DELL Technologies

Dell SafeGuard and Response

VMware Data Retention™ for VMware Carbon Black Cloud™

Increased Event Data Storage

Vmware Data Retention

- 60 / 90 / 180 days of event storage on VMware Carbon Black Cloud Platform

Benefits

- More efficient and proactive security operations
- Increased context from event correlation
- Accelerated investigations with continuous endpoint visibility
- Eliminates overhead of having to migrate events to a 3rd party tool
- Reduction in costs of data event storage
- Clearer view of security trends

Use Cases

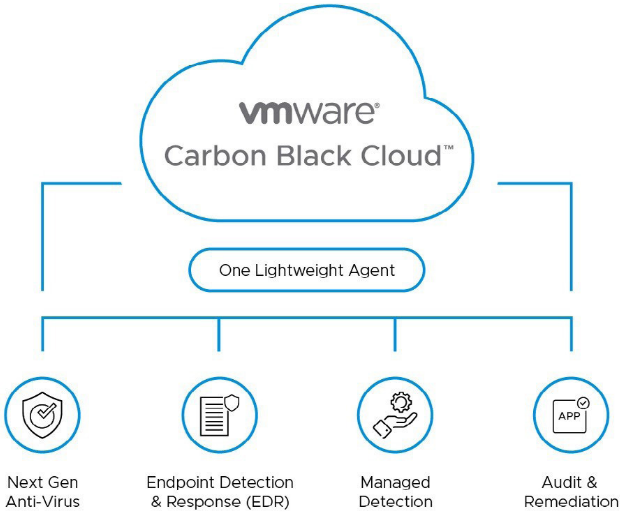
- Respond to incidents with more historical data
- Detect longer term, slower attack techniques

Enterprises face increased complexity across their security stack. On average, it takes 277 days* to identify and respond to a breach, and a key factor is the lack of historical data. To respond effectively to a breach, customers need to be able to rewind the tape for a longer period of time.

With more event data at their fingertips, VMware Data Retention™ for VMware Carbon Black Cloud™ enables organizations to investigate breaches with speed and confidence. VMware Data Retention is delivered as a platform add-on to the VMware Carbon Black Cloud, a next-generation endpoint protection platform that consolidates security in the cloud using a single agent, console and dataset.

Using data continuously collected and sent to the VMware Carbon Black Cloud, both NGAV and Enterprise EDR modules provide immediate access to the most complete picture of an attack at all times, reducing lengthy investigations from days to minutes. Enterprises now have more time to analyze and utilize this data to empower teams to proactively hunt for threats, uncover suspicious behavior, disrupt active attacks, and address gaps in defenses before attackers can.

Cloud-Native Endpoint Protection Program



Learn more at www.Dell.com/endpoint-security

vmware Carbon Black

Key Capabilities

Investigate with Speed and Accuracy

Access to the right data at the right time to close down the MTTR (mean time to resolution.) The ability to have context and visibility for an increased period of time gives security teams the ability to rewind the tape to help them understand the entire attack chain while they investigate the whole attack. This enables security analysts to answer the key questions around what happened, where it happened, and how to resolve it quickly.

Increased Confidence for Threat Hunting

Leveraging the attack chain visualization in the Enterprise EDR Module on the VMware Carbon Black Cloud enables organizations to have confidence in performing historical threat hunts on specific IOCs (Indicators of Compromise) and MITRE-based TTPs (Tactics, Techniques and Procedures) across the entire environment.

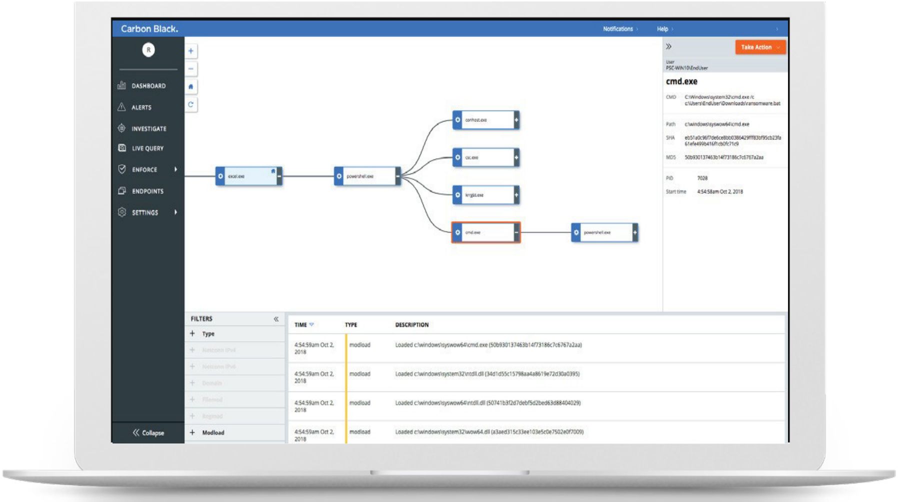
Compliance Regulations

Compliance regulations may require organizations to retain event data for an increased period of time to comply with data retention and audit requirements. Organizations can be ready for audits, including HIPAA, NIST, PCI DSS, and many more, by leveraging VMware Data Retention for VMware Carbon Black Cloud.

Platforms

VMware Data Retention is an add-on service to Carbon Black Cloud and supports:

Windows 7 and above | Windows Server 2008 R2 and above | MacOS 10.10 and above | RedHat 6 and above | CentOS 6 and above | Ubuntu 16.04 and above | SUSE 12 and above | OpenS USE 15 & 42 | Amazon Linux 2



User
PSC-WIN10\EndUser

cmd.exe

CMD C:\Windows\system32\cmd.exe /c c:\Users\EndUser\Downloads\ransomware.bat

Path c:\windows\syswow64\cmd.exe

SHA eb51a0c96f7de6ce8bb0386429fff83bf95cb23fa61efe499b416f1cb0fc71c9

MD5 50b930137463b14f73186c7c6767a2aa

PID 7028

Start time 4:54:58am Oct 2, 2018

TIME	TYPE	DESCRIPTION
4:54:59am Oct 2, 2018	modload	Loaded c:\windows\syswow64\cmd.exe (50b930137463b14f73186c7c6767a2aa)
4:54:59am Oct 2, 2018	modload	Loaded c:\windows\system32\ntdll.dll (34d1d55c15798aa4a8619e72d30a0395)
4:54:59am Oct 2, 2018	modload	Loaded c:\windows\syswow64\ntdll.dll (50741b3f2d7debf5d2bed63d88404029)
4:54:59am Oct 2, 2018	modload	Loaded c:\windows\system32\wow64.dll (a3aed315c33ee103e5c0e7502e0f7009)

FIGURE 1: Enterprise EDR leverages continuously collected endpoint activity data to provide extensive attack chain visualization and a clear understanding of what happened at every stage of the attack.

Contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com,

about Dell solutions to help improve your security posture

** IBM Security: Cost of a data breach 2022 report*

Learn more at www.Dell.com/endpoint-security