access to web-browsing to non-corporate sites, or later prevent the use of mobile devices, or later block access to social media. Ultimately, these controls became impractical if not impossible, because the technologies became core to the way that end-users and the organization worked. In these cases, it was the organizations who focused on safely enabling a new technology that gained the competitive advantage.



Building Security for the Long Tail of Data

So once we shift from whether or not to embrace collaboration, the question becomes how to do so securely. And to do this, we need to make sure we see the full scope of the problem. The knee-jerk response might be to say, “well if users are storing files in Application X, then we should add a security layer for Application X”. And this is a common approach. However, it can get difficult to manage very quickly as users adopt new applications with new features. New partners may use different applications, and thus puts security teams in an endlessly reactive situation where they must adapt to support new applications.

But this approach contains an even bigger problem - it falls back on old perimeter thinking. The built-in assumption is that if we ensure that if the initial access of data is done safely then the data will remain safe. This is a hold-over mentality of a time when users and their data were presumed safe on the inside of the network. That is no longer the case, and data can have a very long and interesting life after being accessed in the collaboration app. Data can be saved, copied, forwarded, and shared in other applications indefinitely. This is the long tail of modern data. There are many paths to access, many devices it can be stored on, and can live indefinitely. In short, data must be secured across all of these phases - when it is accessed in the application, when it is being transmitted and when it is at rest. By bringing security to the actual asset itself, security teams can get out of the losing proposition of trying to predict every how, when, and where of an asset, and instead simply secure the asset itself.

THE VERA APPROACH

Vera provides a way to safely enable collaboration regardless of the applications you use or who you need to collaborate with. Just as importantly, our approach protects your data through all phases, whether the data is at rest, in transit, or in use. You gain full control over exactly who can access the data, how they can use it, and even easily pull back access once a project is completed or if a user changes roles. And just as importantly, security remains transparent to users, who remain free to work with the data based on your policies without any added friction. Here's how it works.

Dynamic Encryption At Rest, In Flight, and In Use

Vera delivers security directly to the data by wrapping each file in an HTML wrapper and encrypting it using AES 256-bit encryption. Each file has its own unique key, which is maintained in the Vera Cloud Platform, which can be hosted by Vera or on the customer's cloud. When a user wants to access a file, a request is sent via SSL/TLS to the Vera Cloud Platform, which checks policy to see if the user is allowed access to the file and if there are any permission or policy restrictions.
If access is allowed, the appropriate key is delivered to the host, once again via SSL/TLS. Keys are never stored on the device unless the user is specifically granted permission to access the file offline. In this way, users can work with and interact with a file just as they always would, but the file is never beyond the control of security policy at any time. Additionally, since the customer has the option to host the Vera Cloud Platform on their own cloud, customers can likewise ensure that they are in sole control of the encryption keys.

Control Permissions and Revoke on Demand

Vera also provides new controls over how a user can interact with your data once its accessed. Users can always have full unfettered access to the file, or additional controls can be layered on by policy. For example, users can be allowed to edit files or can be limited to read only. Policy can allow or disable the ability to copy/paste, print the file, or access it offline. These permissions can be set at the level of an individual, group, or organization. Most importantly permissions can be changed or revoked at any time. If a user leaves the company or changes roles, access can be revoked. Likewise if data is compromised as part of a malicious or accidental breach, access can be instantly revoked to mitigate damage.

Transparent and Frictionless

Unlike DRM and similar technologies, Vera remains transparent to the user and without interrupting the user's normal workflow. Vera's client works in the background to automatically check policies and securely handle the exchange of encryption keys. Even without a client, Vera's agentless option lets user's work on and edit Microsoft Office documents directly within their browser. The only differences a user experiences are those specifically set by your corporate policy, such as removing the option to copy/paste, print, or edit.

Your Data Under Your Control

With Vera, you remain fully in control of your data, and data is never shared with Vera. The Vera Cloud Platform only manages the encryption keys and never contains or stores your data. Additionally, keys for each organization are logically separated and customers also have the option to host the Vera Cloud Platform on their own cloud so that they remain in sole control of the keys. This means that even Vera engineers cannot see your data unless you expressly share it with them. And unlike a service provider which can be compelled to hand over keys via a subpoena, Vera ensures that only you can grant access to your data.

While bringing security to the data layer is a new approach for most enterprise security teams, it can also be seen as an extension to one of the most fundamental security technologies of the past 20+ years. SSL and subsequently TLS have served as core enabling technologies that allowed the Internet to quickly grow into the central hub of commerce that it is today. In order to do business, users needed to know that they were connecting to valid sites, and that their information was safe in flight. This was an ideal job for encryption, but it would only work for the masses if it was completely transparent to the end user.

SSL and TLS served this role, and in the process was able to change how the world accessed information securely. Vera extends this concept beyond the session and transport layers of a network connection to the data itself. The data is encrypted, access is only granted to users or groups that are specifically allowed, and the entire process remains transparent to the user. And just like SSL/TLS, Vera has the potential to securely enable completely new ways of working, collaborating, and doing business while maintaining security.

ARCHITECTING FOR COLLABORATION:

COMPARING VERA AND OTHER TECHNOLOGIES

Vera's approach is certainly not the only option for securing your enterprise data. However, the unique challenges of collaboration provide an ideal example for how Vera can solve problems in ways that other technologies simply can't.

Data Classification

Many organizations have attempted to get control over their data in the past through the use of data classification and tagging. And certainly this can be a good start, but too often it simply serves to document a problem instead of controlling it. Being able to know what and where your data lives is only helpful if you can then enforce control over it. When it comes to collaboration, control is of the essence. People and organizations will want access to your data, and simply knowing a certain type of data was sent to a collaboration app does very little to limit the exposure of that data.

DLP

Other organizations have invested heavily in DLP solutions. DLP comes with a variety of challenges, not the least of which is that the technology tend to incur very strong performance penalties and its reliance on pattern matching makes it prone to generating false positives. The problems of DLP get magnified in the context of collaboration. DLP is often best suited for situations where a very specific type of data is limited to a very specific location (e.g. payment card data should stay within the cardholder environment). However, in the case of collaboration we are intentionally moving a wide variety of data outside of the

perimeter in order to work better, faster, and more efficiently. Worse still, DLP has no notion of controlling the data once it leaves the environment. So while DLP can serve some use cases, it is far from ideal for managing collaboration.

Once your data moves past the DLP fence and CASB proxy, it's in the wild and unprotected.

CASB

Other and far more interesting approach is the use of a Cloud Access Security Broker or CASB. These technologies evolved to extend much of the same level of application control provided by modern firewalls to cloud applications and mobile users. CASB products can play an important role in an organization's security stack, especially for protecting applications themselves (e.g. controlling users working directly in an application like Salesforce).

However, it has several challenges in the collaboration space. First, CASB depends on controlling access at the application level. In other words, CASB controls "how" the data is accessed, and as we've seen there are many of these "hows". A CASB may have great features for your collaboration app, but not for your partner's. And if managing the many applications wasn't enough, CASB products simply lose control when data and files leave the application. Once again, it matters what happens to data once its accessed - where it goes, how it's modified, and who has access. Collaboration is ultimately about enabling your ecosystem, and a collaboration app is only a slice of that ecosystem. Vera's approach to security flows with your data while allowing you to maintain full control.

And while Vera allows organizations to extend security in that other technologies can't, the solution remains highly complementary to any of the technologies listed above. For example, Vera's data-centric approach can work seamlessly with a customer's CASB solution and easily extend controls to areas where the CASB can't enforce.

CONCLUSION

Collaboration is increasingly an essential way that organizations work, and Vera provides a unique way for security teams to embrace this technology safely and with control. The need to allow access to a wide range of individuals, groups, and through an ever-growing list of applications poses serious challenges to traditional approaches to security. Vera addresses these challenges head-on with an approach that keeps the focus on ensuring the security of the organization's assets and data regardless of the application being used. This allows users to work how and when they want, and for teams to adopt and use the tools and apps that best suit their needs. As a result, Vera provides a way to truly free the business while retaining full security and controlling the risk of a data loss and breaches.

Are you interested in Vera? Great! Let's discuss how we can help you.
Visit us at **www.vera.com/contact-us** to get in touch.