vFORUM 2019

NS188

VMware Carbon Black で実現する Intrinsic Security

VMware Carbon Black
テクニカルディレクター・エバンジェリスト
大久保　智

vmware

免責事項

- このセッションには、現在開発中の製品/サービスの機能が含まれている場合があります。
- 新しいテクノロジーに関するこのセッションおよび概要は、VMware が市販の製品/サービスにこれらの機能を搭載することを約束するものではありません。
- 機能は変更される場合があるため、いかなる種類の契約書、受注書、または販売契約書に記述してはなりません。
- 技術的な問題および市場の需要により、最終的に出荷される製品/サービスでは機能が変わる場合があります。
- ここで検討されているまたは提示されている新しいテクノロジーまたは機能の価格およびパッケージは、決定されたものではありません。

10/8/2019

https://www.carbonblack.com/2019/10/08/delivering-intrinsic-intelligent-and-informed-security-vmware-completes-acquisition-of-carbon-black/

Agenda

Carbon Black について

Endpoint Detection and Response とは

VMware が目指すIntrinsic Security

Carbon Black について

Carbon Black Inc.

顧客数	: 6,000 +
Fortune 100	: 35 社
パートナー	: 500 + 社
連携製品	: 140 + 製品
従業員	: 1,100 + 人

本社：Waltham, MA
設立：2002年

Vision :
A World Safe from Cyber Attacks

Endpoint Detection and Response とは

例えば、社外からこんな連絡がありました

御社のネットワークから abc.com 宛に
不審な通信が発生しています。

従来の対応

実施する作業例

ゲートウェイ製品、プロキシのログ等を確認し、不審な通信を行った端末の特定を実施

端末を特定後、詳細を調査、従来型 AV でフルスキャン

フルスキャンしても何も出てこないため、再イメージ

作業により得られる結果

複数機器のログを解析し、工数をかけて端末を特定

なぜ不審な通信をするに至ったかは把握不可

原因が特定できないため、同じ事象が発生する可能性が残存

例えば、社内からこんな連絡がありました

メールに添付された Excel を開いたら青い画面が数秒表示された。
その後いくつかファイルを開けなくなった。

従来の対応

実施する作業例

従来型 AV を使ってフルスキャン

フルスキャンしても何も出てきないので端末回収

回収した端末の調査

作業により得られる結果

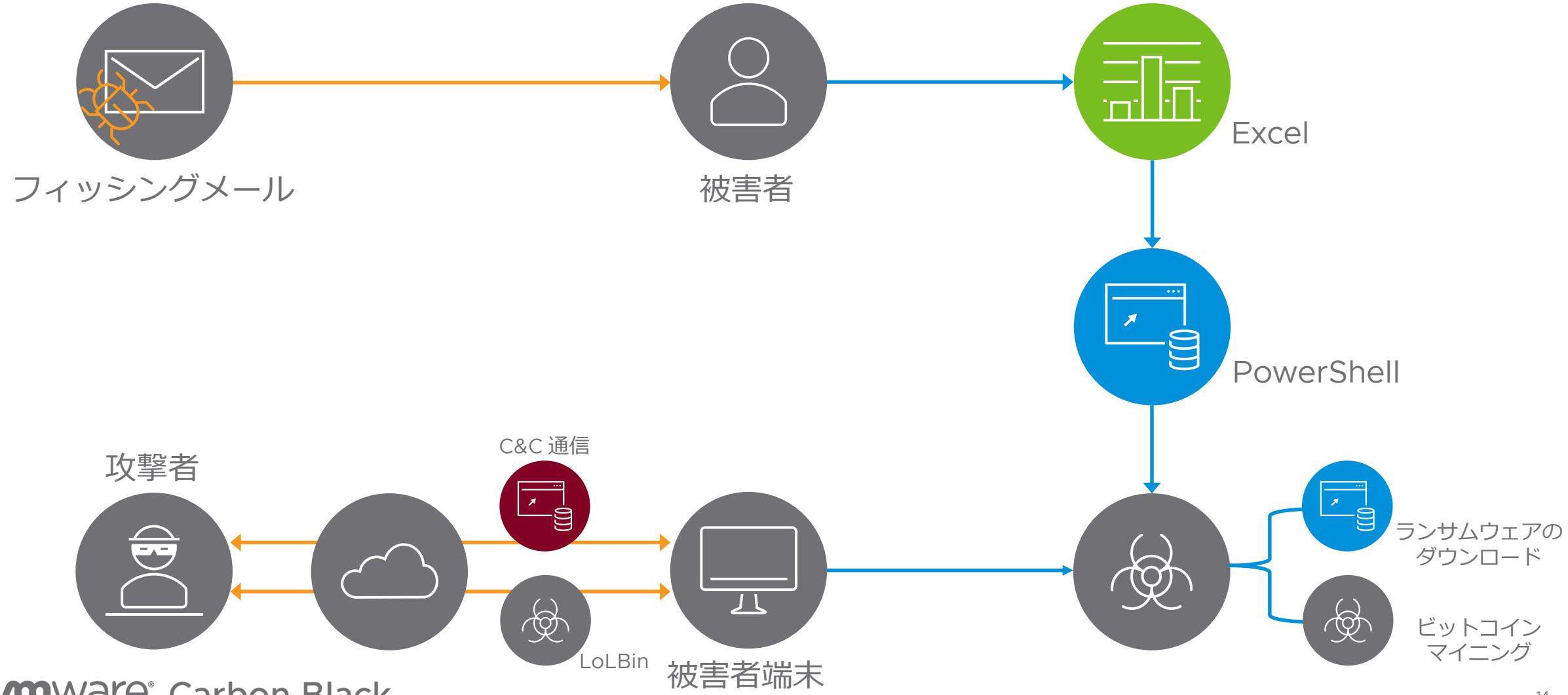
端末調査により現況の把握はできたが、感染経路の特定が不明

感染原因が不明のため、同事象が再発する可能性が残存

端末上で
何が起こっていたのか
見てみましょう

デモ動画

補足：実際の動き



補足：Living Off the Land（環境寄生）攻撃

攻撃者は端末上に既に存在するツールを使います。
そのため、攻撃を検知をするのが
これまでよりも一層難しくなっています。

PowerShell

SSH

WMI

.NET

従来の調査方法と課題

従来の調査方法

ログの収集（アンチウイルス、HIPS、認証、
その他のセキュリティ製品）

資産管理ツール

個別の調査ツール

都度、イベント / 情報を収集

従来の調査方法の課題

多数の製品が生成したログの解析が必要

調査開始時に必要なログが手元にない可能性

端末毎にログを都度収集

情報収集が遅くなり、解析 / 判断に時間は必要

情報が断片的で影響範囲の特定、
全体像の把握や絞り込みが困難

従来の調査方法と課題

世に EDR が出てきた背景

従来の調査方法

ログの収集（アンチウイルス、HIPS、認証、
その他のセキュリティ製品）

資産管理ツール

個別の調査ツール

都度、イベント / 情報を収集

従来の調査方法の課題

多数の製品が生成したログの解析が必要

調査開始時に必要なログが手元にない可能性

端末毎にログを都度収集

情報収集が遅くなり、解析 / 判断に時間は必要

情報が断片的で影響範囲の特定、
全体像の把握や絞り込みが困難

Endpoint Detection and Response に求められる機能

検知

セキュリティインシデントであるかに関わらず、端末上の動作を記録し、集中管理

端末の接続状況に関わらず迅速に調査を進めることが可能

トリアージ・調査

影響範囲の特定・
根本原因の調査が可能

被疑端末のネットワーク隔離が可能

復旧

遠隔より、マルウェアの削除が可能

リモート操作機能による端末の復旧支援が可能

事故後の対応

同事象が発生した際に検知可能

セキュリティポリシーの見直し・強化の判断材料

EDR がある場合
どう対応できるのか続きは
Carbon Black ブースで！

VMware が目指す
Intrinsic Security

Intrinsic = ??

basic to a thing, being an important part of making it what it is [US]

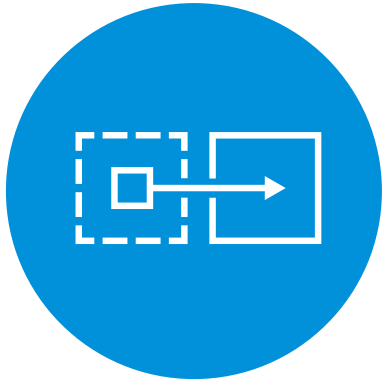
being an extremely important and basic characteristic of a person or thing [UK]

Intrinsic Security = ??

VMware 製品に組み込まれる
セキュリティ機能

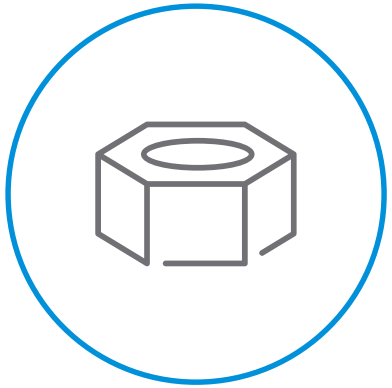
Security Must Be Transformed

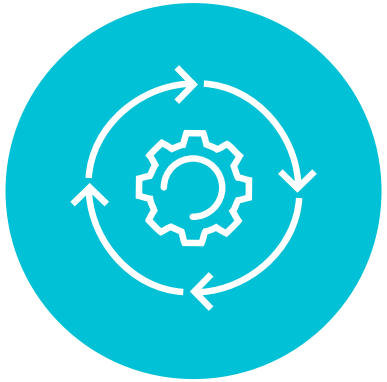
変革が求められているセキュリティのあり方



Built-in

Bolted-on





Proactive

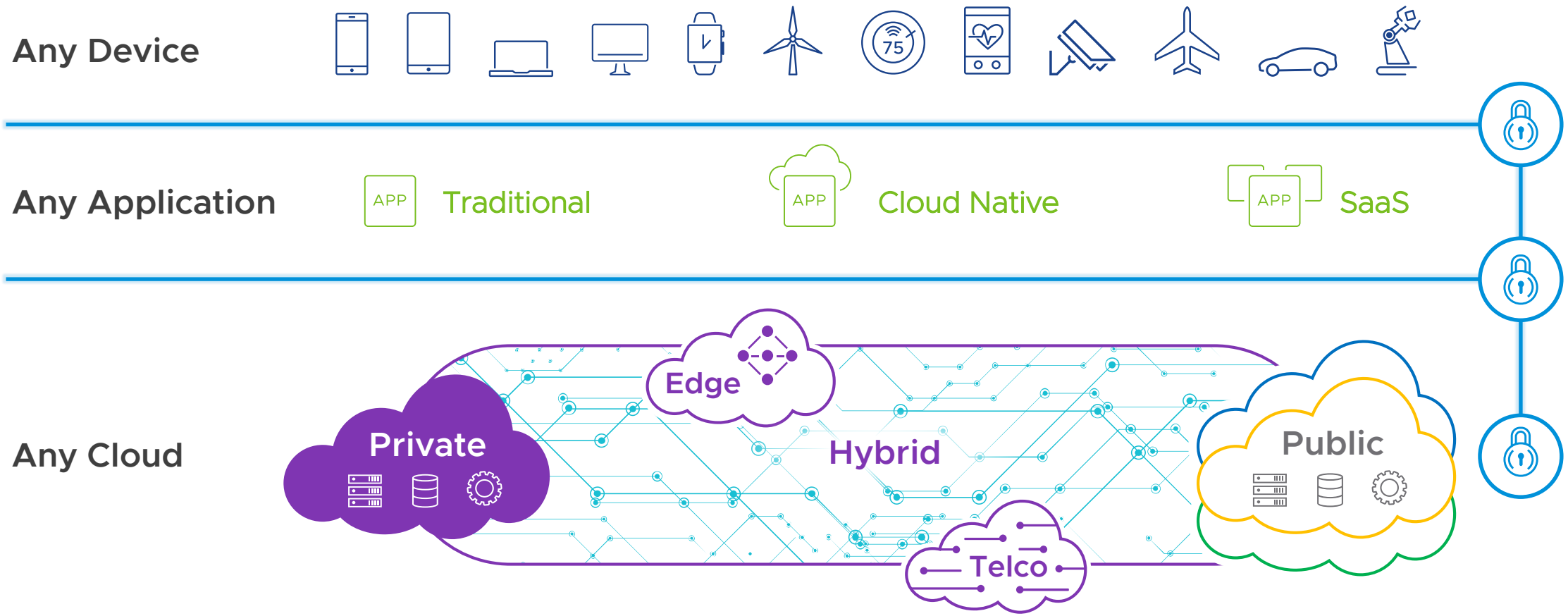
Reactive

Aligned

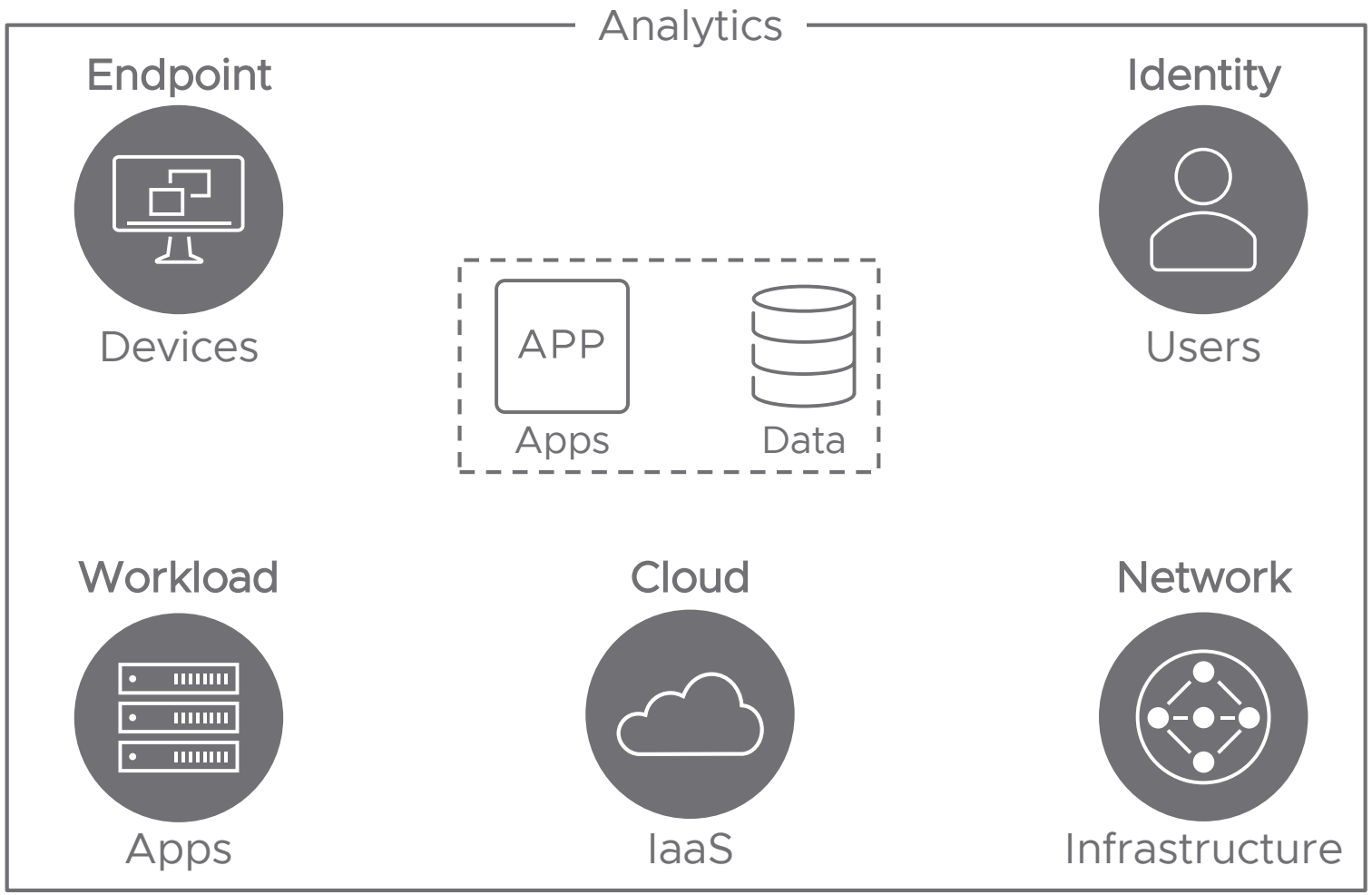
Siloed

VMware Vision

The Essential, Ubiquitous Digital Foundation

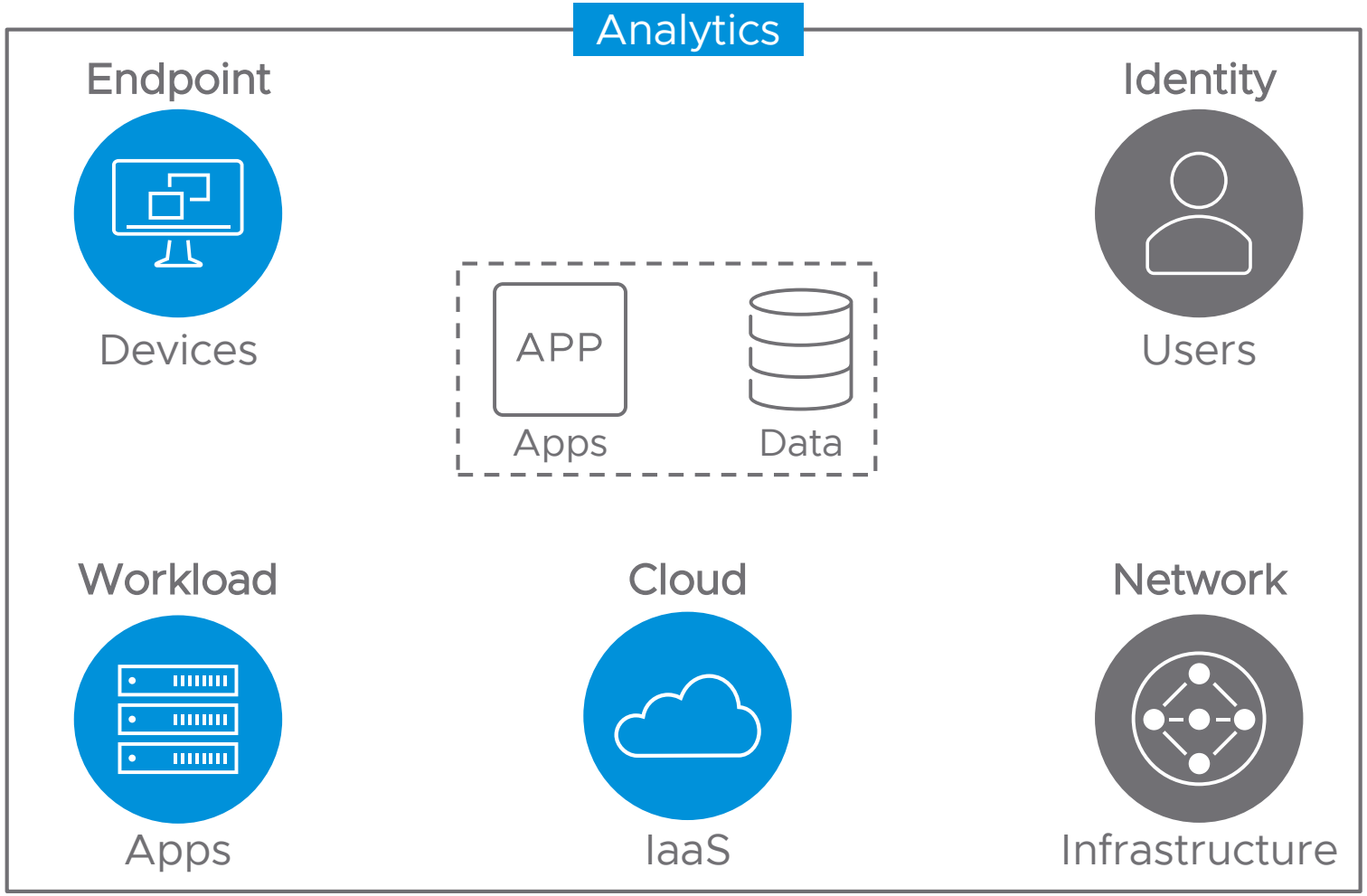


The Intrinsic Security Layer



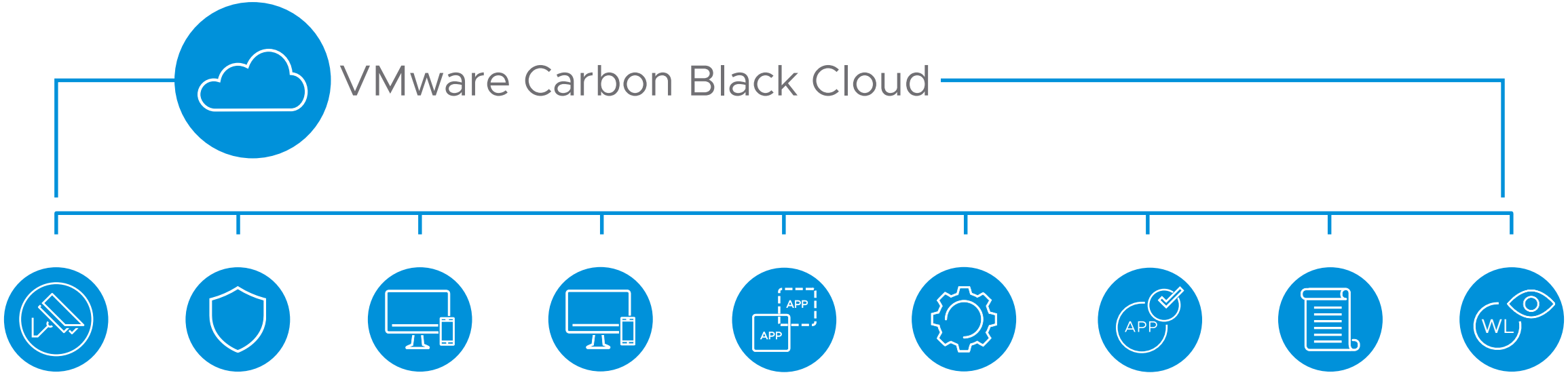
The Intrinsic Security Layer

最後のピース：Carbon Black

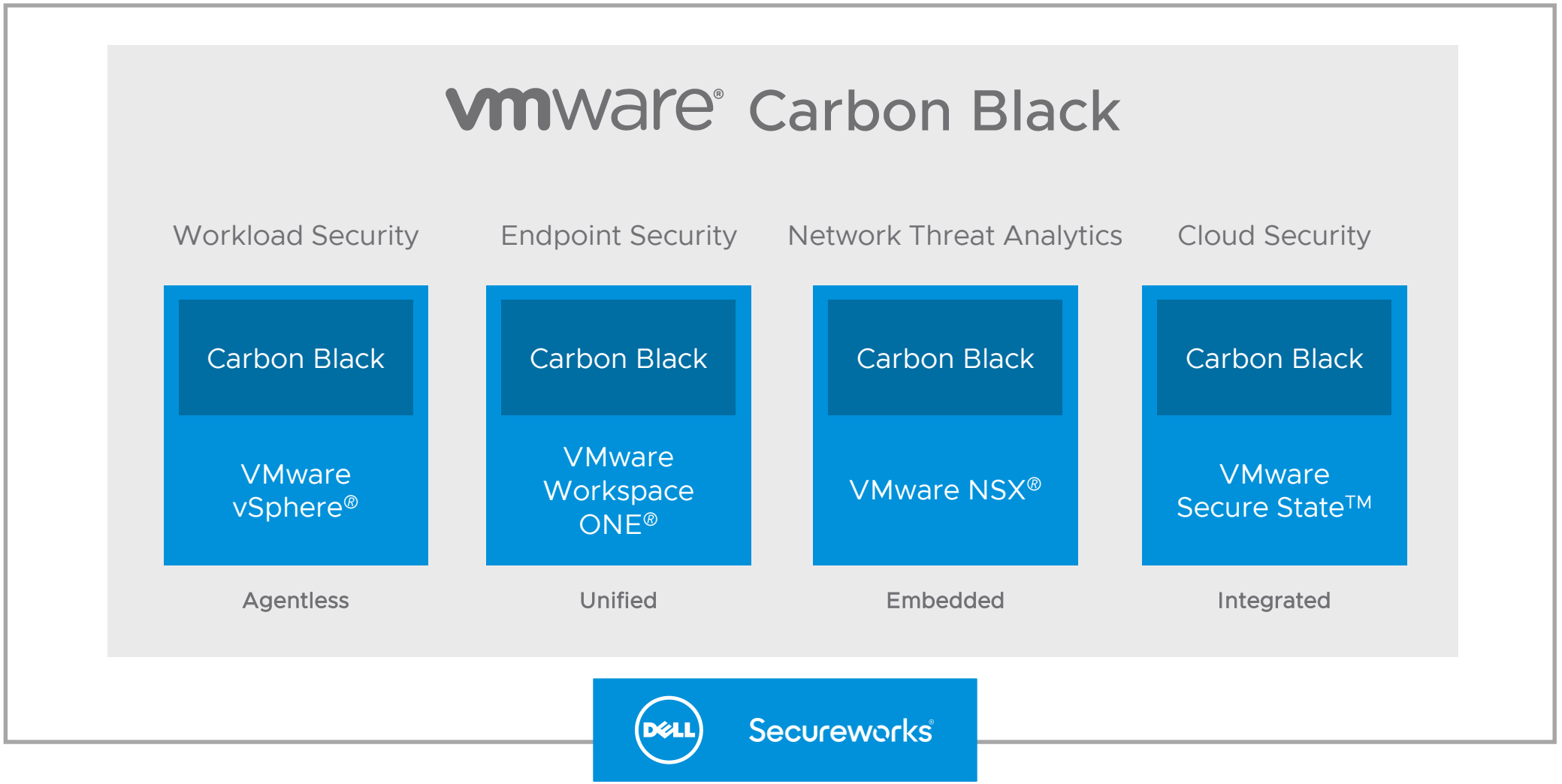


VMware Carbon Black Cloud

統合後に提供していく機能



VMware + Carbon Black + Ecosystem = Better Together



Thank You

vmware Carbon Black