

NS418

AppDefenseとCarbon Black PSCで VMware SDDCを守り抜こう

カーボン・ブラック・ジャパン株式会社
テクニカルディレクター
エバンジェリスト
李 奇 リチャード

#vforumjp

vmware

POSSIBLE
BEGINS
WITH YOU

データセンターのセキュリティ課題



分散化された、変化の多い環境

アプリがより変化の速い、多い、分散化されるようになり、守り難くなっている



数多くのセキュリティツール

セキュリティチームとITチームは多くのツールを運用管理する必要



アプリのライフサイクルが短い

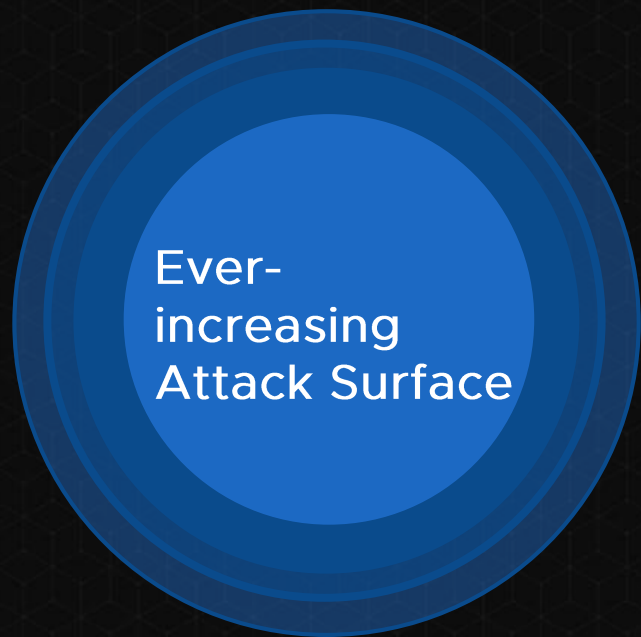
開発時間の短縮によりリリースまで十分にテスト出来ない可能性が高く、セキュリティリスクも増える



対応に時間が掛かる

其々のツールが独立しており、情報が統合されないため、対応に時間が掛かる

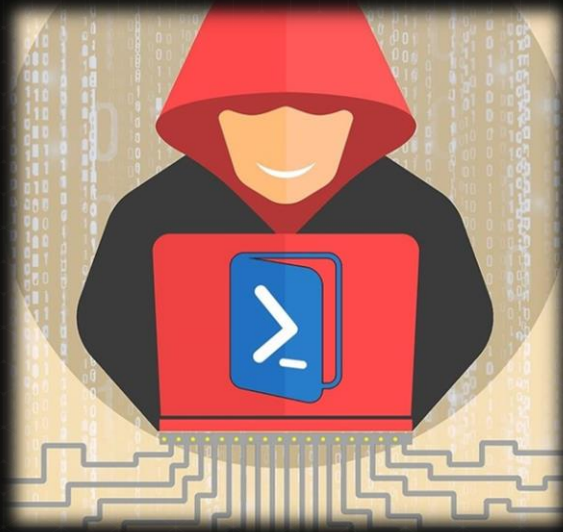
データセンター：サイバー攻撃の最も狙われる対象



データセンターへの脅威は増え続けています

- 攻撃者は検知されず、データセンターに長く潜み続ける
- 攻撃の横展開、組織内、組織外への感染拡大
- PowerShellを悪用する非マルウェア・ファイルレス攻撃はAVでは検知できない
- インシデントレスポンスへの対抗措置
- 仮想通貨のマイニングに悪用される事も

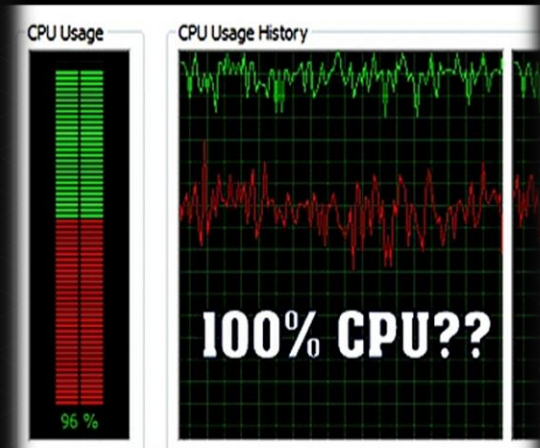
従来のセキュリティの限界



非マルウェア攻撃・
ファイルレス攻撃に
対応出来ない



EDR機能を備えてない；
可視化ができない



システムのリソース
を過度に使う

APPDEFENSE

- 正常な振る舞いの検証にフォーカス
- ポジティブセキュリティモデル：許可するものを定義して、それ以外の振る舞いを検知、ブロック、レスポンス
- サポート環境：vCenter® 6.5+, vSphere® 6.5a
- 「Security Scopes」で許可するアプリを定義
 - 一つの「Scope」には許可するサービス、振る舞い、ルール、そして仮想サーバーが含まれる
 - 「Discovery mode」で振る舞いをモニタリングし、記録出来る
 - その後「verify and protect mode」に移行し、エンフォースメントを実現

vmware

AppDefense

+

Carbon Black.

Cb Defense for VMware



SDDCに特化した セキュリティ

仮想環境を活用して可視化を拡張し、パフォーマンスを犠牲にせずセキュリティを強化する



優れた プロテクション

アプリ中心のセキュリティモデルでアプリコントロールと振る舞い検知・防御、更にEDRの統合を実現

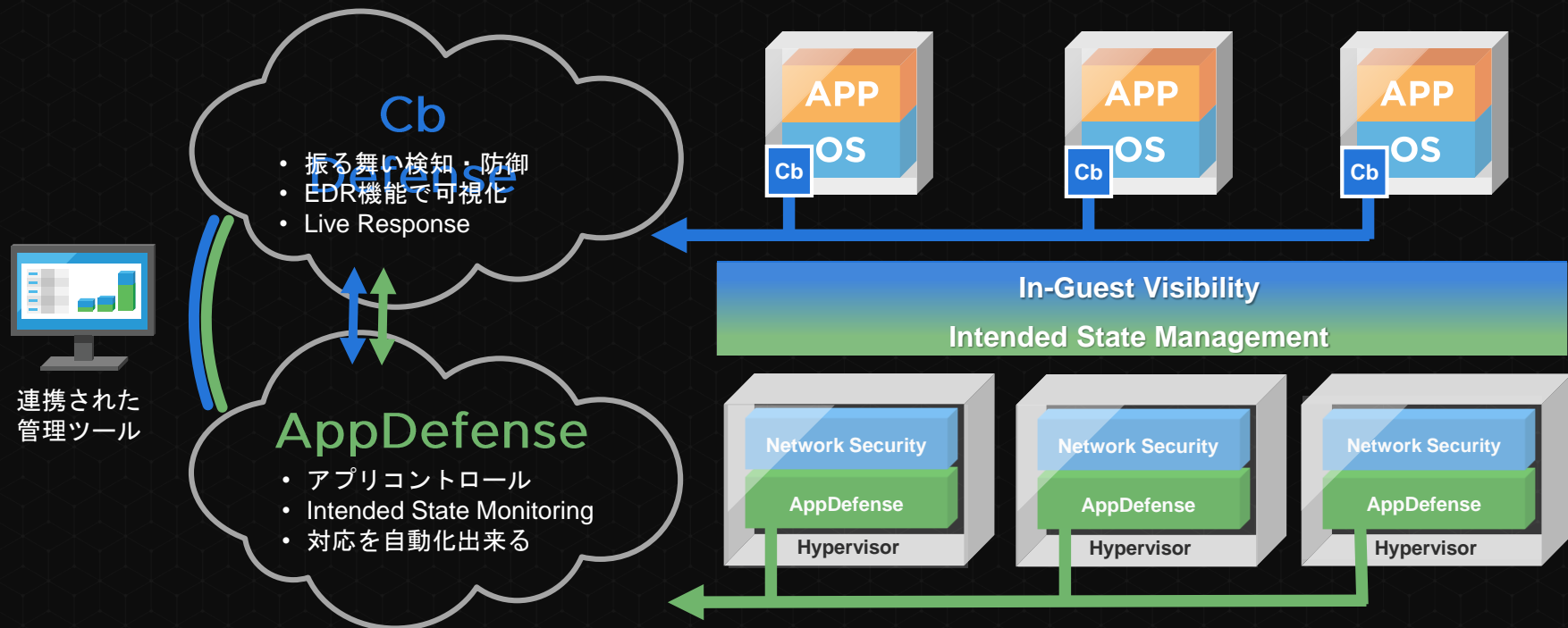


簡素化された 運用管理

ソリューションの連携でITとセキュリティ両チームで可視化領域を共有し、自動的なワークフローを実現

ADVANCED SECURITY FOR ALWAYS-ON ENVIRONMENTS

仮想データセンター環境のためのセキュリティ



ENDPOINT SECURITY PIONEER AND LEADER

4,000+

Customers Globally

33

of Fortune 100

95+

Cb Integration Network
Partners

140+

Product Integrations

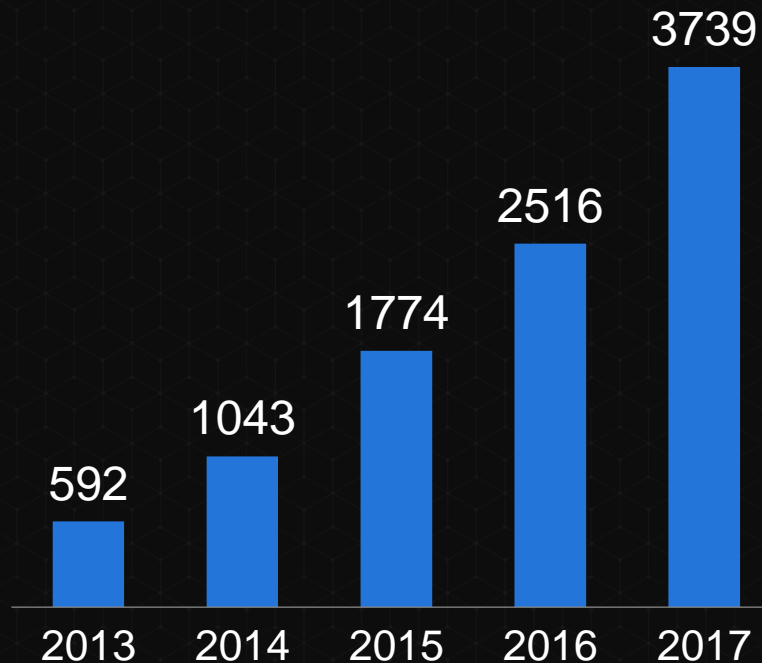
1,100+

Employees

400+

Channel Partners

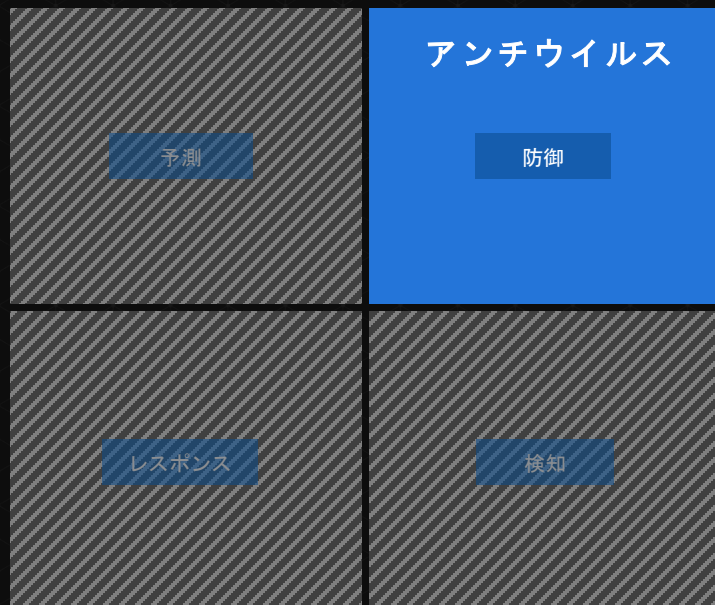
Rapidly Growing Customer Base



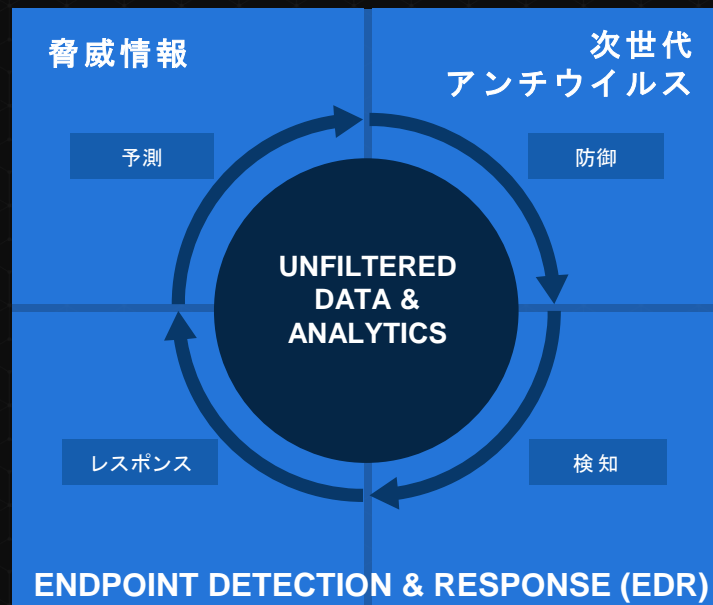
Carbon Black.

データを活用して、セキュリティライフサイクルを実現

従来のアンチウイルス 防御だけに着目

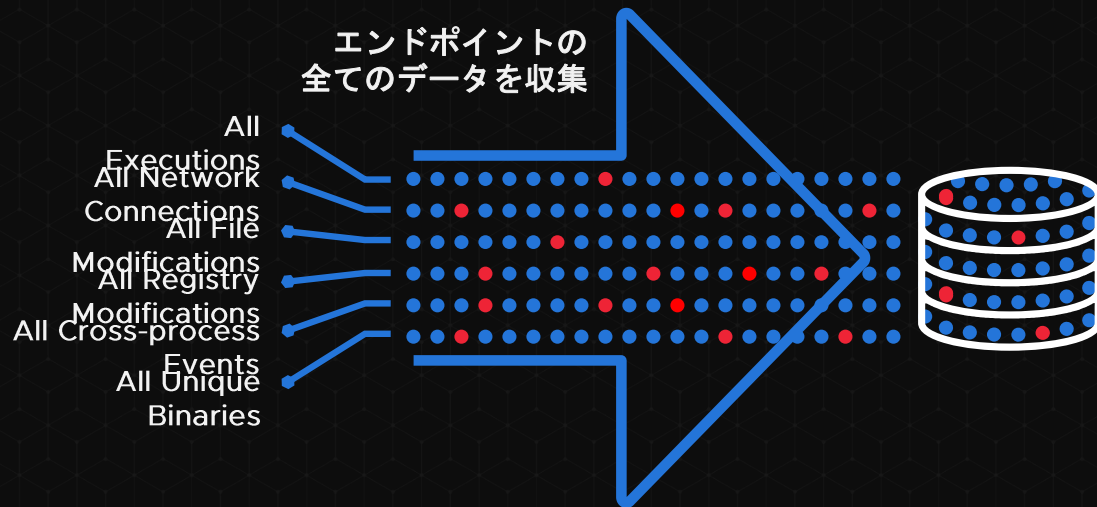


Carbon Black セキュリティライフサイクルに注目



「UNFILTERED」 エンドポイントデータ

攻撃の痕跡を見逃さない



最も役に立つセキュリティデータはエンドポイントのデータ

継続的に:

攻撃を完全に可視化

フィルタなし:

既知 & 未知の攻撃を検知し、防御

集中的に保存:

データをクラウドに保存し、常に解析されて、他社ソリューションとの連携も簡単に出来る

どのくらいのデータを収集されている？



60TB/day Unfiltered data analyzed

8.6M/sec Security events processed
(372B/day)

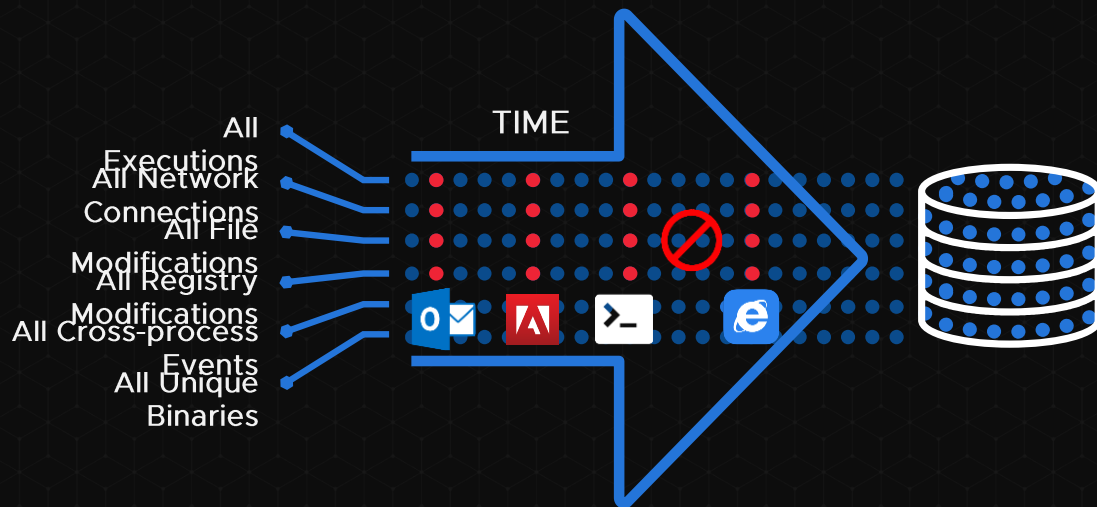
~10X



~10x greater transactional volume than Apple iMessage (40B/day)

2. STREAMING ANALYTICS

ストリーミング：時間軸で前後の動きと関連付けし、
「点と点を繋ぐ」ことで正しい解析結果に導く



一つの時刻だけで判断せず、
前後の動きを繋いで解析

既知の攻撃手法、未知の攻
撃手法、両方とも検知、防
御出来る

クレジットカード詐欺の検
知等で使われた「Event
Stream Processing」の手
法を活用

3. EXTENSIBLE & OPEN ARCHITECTURE



APIs

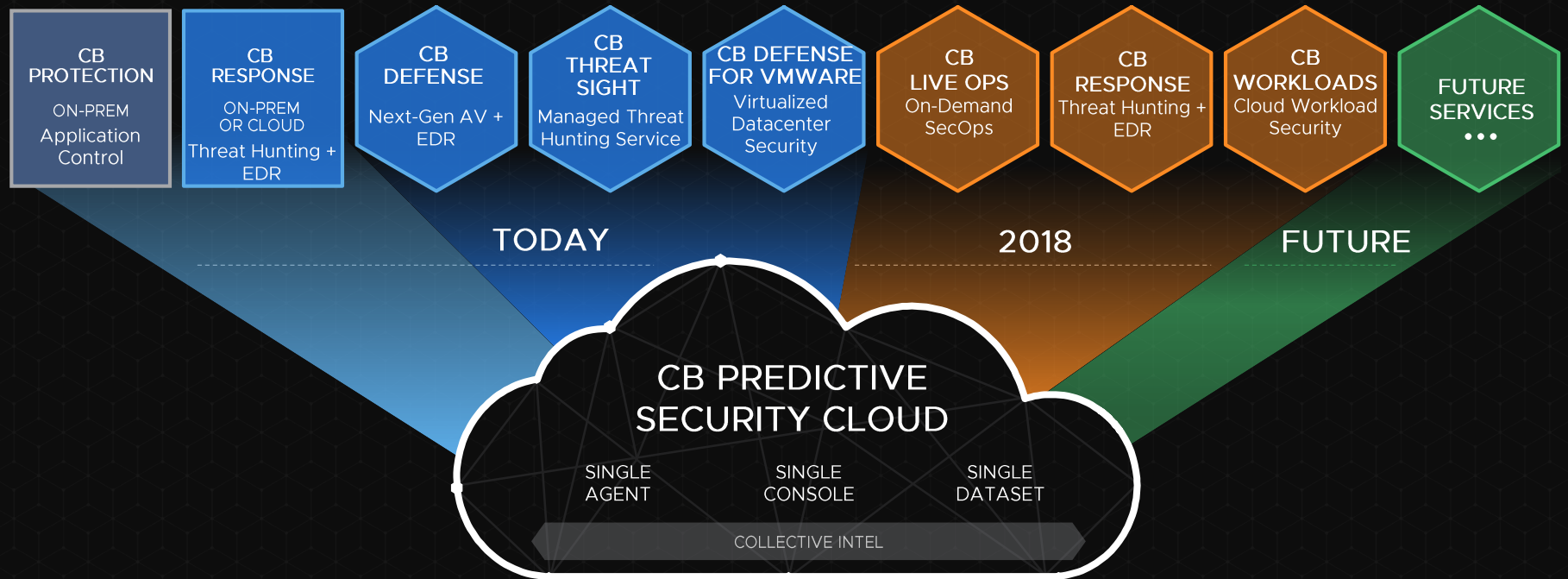
- Raw Data Event Forwarder
- Threat Intel
- Push / Pull for Alerts & Search
- Live Response



OPEN APIs で簡単に
他社ソリューションと
連携可能

120 以上の他社
ソリューションとの連
携が既に実現している

CB PREDICTIVE SECURITY CLOUD





QUICK DEMO

vmware

+

Carbon Black.

AppDefense

ポジティブセキュリティモデル
許可するアプリの振る舞いを
モニタリング
自動的にレスポンス



Cb Defense for VMware

仮想環境を狙う高度な攻撃を
阻止
真のEDR機能を提供
Live Responseで迅速対応



Native Security
Shared Visibility
Common Source of Truth
Shared Context
Common Tools

ADVANCED SECURITY FOR ALWAYS-ON ENVIRONMENTS

Benefits for IT Teams



データセンターに適したセキュリティ

- システムへの影響を最小限にし、パフォーマンスとセキュリティの両立を実現
- 組織の縦割りを減らし、セキュリティチームとの協業を促進
- 自動化やオーケストレーションによってサービスの中断を避ける



優れた可視化

- データセンターで動作するアプリ、プロセスの可視化を実現
- 可視化によって、リソースの最適化にも繋がる
- 可視化によってガバナンスや監査をより効率的に対応可能



簡素化された運用管理

- 運用管理の負荷を軽減できる
- VMwareの連携によってワークフローの自動化ができる
- ITワークフローにスムーズにセキュリティを統合

Benefits for Security Teams



データセンターに適したセキュリティ

- 攻撃を受けるポイントを劇的に縮小させる
- 高度な攻撃からミッションクリティカルな資産を守る
- レスポンス時間を短縮できる



優れた防御スキーム

- 未知の脅威を検知し、複雑な攻撃を阻止できる
- エンドポイントやアプリのコンテキストを把握しているので、より正しい対応が出来る
- データセンターに潜んでいる脅威を積極的につけ出せる



簡素化された運用管理

- セキュリティツールの統合によって複雑な運用を簡素化
- 自動的に対応することでレスポンス時間を短縮
- IT組織の縦割りを減らし、セキュリティチームとITチームとの協業を促進

KEY TAKEAWAYS

- AppDefenseとCb Defenseの連携によって、仮想データセンターの環境に強固なセキュリティを実現できます
- Cb DefenseがエンドポイントからUnfilteredデータを収集し、Streaming Analyticsで解析を行い、未知の脅威・攻撃を検知・阻止できます
- vSphere Platinum EditionにはAppDefenseが標準で付属しています
- 期間限定でCb Defense for VMware（上限100ライセンス）を無償で提供するキャンペーンが実施されています



APPENDIX





VMware AppDefense

Org: Carbon Black Joint Demo...

Alarms

Scopes



Filter scopes



Customer Cloud Platf...



Demo Electronic Healt...

Internal SIEM



Rogue Demo Scope



VMware Horizon 7



<< ⚠ Cb Defense: powershell.exe

PREV

NEXT

Alert Score: 7

Triggered by: Cb Defense

Threat Category: NON_MALWARE

Scope: VMware Horizon 7

Service: Composer

Member: cb-demo-compose

MD5: 097ce5761c89434367598b34fe32893b

Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

CLI: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

Details

Threat Info

Alarm details

Reason: The application powershell.exe read memory from a system security process (lsass.exe). This may have included user credential or password information. A Terminate Policy Action was applied

Generated on: Aug 17, 2018, 2:11:01 AM

Last received: Aug 17, 2018, 2:11:01 AM

CB Defense alert ID: [6L7BBVKN](#)

OS: Windows Server 2016 x64

Remediation status: :-

Parent Process details

Process SHA256: 20a7eb74efd23933a5c0887d3d8ce66fea009a6cd257508cb4b0eb70f8d27c57

CLI: C:\Windows\System32\RuntimeBroker.exe -Embedding



<< ⚠ Cb Defense: powershell.exe

PREV

NEXT

Alert Score: 7

Triggered by: Cb Defense

Threat Category: NON_MALWARE

Scope: VMware Horizon 7

Service: Composer

Member: cb-demo-compose

MD5: 097ce5761c89434367598b34fe32893b

Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

CLI: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

Details

Threat Info

Threat Indicators

5 indicators

Process Name	TTP	Sha256Hash
powershell.exe	READ_SECURITY_DATA	ba4038fd20e474c047be8aad5bfacdb1bfc1ddbe12f803f473b7918d8d819436
powershell.exe	HAS_PACKED_CODE	ba4038fd20e474c047be8aad5bfacdb1bfc1ddbe12f803f473b7918d8d819436
powershell.exe	MODIFY_PROCESS	ba4038fd20e474c047be8aad5bfacdb1bfc1ddbe12f803f473b7918d8d819436
powershell.exe	RAM_SCRAPING	ba4038fd20e474c047be8aad5bfacdb1bfc1ddbe12f803f473b7918d8d819436
powershell.exe	POLICY_TERMINATE	ba4038fd20e474c047be8aad5bfacdb1bfc1ddbe12f803f473b7918d8d819436

Org: Carbon Black Joint Demo...

Alarms

Scopes

Filter scopes

Customer Cloud Platf...

Demo Electronic Healt...

Internal SIEM

Rogue Demo Scope

VMware Horizon 7

Outbound Connections: svchost.exe

Process reputation threat 0 Process reputation trust 10

Triggered by: AppDefense Scope: VMware Horizon 7

Description: Known Process New Behavior Service: Composer

Member: cb-demo-compose

Path: C:\Windows\System32\svchost.exe

MD5: 36f670d89040709013f6a460176767ec

SHA256: 438b6ccd84f4dd32d9684ed7d58fd7d1e5a75fe3f3d12ab6c788e6bb0ffad5e7

CLI: C:\windows\system32\svchost.exe -k netvcs (39 Alarms)

Risk Score: HIGH

Observed Behavior

CLEAR ALARMS ALLOW BEHAVIOUR REMEDIATION ACTIONS

ID	Behavior Severity	Duplicate events	Last Received At	Remediation status	IP Protocol	Rem Port	Host IP	Host Port
36719	N/A	48	Sep 21, 2018, 6:04:40 AM	Action taken: Appdefense - Block And Send Alert	TCP	443		
36714	N/A	44	Sep 21, 2018, 5:35:11 AM	Action taken: Appdefense - Block And Send Alert	TCP	443		
36716	N/A	29	Sep 21, 2018, 5:04:40 AM	Action taken: Appdefense - Block And Send Alert	TCP	443		
36713	N/A	59	Sep 21, 2018, 4:35:12 AM	Action taken: Appdefense - Block And Send Alert	TCP	443	52.165.170.12	
36718	N/A	37	Sep 21, 2018, 4:04:41 AM	Action taken: Appdefense - Block And Send Alert	TCP	443	13.89.220.65	

AppDefense Actions

Suspend

Snapshot


Power Off

Cb Defense Actions

Add to blacklist

Cb Defense Quarantine

ALERT TRIAGE: 6L7B9VKH

**NON-MALWARE**
2:06:05am Aug 17, 2018 7

The application powershell.exe read memory from a system security process (lsass.exe). This may have included user credential or password information. A **Terminate Policy Action** was applied. The alert was undismisssed by jwu+vmware@carbonblack.com.

Investigate

Dismiss Alert

↑

↓

AdministratorWindows Server 2016 x64cb-demo-composeOff-PremisesTarget valueStandardQuarantine DeviceGo Live

Denied OperationTerminatedInvokedInjectedRead MemoryAccessed Target

cb-demo-composeRuntimeBroker.exepowershell.exe

lsass.exeexplorer.exe

SELECTED NODE

vmcb-demo-compose.CBENGLAB.COM

AppDefense Sync: 7:56:10am Oct 14, 2018

Install Status: Both InstalledScope Name: VMware Horizon 7

VMware AppDefense

Service Name: ComposerVMs in Service: 1

VM Details

VM Name: cb-demo-compose

VM ID: vm-87

VM UUID: 50055176-581e-fd0c-63d5-aa851ed2826b

vCenter UUID: 99e2ff57-6bbd-4e13-b7bc-f0f2f447255b

MAC Address: 00:50:56:85:a0:a3

+ AppDefense Module

AppDefense Details

Scope Name: VMware Horizon 7

Scope State: PROTECTED

Service Name: Composer

Service Type: App Server

VMs in Service: 1

View data for

All time

All policies



Configure Dashboard

Export All

Attacks Stopped



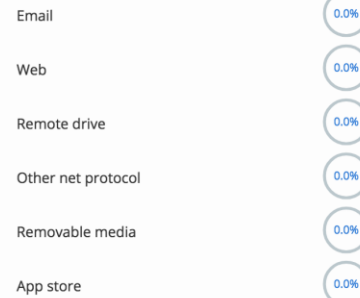
Potentially Suspicious Activity



Attack Stages

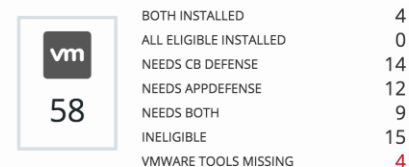


Attacks By Vector



Note: misc. vectors omitted

VMware Cbd Assets *



*Last synchronized with AppDefense: 7:56:10am Oct 14, 2018

Powered by
VMware AppDefense