FORTRA

SOLUTION BRIEF (Vera)

The Vera-Netskope CASB Integration

Introduction

The Vera-Netskope integration empowers organizations to collaborate freely and securely in the cloud. With this powerful new offering, it's no longer necessary to lock down information so completely that employees have a difficult time doing their jobs.

CASB Primer

Cloud Access Security Brokers (CASBs) are a relatively new entrant to the enterprise security stack. As the name implies, CASBs help organizations securely access cloud applications.

Gartner Defines a CASB as

"An 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 number of fronts. At their core, CASBs extend enterprise security policy to cloud applications much in the same way traditional firewalls protect on-premise applications. Organizations can control who has access to a cloud-based app, which features they are able to use within that app and, to some extent, what they can do with the data being extracted from that app.

CASBs also provide insight into which applications are being used in order to better understand end-user needs as well as 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. While CASBs also have the ability to secure enterprise data, their approach differs from Vera's file-based security solution.

The First Step Toward Protecting Sensitive Data

Netskope's market-leading CASB provides an enforcement point when cloud resources are accessed. This is a point-in-time, localized approach to security that effectively extends the physical perimeter of a local network to a new perimeter specifically around cloud applications.

Netskope's data loss prevention (DLP) functionality protects the data within these cloud resources and provides organizations with real-time, granular visibility and control of cloud collaboration solutions. Along with storing data, DLP provides rich, contextual details around usage, including user, service, device, location, activity and content. positives. First, as discussed before, DLP makes a point-in-time decision.

The Vera + Netskope Offering

Vera and Netskope have partnered to produce an integrated solution that offers our customers a new level of data protection, enabling organizations to automatically inspect, detect, secure, track and audit the use of sensitive data throughout its lifecycle, inside and outside of a perimeter. This integration will dramatically improve a company's overall security posture by providing complete control over unstructured data.

Vera and Secure Collaboration

Vera enables secure internal and external collaboration by protecting unstructured data through encryption, access control, and dynamic policy, which dictates what users can and cannot do with the data. Vera can secure any file type and allows users to collaborate using email, Box, Dropbox, SharePoint, etc.

Even if users copy the content, store it on insecure personal drives, share it with external third parties or have it compromised by malware or attackers, the data itself always remains secure, fully trackable and, most importantly, revokable.

How it Works

Cloud collaboration is an inherent part of doing business today for many organizations. Market-leading solutions like Box, Dropbox and SharePoint Online have made it extremely easy to store, manage and collaborate on data among internal employees and external third parties. Without proper security controls in place, however, users must trust that their collaborators will do the right thing with their data.

The Vera-Netskope solution provides these controls with a powerful combination of CASB, DLP and file-level security functionality. This starts with the inspection of content in a repository to determine the level of sensitivity of the data. Once the sensitivity level is determined, Vera takes over by securing the file through encryption, access control and dynamic policy. Vera security persists with the file, allowing the file owner to maintain control even if it leaves the protection of the Netskope CASB sphere.

Specific Use Case 1

Inspect Content & Apply Policy

Netskope runs DLP on a set of files that have been uploaded to a collaboration solution such as OneDrive and determines there is sensitive content contained within those files. A Netskope policy has been defined, assigning Vera to protect sensitive documents. The Netskope solution then calls to apply encryption, access control and the appropriate policy, such as read-only, to the documents. Now the documents are secure, trackable and any action taken on those files will be logged and captured via an audit trail.

Specific Use Case 2

Inherent App Permissions Automatically

Documents have been uploaded to a collaboration environment, such as a Box folder, and will be accessible by both internal and external third parties. Netskope DLP scans those files and detects sensitive content within them. Netskope then calls Vera to secure the files. The files are encrypted and the access controls are applied, with access permissions inherited automatically from the Box folder collaborators. A specific policy is then applied to the files based on who the users are and what level of access they should have. In this example, external users might have view-only rights, as opposed to internal users who may have full read-write permissions.

Specific Use Case 3

Revise Vera Policies Based On Content

Files contained in a collaboration environment, such as Dropbox, have been secured with Vera. Netskope DLP is applied to inspect the content for sensitive information. The files are then decrypted and Netskope's DLP scans the files.

Netskope determines that the Vera security policy previously applied to those files needs to be escalated. Netskope calls on Vera to reapply a new policy based on the sensitivity level of the document. The files are now secured with the updated policy.

Netskope Security Cloud Overview

Netskope's award-winning security cloud provides unrivaled visibility, as well as real-time data and threat protection when accessing cloud services, websites and private apps from anywhere on any device. Netskope delivers data-centric security from one of the world's biggest and fastest security networks, empowering the largest organizations in the world with the balance of protection and speed they need to enable business velocity and secure their digital transformation journey.

Sanctioned SAAS	IAAS PAAS	UNSANCTIONED SAAS	WEB
API Controls		InLine Controls with Cloud XD	
Risk Assessment	Data Protection	Analytics	
Access Control	Threat Protection	Future Services	
NEW EDGE			

THIRD PARTY INTEGRATIONS

- SSO/IAM
- SIEM/UEBA
- Threat Intel Sharing
- and more...

UNIFIED CONSOLE FOR SAAS, IAAS p+ WEB

ENTERPRISE

REMOTE USERSD

IRECT TO NET

BYOD

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.