VMware Carbon Black Cloud Reference Architecture

Table of contents
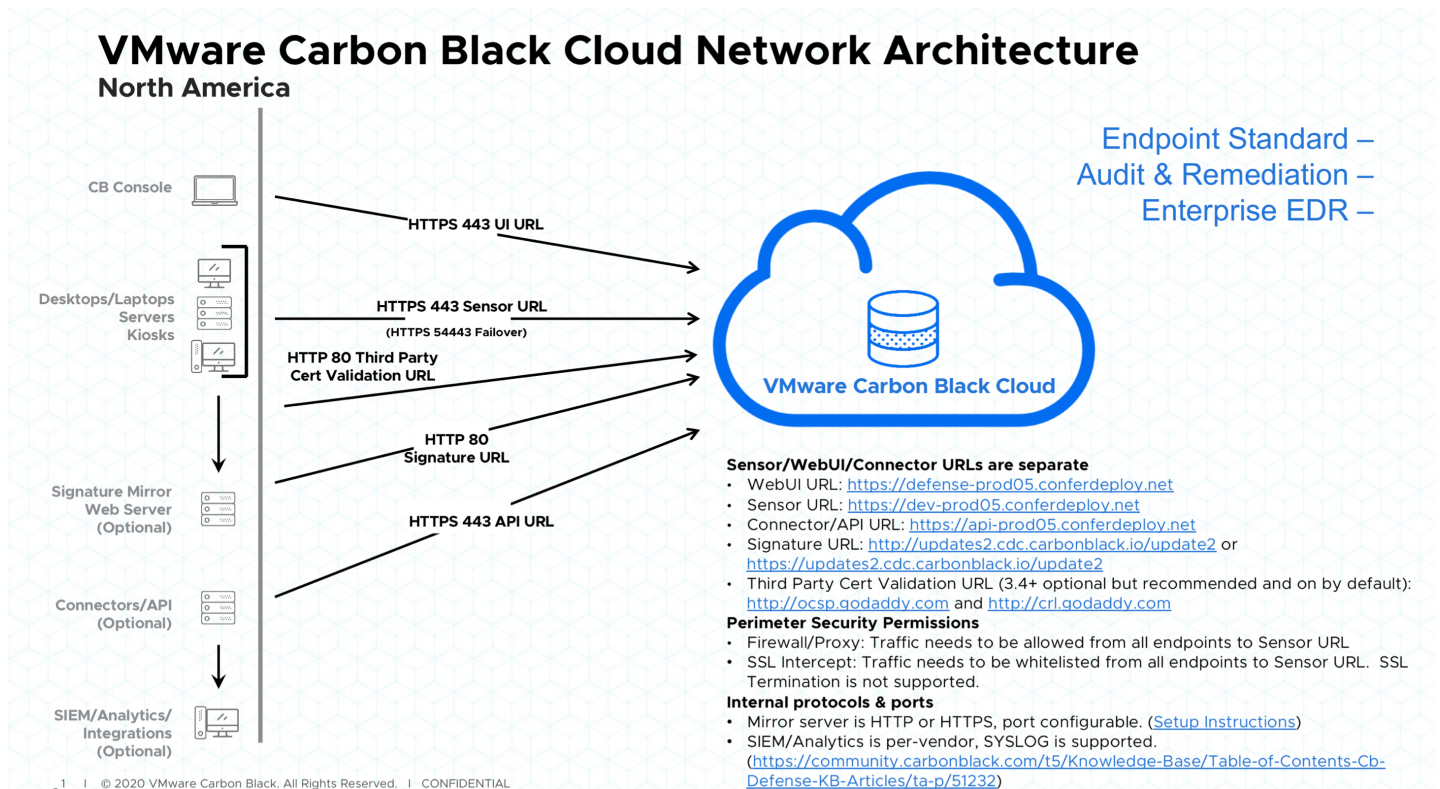
VMware Carbon Black Cloud Reference Architecture

VMware Carbon Black Cloud Architecture Overview

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.

Network Architecture

- **Dashboard (UI/Console) Services**: The Dashboard Services supply login and the WebUI console for the VMware Carbon Black Cloud.

- **Devices Services**: Device Services provides connectivity for all sensor-to-Cloud communications, including;
  - Registration/Installation of Sensors
  - Uploading Event Telemetry
  - New executable reputation lookup
  - Receive Policy Updates and Actions from the Web UI console

- **Event Processing Services**: The Event Processing Services handles the ingestion and indexing of events uploaded from an endpoint by the Endpoint Standard Sensor.

- **Notification Services**: Notification Services enable email & SIEM notifications to send directly from the VMware Carbon Black Cloud.

- **API Services**: Endpoint Standard and the VMware Carbon Black Cloud offers many API Services like:
  - CBAPI & Rest APIs
  - SIEM Connectors
  - Two-Factor Authentication
  - SAML Logins Learn more about the Endpoint Standard APIs here.

- **CDC Reputation Services**: CDC Reputation Services deliver near real-time reputation on files discovered by endpoints running Endpoint Standard.

- **VMware AppDefense Integration Service (Optional Component)**: The VMware AppDefense Integration Service brings workload and endpoint protection to the next level. With the integration in place alerts, actions, and remediation actions are shared between the two consoles, giving security administrators unparalleled visibility.
- **Cloud Analysis Service (Optional Component):** Available for configuration in the Web UI console under the Policy setting "Submit Unknown Binaries for Analysis", the Cloud Analysis Service uploads a copy of unique executables to the CDC Reputation Services for review.
- **Managed Detection (Optional Component):** VMware Carbon Black Managed Detection is a specialized team with dedicated services to monitor and help triage alerts from endpoints.

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 Endpoint Standard, explore our Activity Paths. The activity path provides step-by-step guidance to help you increase your understanding of Carbon Black, including articles, videos, and labs.