HYTRUST

Datasheet

HyTrust **CloudAdvisor**

Mitigating the Security Risk of Corporate Data Sprawl

Organizations are well aware of the risks of maintaining control of their data and the potential risk that sensitive data possesses to their business should it fall into the wrong hands. Uncontrolled and unrestrained, business critical data proliferates at a surprising speed between employee laptops, networked drives, and the almost unlimited space available in virtual deployments and cloud storage solutions. Uncontrolled sensitive data can include customer transaction and credit card data, intellectual property or other high value company data distributed across a wide range of locations, including storage backups, data shares for collaboration, and workload or Virtual Machine (VM) clones.

Gaining Operational Insight into Critical Data

The difficult task of data classification—discovering sensitive data within a corporate IT ecosystem, identifying ownership and ranking it on business criticality—was previously left to manual searches and broad assumptions to determine data file usage and ownership. Today, industry-leading businesses are beginning to take a more proactive approach to identify uncontrolled data and mitigate the far-reaching effects of compromise by using intelligent automation and analytics to accelerate the process and aid compliance.

Automating Data Discovery and Classification

HyTrust CloudAdvisor answers many questions about sensitive data within your organization, such as "where is this data located?", "who is interacting with the data?", and "why is it stored there?" HyTrust enables organizations to quickly define policies to discover critical business data—including Personally Identifiable Information (PII)—to detect anomalous user behavior, defend against unintended exposure, data loss, malicious user access, and regulatory non-compliance with mandates such as the General Data Protection Regulation (GDPR).

Search, Visualize, and Discover Potential Data Risk

HyTrust CloudAdvisor allows organizations to find the data they need, when they need it. With keyword search, data visualizations, and drill-down explorations, IT and security practitioners can easily navigate, analyze and evaluate file content and user activity to support data management, security, and compliance workflows.

View People, Content, and Activities Over Time

Designed to provide complete visibility into the data stored within each virtual machine, HyTrust CloudAdvisor associates file information with user activity over time. Specific data across more than 600 different file types can be keyword-indexed and pattern-matched against customer defined content tags.

HyTrust CloudAdvisor Features

- Identify sensitive or confidential data stored in VMs
- Virtual appliance to facilitate installation and deployment
- Supports VMware vCenter and Veeam Backup and Replication
- Provides granular insight into file usage, content, and location to enable data classification
- Build a profile of user/data activity over time
- Categorize file content based on mime-type, size, location, duplicates, content, dormancy, file metadata, and ownership
- Predefined policies to detect credit card data, social security numbers, healthcare records, etc.
- Define custom policies to detect specific keywords, string and custom data formats
- Analyze VMs to identify file-based user activity over time
- Behavior-based detection triggers automatic data snapshot in event of malicious or anomalous activity
- Enhanced tagging model and built-in tags for GDPR compliance

Proactively Monitor and Protect Sensitive Data
Automatically identify, monitor, and alert on sensitive and confidential files discovered within VMs. Robust, customizable rule sets help protect sensitive data while audit-quality logs maintain all file and user activity to aid in forensic analysis and evidence gathering for compliance.

Recover from Malicious or Unintentional Disruptive Activities
Behavior-based analytics are used to track and analyze user file access and notify IT and security practitioners of potentially suspicious or abnormal activities.

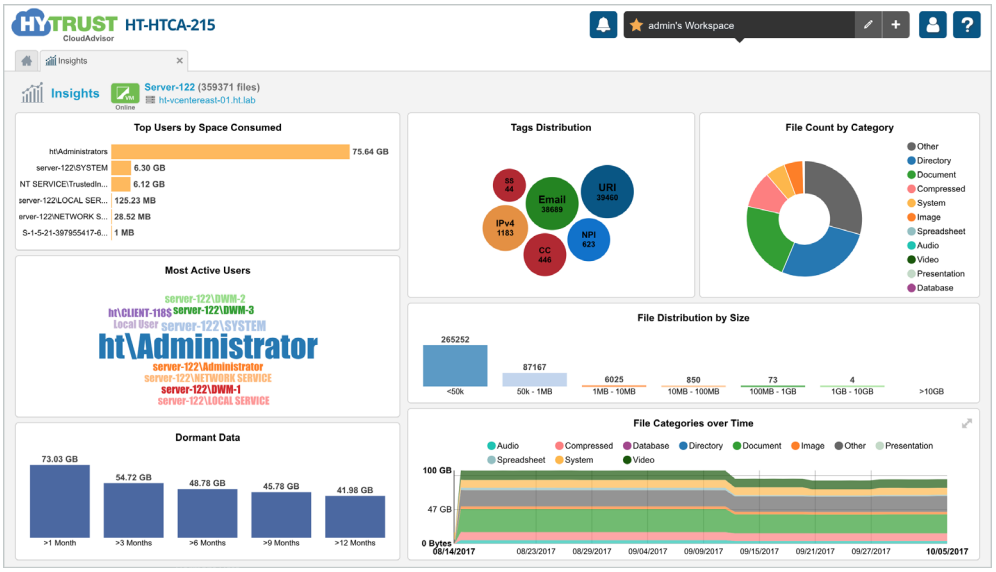


Figure 1. HyTrust CloudAdvisor provides unmatched visibility, insight and actionable intelligence into sensitive data within an organization's virtual environment..

Quickly Deployed and Easily Managed

Upon deployment, HyTrust CloudAdvisor's virtual appliance discovers and enumerates all the VMs within the virtual environment by collaborating with the VMware vCenter or the Veeam backup image.

The discovery process runs at initial setup with periodic runs to track VMs being added/removed from the virtual environment. Once discovered, the regularly updated inventory allows IT and security practitioners to quickly identify new VMs that need to be analyzed, monitored over time, and protected against malicious or careless activity.

Zero Impact, Granular Data Analysis and Tagging

HyTrust CloudAdvisor efficiently indexes all of the relevant file metadata residing within a VM using a read-only snapshot stored within the HyTrust CloudAdvisor virtual appliance, minimizing any impact on the operational VM itself. The frequency at which VMs are analyzed is fully configurable and a VM does not need to be powered-on for the analysis to occur. The analyzed file data is stored as searchable information that can be cross-referenced with user activity to build a data usage profile.

HyTrust CloudAdvisor Benefits

- Know who is accessing data and how it is being used
- Automate discovery and protect sensitive/critical data
- Gain granular insight into each VMs file usage, content, and location
- Customize data discovery policies specific to your business needs
- Analyze VMs whether powered off or running
- Defend against malicious activity by detecting anomalous behavior
- Instantly identify and recover files lost to malware and malicious user activity
- Supports both internal and external compliance initiatives
- Integration with HyTrust DataControl allows for automated encryption of sensitive data as discovered by HyTrust CloudAdvisor

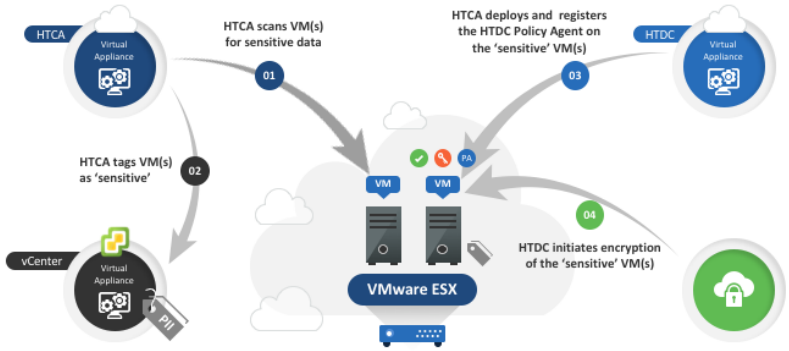
Correlating User and File Activity to Develop Security Insight

Tightly integrated with Microsoft Active Directory to identify user activity related to files stored within a VM, HyTrust CloudAdvisor creates a baseline of activity, which can be used to identify anomalies in user or system behavior over time. Analysis engines running within HyTrust CloudAdvisor evaluates excessive activity, which can automatically trigger an alert, or a safeguard snapshot of the virtual machine should a potentially malicious or anomalous activity occur.

HyTrust CloudAdvisor and HyTrust DataControl Integration

HyTrust CloudAdvisor integrates seamlessly with HyTrust DataControl, enabling the ability to scan both encrypted and unencrypted VMs in a virtualized environment to detect sensitive data based on user defined triggers and then to automatically encrypt those VMs (if not already encrypted) based on policy. Here's how it works:

1. HyTrust CloudAdvisor scans a VM or VMs for sensitive data through a content-based policy with defined triggers, either custom or recommended out-of-the box.
2. When sensitive data is found, HyTrust CloudAdvisor Policy applies the 'sensitive' or otherwise pre-defined tag to the VM(s), including in VMware vCenter
3. HyTrust CloudAdvisor deploys and registers the HyTrust DataControl Policy Agent.
4. HyTrust DataControl initiates encryption of the VM(s) containing sensitive data. Zero-downtime encryption means the VM does not need to be powered down, and one can access the sensitive data while encryption is in progress, including read/write operations.



Summary

HyTrust CloudAdvisor provides unmatched visibility, insight and actionable intelligence into the confidential or sensitive data haphazardly replicated across an organization's virtual environment. Once deployed, HyTrust CloudAdvisor enables IT and security practitioners to automate discovery and accelerate data classification, identify and reduce risk, meet compliance requirements, and proactively protect and secure a company's most valuable data assets. Integration with HyTrust DataControl allows for the automated encryption of sensitive data discovered by HyTrust CloudAdvisor.

"HyTrust CloudAdvisor integrates seamlessly with HyTrust DataControl, **enabling the ability to scan both encrypted and unencrypted VMs in a virtualized environment to detect sensitive data** based on user defined triggers and then to automatically encrypt those VMs (if not already encrypted) based on policy."

To learn more about HyTrust products and services, visit:

www.hytrust.com/products/

HyTrust
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
1-844-681-8100 (US)
1-650-681-8100 (Intl.)

20180626-0025-5