EXECUTIVE SUMMARY

As new technologies become available, it dramatically shifts the way we utilize enterprise data centers and organizations. Data centers are no longer limited to on-premise brick and mortar locations, and with technologies such as cloud, container services and serverless, organizations have to deal with an ever-evolving and changing infrastructure. This creates new challenges for securing these environments.

Trend Micro™ Deep Security™ platform, powered by XGen, is designed to alleviate these challenges.

Offering all of the capabilities that an organization needs to secure their environment - including intrusion prevention, anti-malware and application control - Deep Security’s single server provides you with the latest in threat technologies while helping with tool reduction.

For those running workloads on the Oracle Cloud Infrastructure, instructions on how to get up and running with Deep Security, including the basics of protecting your instances, have been included.

PROTECING ORACLE CLOUD WORKLOADS

ARCHITECTURE

Deep Security was specifically designed to address all security requirements of an organization’s workloads in a heterogeneous data center. This allows Deep Security to work in environments where other security applications may not be able to.


- **The Deep Security Manager** is the console used to provide a view of your organization’s computers you are protecting. The manager’s function is to define policy, apply security to the agents, and view dashboards and reports.

- **The Deep Security Relay** is responsible for distributing security and software updates in your environment. In order to reduce WAN bandwidth costs and provide redundancy to update distribution, it is recommended to have a relay group with one or more relays in each geographically-separated region.

- **The Deep Security Agent** is the component installed on each instance you wish to protect. It is responsible for executing security as determined by the policy applied via the Deep Security Manager.

Generally, the Deep Security Manager should be installed in the location where you have most of the workloads you wish to protect, which may include an on-premises or a virtual machine instance in your Oracle Cloud Infrastructure.

Details on the various deployment options are covered in the deployment sections for the Deep Security Manager, the Deep Security Relay, and the Deep Security Agent.
DEPLOYING THE DEEP SECURITY MANAGER

There are a few options for deploying the Deep Security Manager in your Oracle environment. The Deep Security Manager is provided as a software installer and can be installed on multiple operating systems. A relational database (not provided) is required before installation.

In order for the Manager to properly assign policy to a Deep Security Agent, there must be at least one-way communication between the Deep Security Manager and the instance on which it is installed.

THERE ARE TWO MAIN CONSIDERATIONS WHEN DEPLOYING THE DEEP SECURITY MANAGER:

• The location of the majority of the workloads you want to protect
• Network connectivity

One of the benefits of deploying Deep Security Manager in the Oracle Cloud Infrastructure is the ability for customers to quickly and easily set up Deep Security Manager in conjunction with an Oracle Database. This gives users the flexibility to deploy in a highly-available cloud environment, running within the same VCN, on dedicated hardware (Bare Metal), Exadata or Virtual Machines with RAC support.
CONSIDERATIONS FOR INSTALLING DEEP SECURITY MANAGER ON-PREMISES

If the majority of your workloads are in your data center, then the Deep Security Manager should be installed in your data center as well. In this case, you will require connectivity from your workloads in the cloud to your Deep Security Manager. This can be achieved by opening the necessary ports in your firewall or, optionally, you can use Oracle Cloud FastConnect to ensure bi-directional communication between your cloud and on-premises instances.
FIGURE 1: DEPLOYMENT ARCHITECTURE WITH A DEEP SECURITY MANAGER ON-PREMISES

CONSIDERATIONS FOR INSTALLING THE DEEP SECURITY MANAGER IN YOUR ORACLE CLOUD INFRASTRUCTURE VIRTUAL CLOUD NETWORK

If the majority of your workloads are in Oracle Cloud Infrastructure, you can install the Deep Security Manager inside your Virtual Cloud Network. Using network security lists, you can allow communication between the workloads you wish to protect and the Deep Security Manager.
FIGURE 2: DEPLOYMENT ARCHITECTURE WITH A DEEP SECURITY MANAGER IN ORACLE CLOUD INFRASTRUCTURE

DEEP SECURITY AS A SERVICE

Deep Security Manager is also offered as a service. If you do not want to maintain your own Deep Security Manager (and do not have data sovereignty needs) you can sign up for a Deep Security as a Service account. Deep Security as a Service provides the management console and can be used to protect both your on-premises and Oracle Cloud Infrastructure instances.

![Deep Security as a Service Diagram]

- Optionally use two Deep Security Relay Groups for keeping update traffic local to each site i.e. one Relay Group for Oracle Cloud workloads and one Relay Group for On-Premises workloads.
- No network access is required from Deep Security as a Service to Oracle Cloud or on-premise workloads.
- Use Network Security Lists to allow required communication flow between components.
FIGURE 3: DEPLOYMENT ARCHITECTURE WITH A DEEP SECURITY AS A SERVICE

DEPLOYING THE DEEP SECURITY RELAY

The Deep Security Relay downloads security updates from the Trend Micro ActiveUpdate Servers directly through your WAN connection, and software updates from the Deep Security Manager. When you use relays, security and software updates only need to be downloaded once through your WAN connection. Relays then function as update distribution centers and the security and software updates are downloaded from the specified relay by other agents when they are directed to do so by the Deep Security Manager.

For more information on Deep Security Relays visit:
https://help.deepsecurity.trendmicro.com/Set-Up-Relays.html

DEPLOYING THE DEEP SECURITY AGENT

Deep Security supports many operating systems and, as long as the instance is running an operating system that Deep Security supports, it can be protected. The first step to protecting an instance running on Oracle Cloud Infrastructure is to deploy the Deep Security Agent. Trend Micro has attempted to make deployment of the Deep Security Agent simple, offering multiple ways to deploy the Deep Security Agent to the cloud instances you wish to protect.

To learn more about how the Deep Security Agent can be deployed in your environment read the section that applies:

FOR DEPLOYMENT USING THE DEEP SECURITY SCRIPTS ON INSTANCES THAT ARE ALREADY RUNNING

Deep Security offers scripts that can be used to deploy the Deep Security agent on Linux and Windows instances.

To learn more, visit:

Many organizations use orchestration tools to perform common activities. Deep Security has a rich set of APIs and available scripts for orchestrating the deployment of the Deep Security Agent.

To learn more, visit:

FOR DEPLOYMENT OF THE DEEP SECURITY AGENT DURING PROVISIONING A NEW INSTANCE ON ORACLE CLOUD

When you provision a new instance on Oracle Cloud, you have the option to run scripts as the instance is created. To do this you can click the “Show Advanced Options” in the “Instance” section of the provisioning wizard:

- Copy the deployment script from Deep Security Manager and select the “Paste Cloud-Init Script” on the provisioning wizard.
- Paste the deployment script directly into the text field.

Figure 4: Show Advanced Options to Paste Cloud-Init Script
USING SMART FOLDERS TO VIEW YOUR ORACLE CLOUD INSTANCES
Deep Security does not offer full visibility in to your Oracle Cloud environment. When computers are added to your Deep Security Manager via deployment scripts they are added as physical computers.

On the Computers screen in Deep Security you can create a smart folder. Using attributes of the name that are unique to Oracle Cloud, you can group your Oracle Cloud instances.
USING SMART FOLDERS TO VIEW YOUR ORACLE CLOUD INSTANCES
Deep Security does not offer full visibility in to your Oracle Cloud environment. When computers are added to your Deep Security Manager via deployment scripts they are added as physical computers.

For more information on using smart folders in Deep Security Manager, visit:

ADDING PROTECTION
Deep Security Manager provides sample policies when it is installed. However, most organizations contain a diverse set of workloads. Deep Security allows you to create policies and assign them to the workloads you are protecting based on your needs and the requirements of your organization.

The Deep Security policy defines what protection is applied to a given host, and each security capability in Deep Security can be turned on or off and configured for your particular workload.

For information on creating a policy in Deep Security Manager visit:
https://help.deepsecurity.trendmicro.com/11_0/on-premise/Policies/create-policy.html
PROTECTION MODULES

When configuring a security policy, you need to define what modules are enabled and how they are configured. Outlined below is a brief overview of each capability along with a link to where you can find more information on configuration.

DEEP SECURITY ANTI-MALWARE

Deep Security’s anti-malware capabilities includes malware prevention with web reputation, predictive machine learning, and behavioral monitoring, and can be integrated with Trend Micro Deep Discovery for sandbox analysis. These techniques ensure your environment is safe from known and targeted attacks.

For more information on configuring anti-malware in Deep Security, visit:

DEEP SECURITY FIREWALL

The first layer of defense on any host is created by restricting access. Deep Security offers a stateful firewall that helps you lock down specific open ports and choose where connections can be made. It allows you to define the ports at a policy level so the same policy can be used for similar instances.

For more information on configuring the firewall in Deep Security, visit:
https://help.deepsecurity.trendmicro.com/11_0/on-premise/set-up-firewall.html

DEEP SECURITY HOST INTRUSION PREVENTION

Deep Security offers a host-based intrusion prevention system that examines network traffic flows in order to monitor network-based exploits. Like the firewall, intrusion prevention can be defined at policy level. This allows you to apply intrusion prevention rules based on the requirements of a given instance without having to assign all rules to protect from a network level.

For more information on configuring intrusion prevention in Deep Security, visit:

DEEP SECURITY APPLICATION CONTROL

Deep Security’s application control allows you to monitor software changes on your protected servers and prevent malicious applications from being able to be executed. Application control can be used to prevent unauthorized software from running until it is explicitly allowed (whitelisted) or it can allow unauthorized software to run until it is explicitly blocked (blacklisted).

For more information on configuring application control in Deep Security, visit:
https://help.deepsecurity.trendmicro.com/11_0/on-premise/set-up-app-control.html

DEEP SECURITY INTEGRITY MONITORING

The Deep Security integrity monitoring capability allows you to observe aspects of the instance for indicators of compromise. By monitoring specific directories, registries or processes, Deep Security can alert you if anything has changed on your server. Integrity monitoring also allows you to meet PCI compliancy needs for files that may contain payment card information.

For more information on configuring integrity monitoring in Deep Security, visit:
https://help.deepsecurity.trendmicro.com/11_0/on-premise/set-up-integrity-monitoring.html

DEEP SECURITY LOG INSPECTION

The Deep Security log inspection capability allows you to monitor significant events that may be occurring in your operating system or application logs. Log inspection can also help you detect suspicious behavior in your environment.

For more information on configuring log inspection in Deep Security, visit:
https://help.deepsecurity.trendmicro.com/11_0/on-premise/set-up-log-inspection.html
SUMMARY: DEEP SECURITY AND ORACLE CLOUD INFRASTRUCTURE

Deep Security has been designed to help you meet the security challenges faced as your organization evolves from on-premises to the cloud. With thousands of customers and millions of servers protected, Trend Micro Deep Security is designed for the hybrid cloud, delivering a cross-generational blend of threat defense techniques in a single product that has been optimized for securing physical, virtual, cloud (such as Oracle Cloud Infrastructure), and container workloads. Delivering protection from advanced attacks (like ransomware) and offering multiple capabilities in a single product that allows for vendor consolidation, Deep Security solves real-world problems by simplifying operations without compromising security.

Ranked #1 in market share by IDC and noted by Forrester as having 13 of 22 cloud workload security capabilities, you can feel confident in choosing Deep Security to protect your hybrid cloud deployments.

Learn more at www.trendmicro.com/hybridcloud.