FORTRA

SOLUTION BRIEF (Vera)

Protect Data in The Event of Misconfigurations

Introduction

Recently, there has been a huge increase in data breaches caused by misconfigured access to and exploited vulnerabilities in cloud storage environments. Cybersecurity companies, like Digital Shadows, DarkMatter, Check Point Software and many others, have released their annual cloud security reports citing how misconfigurations are a growing concern that needs to be addressed immediately. Gartner goes as far as to say that 80% of data breaches will be due to misconfigurations and mismanaged credentials, and 95% of cloud security failures will be the customer's fault.[4]

This is becoming a common problem. Microsoft, MongoDB, Elasticsearch, Amazon Simple Storage Service (S3) servers, Box and Rubrik have had misconfiguration issues in the past that have exposed the data of thousands of companies. Unsecured Amazon Web Service (AWS) S3 storage buckets are perhaps the most frequently reported on files that are left unsecured, since they allow anyone using a search engine to access, download and, in some cases, even write to an organization's cloud account.

Consider the Statistics:

An estimated
4 BILLION
data documents were stolen in 2016[4]

7.8 BILLION
records were compromised in 2017[5]

The 2019 Verizon Data Breach Investigations Report (DBIR) states that misconfigurations of cloud-based file storage account for
21% of DATA EXPOSURES
that were caused by errors

According to Gartner, through 2020,
80% of DATA BREACHES
will be due to misconfigurations and mismanaged credentials[6]

Gartner also states that, through 2023,
99% Of Cloud Security Failures
will be the customer's fault[7]

74% of Enterprises
used critical network services with security issues arising from poor configuration, such as failing to follow best practices with system permissions, allowing remote or anonymous logins and disabling important security safeguards[8]

[1] Davis, Jessica. "2 Misconfigured Databases Breach Sensitive Data of Nearly 90K Patients." HealthITSecurity, HealthITSecurity, 7 Aug. 2019, https://healthitsecurity.com/news/2-misconfigured-databases-breach-sensitive-data-of-nearly-90k-patients.

[2] @DMBisson, David BissonFollow. "Misconfigured ElasticSearch Cluster Exposed Over 90 Million Records." The State of Security, 9 July 2019, https://www.tripwire.com/state-of-security/latest-security-news/misconfigured-elasticsearch-cluster-exposed-over-90-million-records/.

[3] Sheridan, Kelly. "Rubrik Data Leak Is Another Cloud Misconfiguration Horror Story." Dark Reading, Jan. 2019, https://www.darkreading.com/cloud/rubrik-data-leak-is-another-cloud-misconfiguration-horror-story/d/d-id/1333767.

[4] Whittaker, Zack. "Over Four Billion Data Records Were Stolen in 2016." ZDNet, ZDNet, 30 Jan. 2017, https://www.zdnet.com/article/over-four-billion-data-records-were-stolen-in-2016/.

[5] Solove, Daniel. "Data Security Is Worsening: 2017 Was the Worst Year Yet." TeachPrivacy, 28 Nov. 2018, https://teachprivacy.com/data-security-is-worsening-2017-was-the-worst-year-yet/.

[6] Panetta, Kasey. "Gartner's Top 10 Security Predictions 2016." Smarter With Gartner, https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/.

[7] Magic Quadrant for Cloud Access Security Brokers https://www.gartner.com/doc/reprints?id=1-5P8KQRA&ct=181101&st=sb

[8] DarkMatter Cybersecurity Report, June 2019

Common Reasons for Misconfigurations

Although the business models of Amazon and other cloud service providers (CSPs) have a built-in infrastructure that processes data, it's the user's responsibility to protect the data that is stored in that infrastructure. The CSP provides the installation and management of the underlying hardware and software infrastructure, but the secure configuration of consumed resources is your responsibility.

When the deployment of cloud workloads, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), containers, serverless and cloud security services like networking, encryption, Web Application Firewall (WAF) and Security Information and Event Management (SIEM) are not automated, configurations that are done manually with a console may easily result in human error. Default configurations can also cause problems. For example, the Box breach[9] that left thousands of sensitive documents exposed was actually a misconfigured default setting that was easily exploited by security researchers. Box has since changed those default settings.

Insufficient Access Restrictions

In many cases, cloud services like MongoDB and Elasticsearch are left wide open and only restrict access when these settings are changed manually. There are many reasons for this, one being that it improves the user experience substantially if the functionality is free of any obstacles. In that case, it's fast and easy for anyone to use. Another reason is that it's also a result of IT departments cutting corners, as they want to set up networks without having to constantly manage credentials and logins.

[9] Whittaker, Zack. "Dozens of Companies Leaked Sensitive Data Thanks to Misconfigured Box Accounts." TechCrunch, TechCrunch, 11 Mar. 2019, https://techcrunch.com/2019/03/11/data-leak-box-accounts/.

Not Following Internal Security Policies

In Rubrik's case, an investigation found that the cause was developer error. The sandbox development data repository defaulted to a lower security access level. Rubrik failed to follow its security procedure to correctly set the access control, but has since resolved the issue and rolled out multiple levels of approvals and security reviews to ensure it doesn't happen again. This example shows how data incidents can very easily happen, not due to negligence or maliciousness, but because of honest mistakes. We can still safeguard sensitive information by protecting the data itself.

Failure to Audit Resources

Do you conduct regular audits of local and cloud assets? You can't protect what you don't know about. It's important to evaluate access settings and permissions on a regular basis to determine what is working and if there are any new settings implemented that weren't accounted for, or perhaps access controls and permissions that should be there but aren't.

As stated above, misconfigurations are a top contributor to data breaches and other security issues in the cloud. In many cases, the difference between a devastating breach and a secure cloud server boils down to simply knowing where to look and which options to implement. This becomes easier when there is an automated way to protect sensitive data at the file level.

How Vera Protects Data in the Cloud

Vera's architecture is designed to address the challenges created by today's highly collaborative, cloud-based and mobile-centric work environment. We provide flexible, transparent data security that has three primary components:

1. Storage, Transit and Data-Agnostic: Due to the highly collaborative nature of business, it is not safe to assume that enterprise data resides solely in controlled systems. A better approach is to design a system that can operate securely, independent of how information is shared or stored. To ensure the control, management and ownership over critical data, the platform must permit any kind of content type to be controlled and monitored consistently.

2. Data-Centric and Policy-Driven: Secure cloud platforms permit the centralization of policies that govern the management of sensitive enterprise data. By giving organizations central control over access, sharing and collaboration, policies follow the data and can be implemented globally and automatically across the entire organization.

3. Designed for Flexibility, Adoption and Compliance: In a complex organization, data security is improved through adoption and compliance. The fastest path to these goals is through useful, flexible and consistent user experiences. Securing data must be simple and transparent, with as little friction as possible for collaborators receiving secured data. No matter what platform.

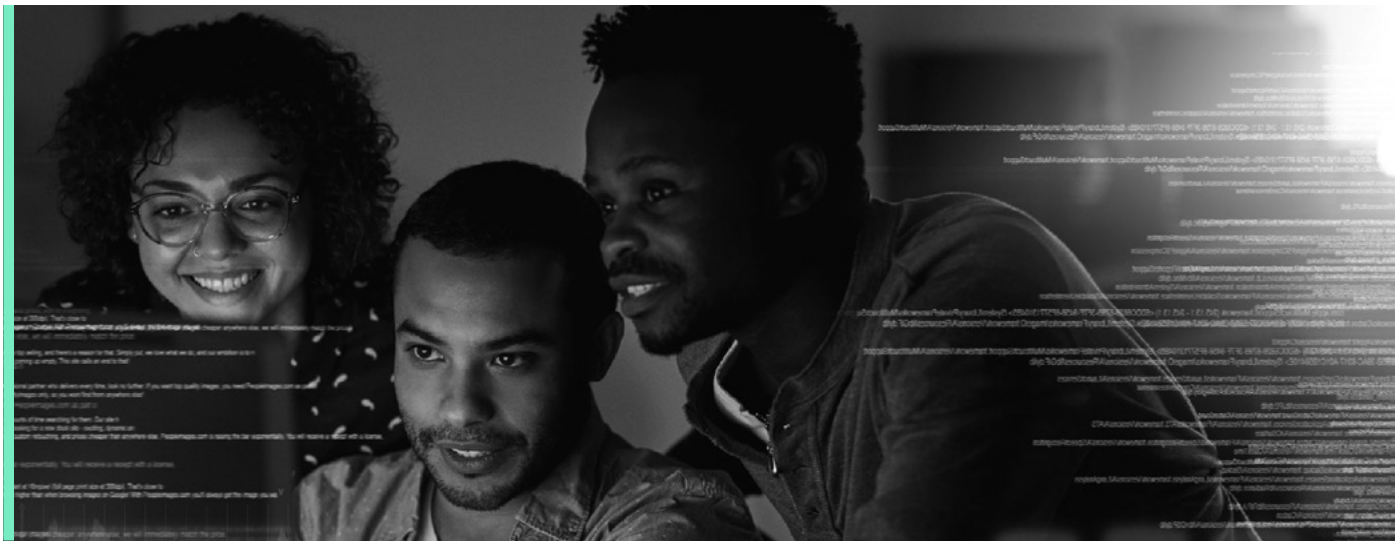
Integration with Cloud Access Security Brokers (CASBs)

CASBs have proven to be highly valuable to enterprises on a variety of fronts. At their core, a CASB is able to extend a 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 can 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 CASBs functionality into their offerings. This similarity to firewalls also begins to highlight the differences between Vera's content-based security and CASBs.

What we see is that a CASB can lose control over data after it has been accessed. Users can still copy the content, store it in unsecured personal drives, share it with other parties, or have it compromised by malware or attackers. While a CASB can help illuminate an application's blind spot, it does not ensure that data itself remains safe.

To address these requirements and deliver a highly available, flexible and confidential security system that can serve both large and small businesses alike, Vera incorporates three primary components in its platform architecture: a secure cloud platform, a set of end-user clients and a web-based administration dashboard.



Vera Platform

The central component of the Vera service is the cloud platform. The Vera Cloud Platform manages the policy and controls for each customer, or tenant on the platform. It also securely manages the processes of creating keys, enforcing access policies and aggregating events and activities for audit and reporting purposes. No customer data or content is stored on the Vera Cloud Platform.

Vera End-User Client

The end-user clients on mobile devices, Microsoft Windows and Mac OS X desktops facilitate the encryption, decryption and policy determination for everything secured by Vera. Through each endpoint, Vera can transparently confirm identity, protect new data as it is created, enforce policy restrictions and ensure the secure transmission of keys and policy to and from the Vera Cloud Platform. An end-user client permits IT teams to centrally manage access on devices both inside and outside the enterprise's control.

Vera Platform

The Vera Dashboard gives both end-users and administrators full visibility and control over all the activity around content, no matter where it is stored or how it is transmitted. Through the Vera Dashboard, an admin can manage access controls, set and update policies, oversee users and activity and run audit reports on usage.

We make it easy for organizations to secure a variety of file types, including all files that are accessed because of a misconfiguration. Vera protects those files, and protects them regardless of where they travel and are ultimately stored. We take an integrated approach to this solution by incorporating different parts of the security infrastructure, from Data Loss Protection (DLP) and classification tools to SIEMs and activity monitoring tools.

Want to Know More?

Vera's unique security model follows your data wherever it goes. For every individual in your organization, we make it effortless to securely collaborate with anyone, no matter which tools they choose to use. For IT and Security practitioners, Vera provides powerful management and oversight in a cloud-based platform that can coordinate and monitor activity independent of where content is stored.

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.