Ransomware Protection- VMware Security Solutions Guide

VMware Maturing your Security

© VMware LLC.

Table of contents

vmware by Broadcom © VMware LLC.

Ransomware Protection- VMware Security Solutions Guide

Overview

Over the past decade the security industry continues to be plagued by ransomware and adversarial breaches. Observations by VMware and other industry vendors highlights the increase in destructive characteristics often times crippling organizations. According to VMware's Global Security Insights Report,

> Ransomware ranked as second most common vectors that caused breaches.

In the current landscape it is not if, but when you will be hit by a ransomware threat.

This solutions guide is designed to provide an overview of VMware Security's capabilities aligned to the Ransomware lifecycle.

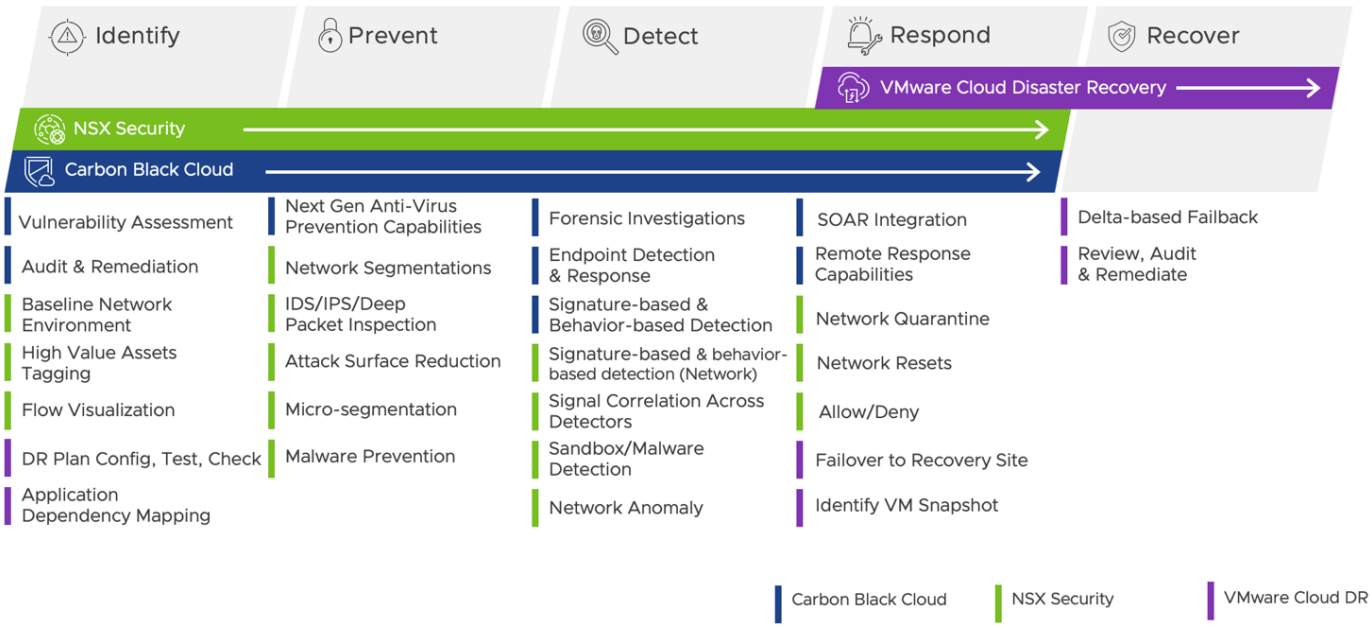
© VMware LLC.

VMware Security

The goal of **Maturing Security** is to evolve your threat defenses to defend against adversarial threats including, but not limited to, ransomware. This solutions guide will detail VMware Security's ability to cover the full ransomware protection cycle from "Identify" to "Recover" (NIST Ransomware Risk Management: A Cybersecurity Framework):

- **Identify**: Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.[1]
- **Prevent**: Develop and implement the appropriate safeguards to ensure the delivery of services.[1]
- **Detect**: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.[1]
- **Response**: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.[1]
- **Recover**: Develop and implement the appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity event.[1]

The following image shows coverage and capabilities of the VMware solutions **VMware Carbon Black Cloud**, **NSX Security**, and **VMware Cloud Disaster Recovery** across the NIST Ransomware framework.

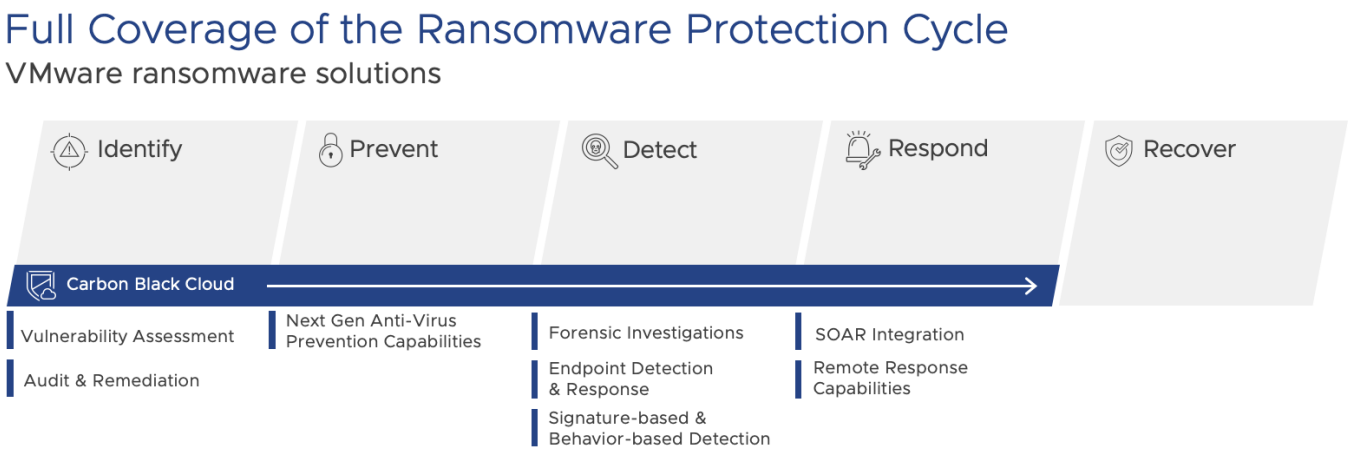


It is important to have capabilities to cover the entire Ransomware Protection cycle. VMware Security is looking at connected control points across endpoints, workloads, network, identity, and cloud; both natively and integrated to deliver higher fidelity alerts. Carbon Black, NSX, and VMware Cloud DR can not only cover the cycle with robust security capabilities but also operationally enable each other. With Carbon Black and NSX, VMware can provide robust security capabilities and use the investigative data they provide to inform solutions like VMware Cloud DR.

Continue to the subsequent sections to dive into each of the products specific capabilities. This solutions guide will cover the **Carbon Black Cloud**, **NSX Security**, and **VMware Cloud Disaster Recovery**

© VMware LLC.

VMware Carbon Black



Product Overview

VMware Carbon Black is a next-gen AV and endpoint detection and response (EDR) solution with multiple layers of prevention, robust visibility, and response capabilities baked into a single central cloud console.

Key Advantages for Ransomware Protection:

- **Multi-layered prevention approach** provides protection against advanced threats
- Protect and detect **ransomware like behaviors**
- **Built-in response capabilities** in the console that decrease time to resolution
- **Ability to search and filter across all events in the environment for the past 30 days** giving admins confidence they have the data they need for investigation
- **Alert visualization** that gives an easy-to-understand view of events occurring during an attack

Get Hands-on

At VMware, there are several ways to get hands-on with our products today.

Review the below tabs to access the labs now.

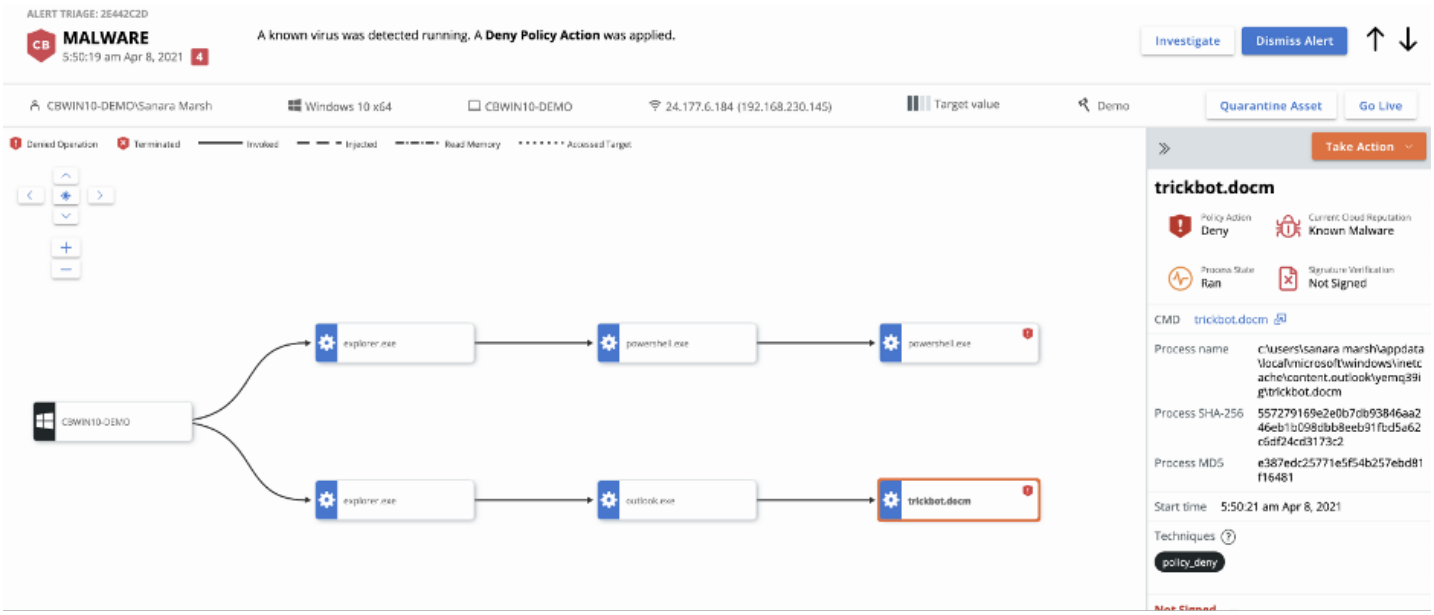
- Malware Lab
- Threat Hunting Lab

VMware Carbon Black Malware Lab

This walkthrough will enable you to get hands-on with the VMware Carbon Black Cloud. The Malware Lab contains actual attacks that you can run live in a test environment to see how prevention and visibility work against the Carbon Black Cloud solution suite.

To learn more, access the VMware Carbon Black Cloud Malware Lab

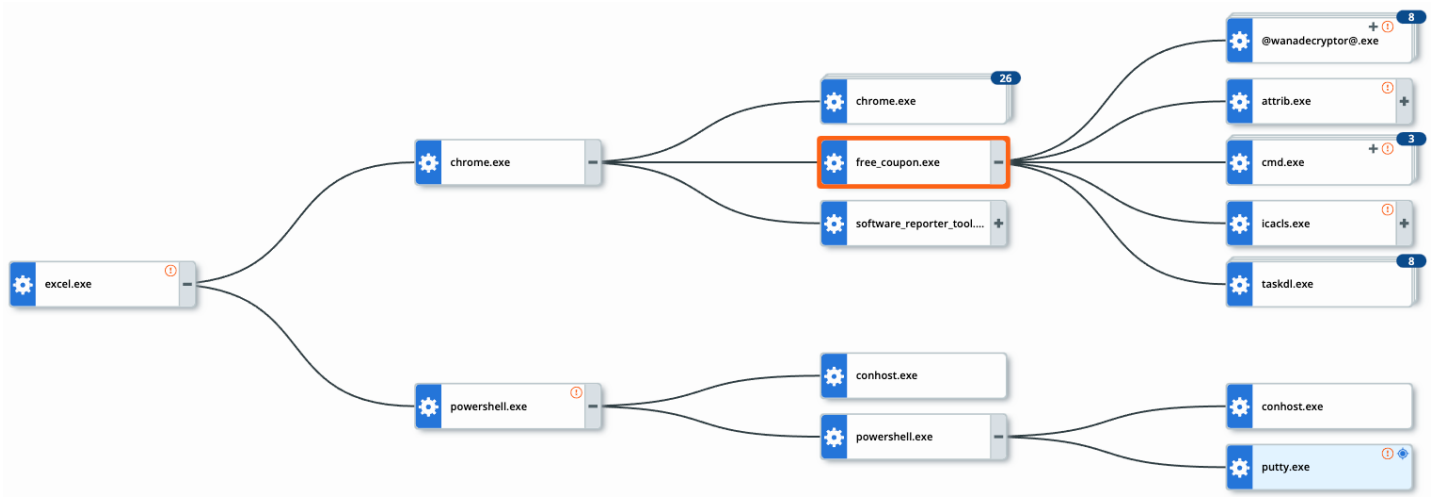
© VMware LLC.



VMware Carbon Black Threat Hunting Lab

Threat hunting is a very important activity in securing modern networks. While we want it to be as automated as possible, it requires a degree of human analysis by cybersecurity professionals. Fortunately, VMware Carbon Black Cloud simplifies and enriches the data it shows and alerts on so that even individuals with little to no formal training in threat hunting can understand what is occurring on a system when they see it in their VMware Carbon Black Enterprise EDR dashboard.

Access CB Ransomware - Threat Hunting lab.



Additional Resources

To learn more about VMware Carbon Black products, visit our Product Paths in TechZone. Product learning paths are designed to take you from A-Z to understand everything from product overviews to optimization/best practice content per product.

Product Learning Path

These paths help you understand the breadth of our products. They are designed to have something for people of every experience level.

Carbon Black Cloud Endpoint Standard Activity Path

June 02, 2021

The fastest way to learn Carbon Black Cloud Endpoint Standard! Using articles, videos, and labs, the activity path provides curated assets to help you level up [• • •]

Tags

Start Learning

Carbon Black Enterprise EDR Activity Path

June 02, 2021

VMware Carbon Black Enterprise EDR is an advanced threat hunting and incident response solution delivering continuous visibility for top security [• • •]

Tags

Start Learning

Carbon Black Audit & Remediation Activity Path

June 09, 2021

Audit and Remediation is a real-time assessment and remediation solution that gives teams faster, easier access to audit and change the system state of [• • •]

Tags

Start Learning

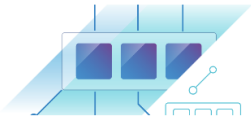
Carbon Black Workload Activity Path

June 02, 2021

Tightly integrated with vSphere, VMware Carbon Black Cloud Workload provides advanced security that alleviates installation and management overh [• • •]

Tags

Start Learning



Carbon Black Container Activity Path

March 15, 2022

Trying to move towards enterprise-grade container security at the speed of DevOps? Want to provide your security teams the visibility and the ability to [• • •]

Tags

Start Learning

Carbon Black App Control Activity Path

June 03, 2021

Carbon Black App Control is used to lock down servers and critical systems, prevent unwanted changes and ensure continuous compliance with [• • •]

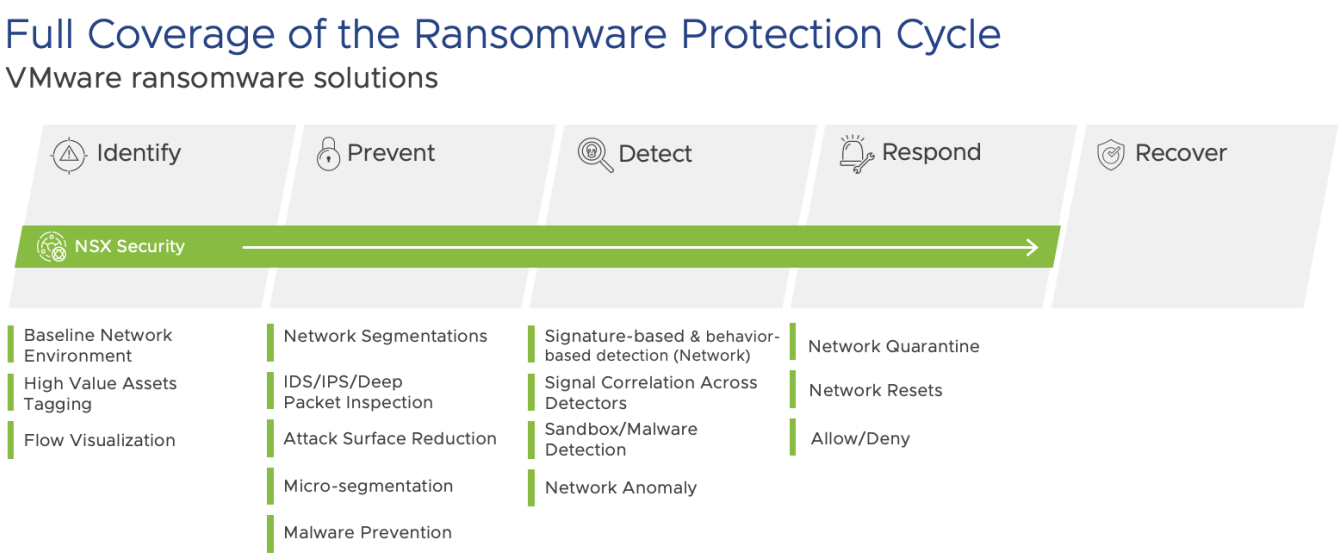
Tags

Start Learning

© VMware LLC.

NSX Security

1232x639



Product Overview

Leverage a distributed network security architecture delivered in software and embedded in your infrastructure to detect and stop threats inside your network. The real damage of a breach happens when attacks can move laterally in your network making East-West the new battleground. NSX Firewall enables you to secure against threats with a modern distributed architecture that's easy to operationalize and scales across your multi-cloud environments.

Key Advantages for Ransomware Protection:

- **Complete network security coverage** across all traffic flows and workload types
- **Analyze advanced threats** with a full-system emulation sandbox
- **Easily create, enforce, and manage** granular micro-segmentation policies to secure the East-West
- **Network quarantine** infected guests preventing lateral movement
- **Flow visualization** to understand malicious traffic and activity

Additional Resources

1. **NSX TechZone Security Resources**: https://nsx.techzone.vmware.com/security-resources
2. **NSX Firewall Solutions Page:** https://www.vmware.com/solutions/nsx-firewall.html
3. **Micro-Segmentation Solutions Page:** https://www.vmware.com/solutions/micro-segmentation.html

© VMware LLC.

VMware Cloud Disaster Recovery

Product Overview

VMware Cloud Disaster Recovery is VMware's on-demand disaster recovery service that is delivered as an easy-to-use SaaS solution and offers cloud economics to help keep your disaster recovery costs under control.

Key Advantages for Ransomware Recovery:

Keeping in mind that VMware Cloud Disaster Recovery does not detect, prevent, or remove ransomware, it does provide the following capabilities to help recover from a ransomware attack:

- **Offsite air-gapped backups** reduce the direct impact of the attack
- **Immutable VM snapshots** with data integrity features ensure previous clean recovery points can't be altered by malware
- **RPOs as low as 30 minutes** and deep history of snapshot copies
- **Instant Power-On of VMs** in an on-demand SDDC in the cloud
- **Granular recovery of files and folders** without powering on VMs
- **Non-disruptive testing of recovery plans** drives recovery readiness—iterate over potential recovery points to find the best candidate to conduct failover and failback operations
- **Greenfield, clean operating Isolated Recovery Environment (IRE)** to recover VMs
- **Automated** recovery at the scale of 1000s of VMs

Additional Resources

1. **VMware Cloud DR Product Page**: https://www.vmware.com/products/cloud-disaster-recovery.html
2. **VMware Cloud DR TechZone**: https://vmc.techzone.vmware.com/resource/introduction-vmware-cloud-disaster-recovery-vcdr
3. **VMware Cloud DR Ransomware Recovery**: https://www.vmware.com/products/cloud-disaster-recovery/ransomware.html

© VMware LLC.

Summary and Additional Resources

Summary

Ransomware is a serious threat to all organizations across all industries. VMware provides many capabilities to protect organizations from ransomware attacks. If organizations are infiltrated, VMware technologies enable security operations to protect, detect and respond to these threats

Additional Resources

1. **NSX TechZone Security Resources**: https://nsx.techzone.vmware.com/security-resources
2. **Carbon Black TechZone**: https://carbonblack.vmware.com/

Changelog

The following updates were made to this guide:

Date	Description of Changes
4/29/2022	

Feedback

Your feedback is valuable.

To comment on this paper, contact VMware Carbon Black Technical Marketing techzone-sbu@vmware.com.

© VMware LLC.

Copyright © 2005-2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.