FORTRA

SOLUTION BRIEF (Vera)

How Vera Extends Security in Data Loss Prevention (DLP) Products

Introduction

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.

Data Protection Challenges and Requirements

Data Loss Prevention (DLP) products are often evaluated as an option to help secure organizations in a "post-perimeter" architecture. It's one of the legacy approaches to securing enterprise data. It can be either network or endpoint-based, each having its own unique benefits and challenges. DLP technologies have traditionally been prone to false positives, and as such, some of 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 the network. However, as content and locations get more complex, DLP can develop problems very quickly.

While DLP provides value in certain cases, (such as preventing the loss of data, internally), it does not solve the fundamental problem facing organizations -- how to keep data secure in the real world where content moves and is always accessible. In this solutions brief, we evaluate the respective strengths and weaknesses of this approach and how Vera can help compliment your DLP efforts.

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. As content and locations get more complex, DLP can develop problems very quickly.

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 dtenied by default. This not only makes policy much simpler, but it removes the constant specter of false positives.

There can be a 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, 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.

How does your DLP protect files that you need to share with external users?

Does your DLP policy allow limited access such as document time bombs or view only?

Do you find that currently trying to use DLP to achieve your desired outcome introduces a lot of friction?

How do you revoke access to an internal or an external user that once had authorized access to a file?

Summary: The Data-Centric Approach

Vera extends a DLP's flexibility. DLP is very binary in terms of what happens to the data: they either allow it or block it. There are some related activities such as warning the user that the data is suspect, or requiring approval, etc., but the end result is still going to be one of those two things - allow or block. If the data is allowed to travel, all control over it is lost.

Vera also allows DLP admins to relax those stringent rules around unstructured data which provides a better experience for users. When security tools are actually used by employees, the security posture of the organization increases.

A data-centric approach solves these challenges. 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 DLP can't accomplish. Data and content can move, yet IT and Security teams remain in control and can adapt as situations change.

Additional Capabilities

Dynamic File Protection

- Dynamically control user file permissions
- AES 256-bit encryption to any file type
- Granular visibility and centralized control
- Understand how your content is used, by whom, and proactively investigate unauthorized access attempts
- Policies can be based on a number of pre-defined parameters including file location, name, type, securer, sender, recipient, group or other pre-existing permission structures

Real-Time Access Control

- Decoupled data and access control
- Real-time management for all file types
- Targeted access for users, groups, and domains
- Access control is easily managed from desktop, mobile, and browsers

Flexible Deployment Options

- Pure SaaS deployment model
- Allows for a hybrid model where Vera infrastructure for protecting/viewing files
- Key management can be deployed on-premise
- VPC option in AWS for customers with high security postures
- On-premise for federal services and military
- SDK allows for integration into third party applications such as web apps, DLP, classification, and DMS
- Integrate with ID management solutions such as Okta, Google, AD, LDAP
- Integration with existing file share solutions such as Box, Dropbox, SMB, SharePoint and OneDrive
- Configurable to work with enterprise email archiving solutions

Vera is a data and content security solution that enhances an organization's ability to protect, govern and manage the transmission of information without impacting employees or the existing security choices the organization has made. Files secured by Vera can still be protected by gateways, firewalls and endpoint technologies, but customers choosing Vera can now extend these controls beyond the boundaries of their business.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.