Endpoint Protection Platform for Virtual Desktop Infrastructure (VDI) Datasheet

Introduction

The SentinelOne Endpoint Protection Platform offers a lightweight and efficient solution to secure the growing need for virtual environments, including thin clients, layered applications, and other VDI scenarios.

VDI solutions have been an underlying IT trend in some of the key business sectors for a number of reasons ranging from cost, compliance and seasonality of workers. And improvement storage performance improvements will only drive the adoption further.

Securing VDI deployments is imperative to minimize the business risk and achieve regulatory compliance, especially in the face of increasing magnitude and complexity of cyber threats. VDI also presents some unique challenges for security along with some common issues seen in traditional endpoint deployments.

Patching is not always rapid:

Patching requires updating the golden image and need to be certified before rollout.

Balancing cost and complexity:

One of the biggest desired benefits of virtualization is cost savings with oversubscription.
VDI implementations tend to be as light-weight as possible to optimize deployments and maximize resource utilization. Consequently, the layers of security controls are always deep.

False sense of security:

Given the temporal nature of VDI sessions, there is sometimes a false sense of security that drives user behavior. The threats to this environment however are as real – malware such as screen scrapers and key loggers put user credentials and business information at an equivalent risk as traditional endpoint because the virtual desktop is not isolated from corporate environment.

VDI performance accentuates risk:

Traditional AV scans that cause performance problems on traditional endpoints with dedicated CPU experience a more extreme resource crunch when running in shared virtual CPU environment resulting in AV storms. Such scans can take an order of magnitude more time and also negatively impact user experience.

SentinelOne Endpoint Protection Platform for VDI

The SentinelOne Endpoint Protection Platform (EPP) for VDI helps customers address the challenges face with traditional VDI security. The SentinelOne agent deploys in a VDI environment as a light-weight agent consuming minimal execution resources. Additionally, it does not require signature updates that increase CPU, memory or I/O contention. The reduce resource requirements enables organizations to maximize VM density on their virtual infrastructure.

The SentinelOne EPP for VDI supports the same level of protection for a VDI environment as offered with physical endpoint devices with pre-execution, on-execution and post-execution scans for prevention, detection and response. SentinelOne EPP supports full spectrum threat coverage with reputation engine, local analysis for file-based malware, deep inspection for document based malware, scripts/PowerShell, memory based attacks, weaponized documents and warranty against ransomware attacks. Additionally, SentinelOne EPP can enable automated zero-touch mitigation and remediation to accelerate speed of response and minimize business risk.

SentinelOne EPP can be deployed to support both persistent and non-persistent VDI deployments with retention of historical threat information even if the devices are deleted. Additionally, it supports both on-premise or cloud-based virtual desktop solutions:

Desktop virtualization:

Also referred to as server-based VDI, desktop virtualization allows hosting a desktop operating system in a virtual machine on a centralized server. Examples of enterprise application virtualization software include Citrix XenDesktop, Microsoft App-V, VMware Horizon and Systancia AppliDis.

Terminal Services:

A server-based computing and presentation virtualization component to access applications and data on a remote computer over a network. Examples include Microsoft Windows RDP and Citrix XenApp.

Desktop as a Service (DaaS):

Remote desktop virtualization from SaaS Cloud computing. Examples of enterprise DaaS environments include VMware Horizon and Amazon WorkSpaces.

Benefits

Stronger security

- Visibility and coverage across the kill chain with pre-execution, on-execution and post-execution scans
- Detection, prevention, response, remediation and forensics capabilities in one agent/one console architecture

Better scalability

- Higher VM density via the use of artificial intelligence and behavioral analytics that removes the need for daily/ weekly signature updates or a full disk scan

Deployment flexibility with ease of manageability

- Single agent, single console architecture streamlines deployment and manageability
- Automatic decommissioning of VDI instances no longer in use as part of the policy
- Support all VDI use cases - persistent and non-persistent
- Managed by SaaS console or On-Prem
- Automatic decommissioning of VDI instances no longer
- Concurrent license model to save on your security coverage costs

SentinelOne is recognized as a Visionary on the 2017 Gartner MQ for Endpoint Protection Platforms.

Ransomware protection. Guaranteed.

SentinelOne covers customers up to $1,000/ endpoint (up to $1M total) to recover files in the event of an undetected ransomware attack.

Technical Requirements

USER ENDPOINT CLIENTS

Operating Systems

Windows 7, 8, 8.1, 10
Mac OSX 10.9.x, 10.10.x, 10.11x, macOS 10.12x
CentOS 6.5, 7.0, 7.2
Red Hat Enterprise Linux 6.5, 7.0, 7.2
Ubuntu 12.04, 14.04, 16.04, 16.10

VIRTUAL ENVIRONMENTS

Citrix XenDesktop and XenApp
VMware Horizon
Systancia AppliDis
Microsoft App-V and Windows RDP
Amazon WorkSpace

SentinelOne is a certified AV replacement for Windows and MacOS.

TUCANA
MASTERS IN MEASUREMENT
www.tucana.com
info@tucana.com

For more information about SentinelOne Next-Generation Endpoint Protection Platform and the future of endpoint protection,

SentinelOne
The future of endpoint security

© 2017 SentinelOne, Inc. All rights reserved.