AURORA

Addressing Cloud Data in AWS Using DLP

Symantec™ by Broadcom Software

aws

aurorait.com
sales@aurorait.com
888-282-0696

Introduction

The recent COVID-19 pandemic accelerated the adoption of remote work. Companies are increasingly moving away from earlier remote work solutions, such as establishing VPN tunnels for remote workers to connect securely to the companies' on-premise systems, in favor of cloud solutions, like AWS Workspaces.

AWS Workspaces offers virtual desktops-as-a-service, an easy, familiar way for employees to work from home. Employees connect to AWS Workspaces from their own devices, and login to your company's active directory user. Your on-premises group policies are automatically applied to the AWS Workspace, so your users have the same access and privileges through AWS Workspaces as they would have if they were logged into a company device in the office.

Amazon Workspaces is a virtual workspace that employees can access using their own, or company-provided devices, over the internet. If the company uses Amazon Virtual Private Cloud (VPC) infrastructure, they can connect their VPC(s) directly to their Workspace. If the company has on-premise infrastructure in their offices, they can establish a VPN to connect their on-premise network to their Workspace network.
The connection from a user's endpoint - usually a laptop or desktop, whether it is owned by the user or by the company - uses the PC over Internet Protocol (PCoIP).

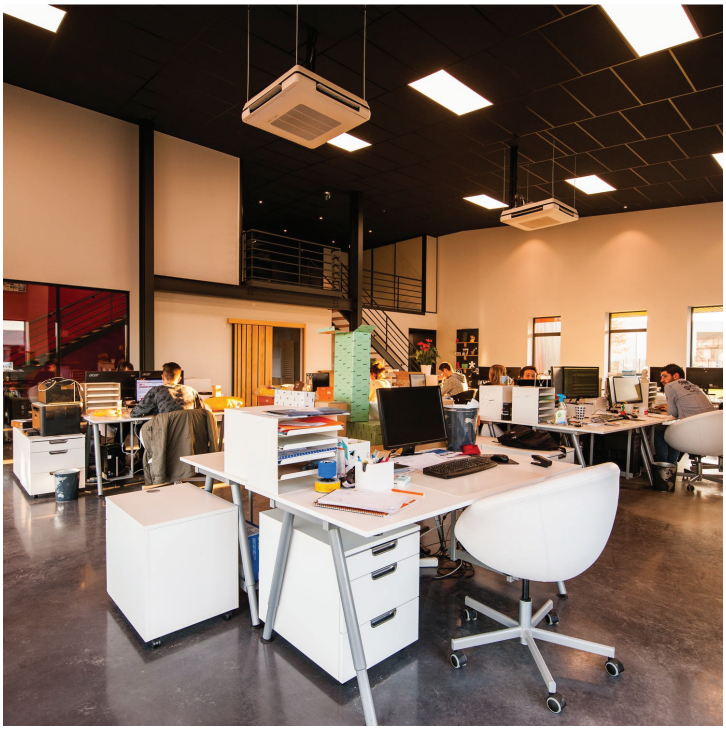
The virtual workstation sends an image of a desktop to the user's endpoint, and receives mouse and keyboard events from the user's device. The user can view and modify data, but the data itself is not downloaded to the user's device. This reduces the company's exposure to vulnerabilities or malware that may be present on a user's device.

Together with more mature cloud offerings like Amazon Elastic Compute Cloud (EC2) and Amazon Secure Storage Service (S3 buckets) infrastructure-as-a-service offerings, Workspaces is accelerating the movement to the cloud. The companies that rely on AWS infrastructure and services must, however, remember that they are responsible for securing the data they use and store in the cloud.

aurorait.com
sales@aurorait.com
888-282-0696

Shared Responsibility

Regardless of how you use the cloud, whether VPC or Workspaces, you must remember that security is a shared responsibility in the cloud. Generally speaking, Amazon is responsible for the security of the cloud infrastructure - the hardware, software, networking, and facilities that run AWS cloud services, and the customer is responsible for security in the cloud. If your company uses cloud storage, compute or workspace solutions, you are responsible for making sure that the data hosted on the cloud infrastructures is not lost, misused or accessed by unauthorized users. Cloud-ready data loss prevention (DLP) solutions, like Symantec DLP, will discover sensitive data stored on your cloud infrastructure, monitor traffic to, from and between your cloud endpoints, and take action to prevent the loss, misuse or exposure of that data based on policies your company defines.



This paper will describe how Aurora can deploy and configure Symantec DLP to secure your sensitive data within AWS EC2, S3, or Workspaces resources. We chose Symantec DLP because it is the market leading solution. Symantec DLP protects:

- **data in use** on endpoints, like virtual desktops and printers;
- as **data in motion** over the network;
- **data at rest** in storage repositories;
- content extracted from cloud apps, such as Office 365 or G-Suite;
- and email and other web traffic.

Symantec DLP not only monitors a broader range of applications and data formats than its competitors. It also enables your information protection team to detect and respond to incidents more quickly with Information Centric Analytics (ICA).

aurorait.com
sales@aurorait.com
888-282-0696

Extending Symantec DLP to AWS Workspaces and VPC

The products that were used during the deployment of Symantec solutions into the AWS cloud environment include: Symantec DLP Enforce, DAR, DIM, Network Discover, Web Prevent, Network Prevent, ICA, and Endpoint Prevent

AURORA

Symantec by Broadcom Software

Integrating Symantec DLP into cloud environments sufficiently can be complex. Aurora has the expertise and experience with Symantec DLP and deep understanding of the AWS environment needed to extend your Symantec DLP coverage to cloud-based services and infrastructure, including AWS workspaces, VPC, EC2 and S3. We will leverage the flexibility and scalability of virtual desktops while still protecting your sensitive data.

To successfully extend your DLP policies to within AWS VPC, Aurora will deploy a dedicated detection server with integrated AWS Transit Gateway service to protect your servers and remote virtual desktops. We can also setup a fully deployed detection server to scan data at rest in resources such as data repositories and SQL databases. This detection can also monitor Linux shares to protect sensitive data from unauthorized sharing.

Aurora will also use detection servers within Amazon VPC to prevent sensitive data from being leaked to the Web. We can also set up proxy components on endpoints, as needed, to route traffic through Symantec Network Prevent, allowing it to inspect all network traffic to and from the end users.

Additionally, we will prevent accidental or deliberate exposure of sensitive data by deploying Symantec Web Prevent and Symantec Endpoint DLP to discover sensitive data, detect and then block unauthorized attempts to share that sensitive data.

The use of Symantec's CloudSOC service can provide greater protection for data within the Amazon S3/EC2 Buckets. CloudSOC will help to give your organization greater visibility of those buckets. You will not need a detection server with CloudSOC. The Symantec DLP Enforce platform integrates fully with CloudSOC to extend seamless DLP coverage into the cloud, using the same DLP policies and response workflows protecting your endpoints, networks and data centers.

We can also integrate Symantec's Information Centric Analytics (ICA) and Symantec Enforce Server data to analyze user behavior and rapidly identify insider threats and data breaches. This combination of Symantec's DLP and ICA provides revolutionary protection against cyber-attacks to every component of a complex cloud environment.

aurorait.com
sales@aurorait.com
888-282-0696

Symantec DLP Overview

Aurora is an established premier partner of Symantec, a division of Broadcom, with deep knowledge and experience within their security portfolio. Our goal is to tailor Symantec's broad security solution sets to align with our clients' own needs and maximize their return on investment. We can help you protect data in Amazon cloud environments in new and innovative ways. Contact us if you are considering implementing Symantec solutions into your AWS environment.

Aurora uses Symantec Data Loss Prevention(DLP) to help clients prevent data breaches by discovering sensitive data wherever it is moving or stored, monitoring how it is being used, and providing real-time protection to prevent exposure or data theft.

Protecting Data in Use on Endpoints
Symantec's Endpoint DLP is a single lightweight agent installed on every endpoint that needs to be scanned (Windows and Mac). The agent has two modules: Endpoint Discover and Endpoint Prevent. Endpoint Discover scans local hard drives to find sensitive data stored on local laptops or desktops. It can take a wide range of actions to protect that data, including quarantining local and remote files and applying policy-based encryption and digital rights management. Endpoint Prevent monitors and controls users' activities. It can alert users to security concerns and take some actions, including enforcing encryption and digital rights management of data transferred to USB devices, to prevent accidental data exposure.

Protecting Data in Motion over the Network
Symantec DLP for Network monitors data in motion over networks and prevents it from being leaked. DLP Network Monitor looks for sensitive content and metadata in outbound traffic on your network. Network Prevent for Email analyzes corporate email traffic and can be configured to modify, redirect or block messages containing sensitive content. Network Prevent for web performs a similar service by monitoring corporate web traffic; it can be configured to remove sensitive HTML content and block requests.

Protecting Data at Rest
Symantec DLP for storage discovers and secures sensitive data stored on file servers, endpoints, cloud storage, network file shares, databases and other repositories. Symantec DLP Network Discover is capable of high-speed scanning over large, distributed environments and can recognize and scan over 330 different file types, including custom file types. Symantec DLP Network Protec can automatically clean up and secure exposed files detected by Network Discover. It can take a range of remediation actions including quarantine or moving files, and enforcing encryption and digital rights management policies.

Protecting Data in the Cloud
The Symantec DLP Cloud Detection Service protects data in motion and data at rest across more than 100 sanctioned and unsanctioned cloud apps, including Office 365, G-Suite, Box, and Salesforce. It extends existing policies and detection capabilities to cloud applications, and can take actions to prevent exposure of sensitive files including, un-sharing, quarantining, and blocking them from leaving. It can also enforce encryption and digital rights management policies. Symantec DLP Cloud Service for Email performs the same function for corporate email traffic.

aurorait.com
sales@aurorait.com
888-282-0696