VERA

THE ACRONYM JUNGLE

UNDERSTANDING THE BENEFITS AND CHALLENGES OF DATA LOSS PREVENTION (DLP) AND CLOUD ACCESS SECURITY BROKERS (CASB)

As organizations become increasingly mobile and cloud-based, IT and Security teams can no longer rely on the traditional perimeter models to protect their key assets and content. End-users are highly mobile, have many devices and connectivity options, and expect to be able to access their content from anywhere. Likewise, applications have quickly transitioned to the cloud, whether as SaaS-based applications or hosted in cloud-based data centers. When users, data, and applications can all live beyond the perimeter, a new approach is required.

Vera introduces a new data-centric approach that allows policy to follow enterprise content no matter where it goes, and even allows access to content to be revoked at any time, even if it is sent outside the enterprise.

However, Vera is certainly not the only solution to focus on protecting enterprise content. DLP and CASB solutions are often evaluated as options to help secure organizations in a post-perimeter architecture. While these technologies can provide value, they do not solve the fundamental problem facing organizations - how to keep their data secure in the real world where content moves and is always accessible. In this paper, we will evaluate the respective strengths and weakness of these approaches and how they compare to Vera.

Data Protection Challenges and Requirements

While most IT and security teams have experienced the erosion of the network perimeter first-hand, it is important to recognize that this is a sign of a more fundamental challenge. If we don't properly address these underlying challenges, an organization can run the risk of building new, costly perimeters with the same problems as the old perimeter.

Perimeter security typically does a very good job under the right circumstances. It provides excellent point-in-time security when content traverses a specific point of control. The limitations of this approach are well documented, however. In a world of continuous productivity, collaboration across companies and services, and truly productive mobility, it's vital for organizations to confront this shift head-on by attaching security directly to the data itself. Organizations need to effectively protect any kind of data, and then track, audit and manage the policies securing it in real-time, no matter how far it travels.

Current solutions, from on-premises storage to Enterprise Content Management (ECM) to modern enterprise sync and share tools – like Box, Dropbox, and OneDrive – can address different parts of this problem. However, none have the capability to fully protect the full lifecycle of enterprise content. Companies regularly store and share information across multiple repositories, and the daily course of business disperses that data across different systems, from CRM to ERP to HRM and even to financial systems. As organizations and individual workers become more continuously productive, IT and security teams need tools that can simply extend these controls across platforms.

Point-in-Time Security vs. Continuous Security

Data exists much longer than a single point in time. For example, while it may be ok for data to move from point A (internal network) to point B (remote employee), we may not want it to move to point C (competitor). However, once it's past the enforcement point, a perimeter-based solution no longer has any control. Additionally, the policy around a piece of content can change over time. Maybe a partner needed access to information for a specific project. Once the project is complete, the partner should no longer need access. Yet, in a traditional model, once access is granted, that access remains perpetual.

Boundary-Specific vs Universal Enforcement

Additionally, for perimeter technologies to work, they need content to traverse a specific control point and in a specific way. Traditionally this is the boundary between the private enterprise network and the Internet. Obviously, files that are shared while outside of the perimeter are not secured in this case.

However, it's important to remember that data must also cross the perimeter in a certain way. An employee who puts data on USB drive, sends content via mobile phone over a cellular network, or encrypts his traffic with a personal VPN will all easily leave the local environment without being controlled by the perimeter.

While these examples are likely well-known, it is important to recognize that DLP and CASB both suffer from these same fundamental challenges. They make point-in-time decisions when content hits a specific boundary. Just like with the traditional network perimeter, problems arise when content moves in unexpected ways, and all control is lost once the content leaves the control point.

This is where Vera's approach provides a starkly different and demonstrably stronger approach. Policy is continuous regardless of where the content goes. Content can leave the trusted environment, yet still only be accessed and used by specific users who are approved. Policy can adapt to changes, allowing access to be revoked as needed. Policy becomes consistent, continuous, and not dependent on location. This architecture provides the ability to actually complement and compensate for the challenges of the perimeter instead of simply extending the same problems to new locations.

Data Loss Prevention

DLP is one of the long-standing and more traditional approaches to securing enterprise data. It can be either network or endpoint-based, each having their own unique benefits and challenges. DLP technologies have traditionally been prone to false positives, and as such, some their best use-cases are for controlling very predictable and structured content in very specific situations. For example, DLP might be used for ensuring that credit card numbers do not leave the Cardholder Data Environment of network. However, as content and locations get more complex, DLP can develop problems very quickly.

Positive vs. Negative Controls

A core challenge of DLP is that it is based on a negative control model. In many ways, you can think of DLP as an IPS, where instead of trying to match malicious exploits coming into the environment, DLP tries to match sensitive content going out. In InfoSec parlance this is a "negative control" where the goal is to detect something bad and block it (and conversely let everything else go through). And this model is why DLP has earned the reputation for being both slow and prone to false positives. It must analyze all content and try to match it to block lists. This requires lots of analysis and the matching can be wrong as enterprise content is constantly changing.

The counterpoint to negative control models is the positive control model. Once again using a network example, a firewall is an example of a positive control. Security specifies what should be allowed (e.g. port 80) and everything else is denied by default. Vera takes a much more positive approach although at the content level instead of the network level. Vera policy defines who should have access to the content and what they should be able to do with it. Everything else is denied by default. This not only makes policy much simpler, but it removes the constant specter of false positives.

The Challenges of Data Loss Prevention Technologies

Unfortunately, DLP also carries a large number of challenges in addition to false positives. First, as discussed before, DLP makes a point-in-time decision. Once data leaves the point of control whether at the endpoint or the network, the DLP no longer has control over that content. If that data is forwarded, copied, stolen, or accidentally exposed, there is very little that DLP can do.

Additionally, users can evade DLP either intentionally or accidentally. Data moved on a USB would be invisible to the DLP. An employee accessing their webmail on an unmanaged device could easily circumvent a host-based control. A user (or malware) encrypting the content or sending through encrypted channels could evade DLP controls. Once again, Vera's approach is unphased by any of these challenges. Security is built into the content and follows it regardless of where it goes or how it is transmitted.

Cloud Access Security Brokers (CASB)

Cloud Access Security Brokers are a relatively new entrant to the enterprise security stack. As the name implies CASBs help to secure organizations accessing cloud applications. Gartner defines CASB as:

"on-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed."

CASBs have proven to be highly valuable to enterprises on a variety of fronts. At their core, a CASB is able to extend security policy to an enterprise's cloud applications in much the same way a traditional firewall would protect on-premise applications. Organizations can control who should get access to a cloud-based app, what features they should be able to use within that app and so on. A CASB can also give an organization insight into what applications are being used so that they can better understand user needs and their attack surface. With this similarity to traditional firewall functionality, it's no surprise that most firewall vendors have acquired or integrated CASB functionality into their offerings.

Limitations of CASB

This similarity to firewalls also begins to highlight the differences between Vera's content-based security and CASB. In fact, Vera closely partners and integrates with CASBs as opposed to competing with them.

One of the major differences can be found in the definition of a CASB itself. Revisiting the definition above, CASB is an enforcement point that is applied as cloud resources are being accessed. Once again, this is a point-in-time, localized approach to security. It effectively extends the physical perimeter of local network to a new perimeter specifically for cloud applications.

A better approach is to design a system that can operate securely, independent from how information is shared or stored.

Just as we saw in earlier examples, this means that CASB loses control over data after it has been accessed. Users can still copy content, store it in insecure personal drives, share it with other parties, or have it compromised by malware or attackers. While a CASB can help illuminate an application blind spot, it does not ensure that the data itself remains safe.

"Vera provides one of the most pivotal technologies eluding enterprise IT: A solution truly balancing strong security and simple user experience."

Nick Mehta, CEO, Gainsight

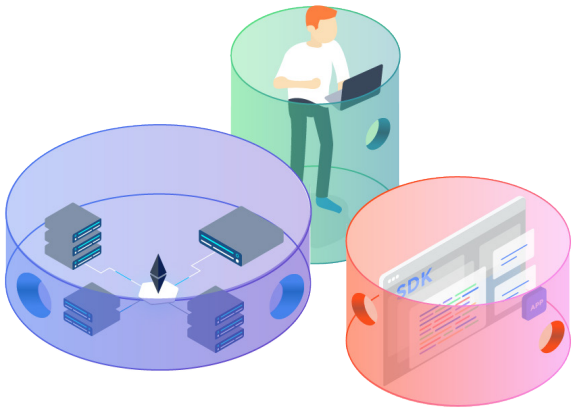
Moving Beyond Trusted Walls

This lack of control after data is accessed highlights another major challenge in information security today. Just because a user can access an asset should not mean that they are inherently trusted going forward. Even in traditional on-premise networks, organizations are increasingly moving to “zero trust architectures”, where all users are presumed to be compromised and every access to data is reviewed and approved based on policy.

Centralization of policy management and administration is critical, ensuring that copies of documents or edited versions do not lose the original’s security.

And while IT teams can enforce fine-grained control on their internal networks, they can’t extend this approach to the Internet. CASB creates a new enforcement point in front of a cloud application, but control is lost after access. Once a user accessing content in a CASB, most organizations simply have to revert to simply trusting the user to keep that data safe.

A data-centric approach solves this problem. Vera ensures that policy is checked and enforced whenever data is accessed regardless of where or how the access takes place. Instead of trying to control everything around the data, Vera extends control to the data itself. Trust can be defined down to an individual and controlled in terms of what the user is allowed to do with the data. Trust is also adaptive and can be revoked at any time. This provides a logical approach to protecting data in a truly modern way that neither DLP or CASB can accomplish. Data and content can move, yet IT and Security teams remain in control and can adapt as situations change.



For more information about Vera or to schedule a demo for your organization, please visit us at **www.vera.com** or find us on Twitter **@VeraSecurity**