VMware Carbon Black Cloud Reference Architecture

vmware

Table of Contents

Overview

Introduction

The reference architecture document provides a standardized blueprint or template that outlines the key components and design principles for the Carbon Black solution.

Audience

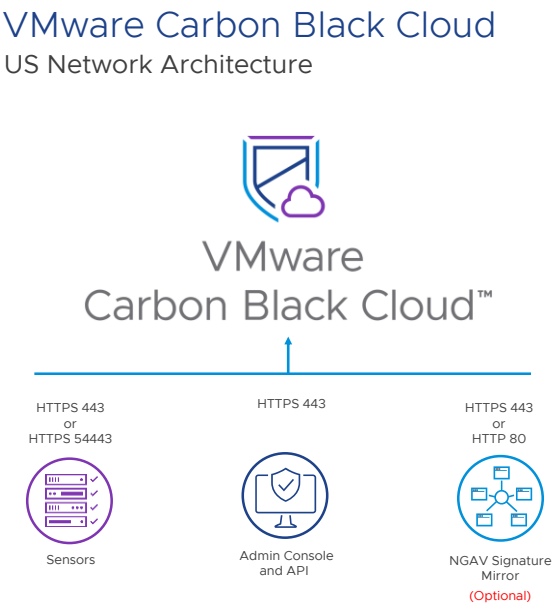
This document is intended for architects, developers, and other stakeholders involved in designing, implementing, and maintaining a system.

Network Architecture

Introduction

The VMware Carbon Black Cloud (CBC) is a cloud solution running on a standard client-server model. No infrastructure is needed to support the management and deployment of the CBC.

US Network Architecture



Sensors
- https://dev-prod05.conferdeploy.net

Admin Console and API
- https://defense-prod05.conferdeploy.net

Unified Binary Store Download
- https://cdc-file-storage-staging-us-east-1.s3.amazonaws.com

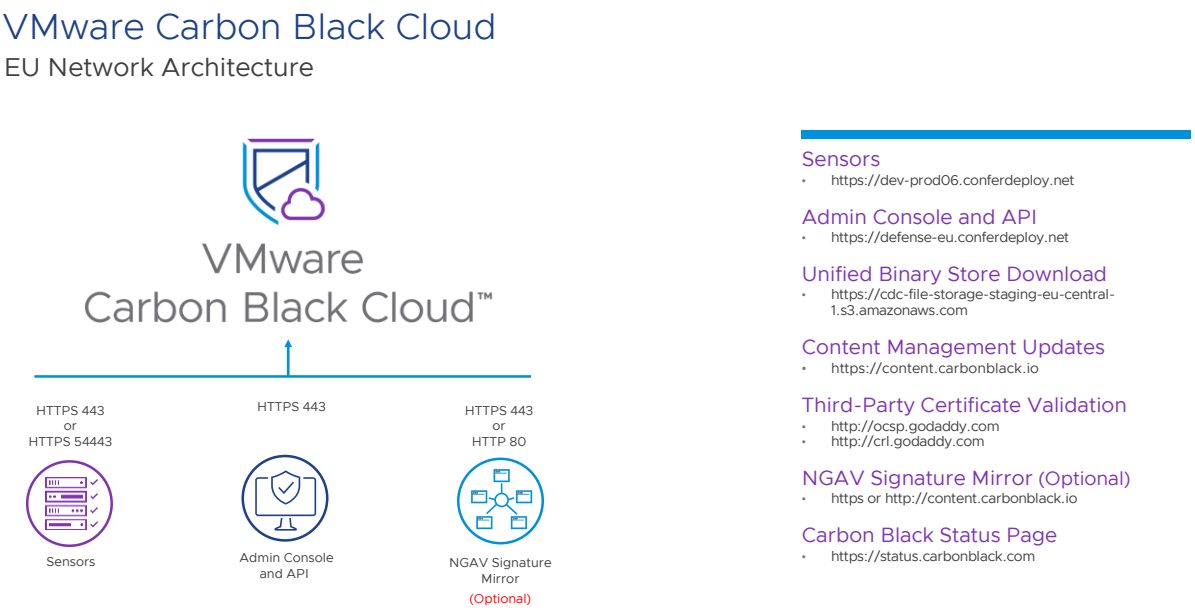
Content Management Updates
- https://content.carbonblack.io

Third-Party Certificate Validation
- http://ocsp.godaddy.com
- http://crl.godaddy.com

NGAV Signature Mirror (Optional)
- https or http://content.carbonblack.io

Carbon Black Status Page
- https://status.carbonblack.com

EU Network Architecture



Sensors: Communication between the sensor and the console/backend is done using this URL. If you do not make specific network firewall changes to access the Carbon Black Cloud backend applications, the sensors try to connect through existing proxies.

Admin Console and API: URL for console access and API requests.

Unified Binary Store download: The Unified Binary Store (UBS) is a Carbon Black Cloud service responsible for storing all binaries and the corresponding metadata for these binaries. UBS obtains data on first execution of a binary.

Content Management Update: URL for the UBS, signatures, and dynamic rules engine updates

Third-Party Certificate Validation: URL for verifying sensor comm certificates. The crl.godaddy.com and ocsp.godaddy.com domains use OCSP (Online Certificate Status Protocol) and Certificate Revocation List (CRL) checks to validate a sensor's install certificate.

NGAV Signature Mirror: Updating signature pack susing local server

Carbon Black Status: Carbon Black Status page.

Note: Operational environments that implement a man-in-the-middle proxy should note that additional third-party certificate validation URLs can be needed depending on the server certificates that the proxy uses. Additional URLs include anything specified under the "CRL Distribution Points" and "Authority Information Access" extensions of the proxy server SSL certificate. Failing to allow communication to third-party certificate validation URLs on TCP port 80 can lead to communication failures between the sensor and the

backend.

Summary and Additional Resources

Conclusion

This document helped you get a high-level understanding and overview of the VMware Carbon Black Cloud architecture.

Additional Resources

For more information about VMware Carbon Black Cloud, you can explore the following resources:

- TechZone – Additional Technical resources and demos
- VMware Docs – Product documentation, OER guides.
- Uex – Carbon Black User exchange and community pages
- Developer Network – Details on our Open APIs, integrations and platform SDKs.

Changelog

The following updates were made to this guide:

Date	Description of Changes
2023/03/06	• Guide was published.

Feedback

Your feedback is valuable.

To comment on this paper, contact VMware Security Business Unit Technical Marketing at sbu_tech_content_feedback@vmware.com

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.