Schutz von Workloads in der Cloud

So schützen Sie Workloads in Hybrid Clouds

vmware®

Inhaltsverzeichnis

Kurzfassung

Die Hybrid Cloud steht im Mittelpunkt der digitalen Transformation. Heute geben über 90% der Unternehmen an, eine Multi-Cloud-Strategie zu verfolgen – wobei die meisten davon Public und Private Clouds kombinieren.[1] Das Gute daran: Dieser Ansatz bietet die nötige Flexibilität und Skalierbarkeit für schnelle Innovation. Andererseits ist dies häufig mit zusätzlichen Komplexitäten und Risiken verbunden, sodass Sicherheit zu einem wesentlichen Aspekt in Private und Public Clouds wird.

Wenn Unternehmensteams kritische Workloads in Multi-Cloud-Umgebungen bereitstellen und verwalten, sind Transparenz in Bezug auf den Sicherheitsstatus von Workloads sowie Kontrolle der Angriffsfläche unabdingbar, um Daten zu schützen und den Betrieb aufrechtzuerhalten.

Viele verschiedene Teams im Unternehmen, einschließlich IT-Ops und SecOps, sind wichtige Stakeholder im Hinblick auf die Performance, Verfügbarkeit und Sicherheit von Cloud-Workloads. Ein wesentlicher Erfolgsfaktor ist auch, dass die Teammitglieder aufeinander abgestimmt und nicht fragmentiert sind.

Dieses White Paper befasst sich mit den wichtigsten Herausforderungen, auf die Unternehmensteams beim Schutz von Cloud-Workloads gestoßen sind, und mit der Frage, wie diese mithilfe des Intrinsic Security-Ansatzes von VMware auf Basis von VMware Carbon Black Cloud™, VMware vSphere® und VMware NSX® überwunden werden können. Zudem befasst sich dieses White Paper damit, warum die Cloud eine neue Denkweise in Bezug auf Risiken anstößt – eine, die teamübergreifende Stakeholder zusammenbringen und so zur Überwindung der digitalen Kluft beitragen kann. Eine Checkliste für die Evaluierung von Plattformen zum Schutz von Cloud-Workloads hilft Unternehmen, bei der Lösungssuche wichtige Anforderungen zu prüfen.

Sicherheitsherausforderungen bei Private, Public und Hybrid Clouds

Das Bereitstellen und Verwalten von Workloads und Anwendungen in Private, Public und Hybrid Clouds ist eine gemeinsame Anstrengung. Herkömmliche IT ist heute zu einem Kollektiv geworden. IT-Ops, DevOps und SecOps arbeiten zusammen, um Anwendungen und Services über die Cloud bereitzustellen und zu schützen.

1. Flexera, „Flexera 2020 State of the Cloud Report“, April 2020.

Wie in Tabelle 1 veranschaulicht, kann eine fehlende teamübergreifende Koordination und Planung unter Einbeziehung der einzigartigen Aspekte von Cloud-Workloads zu erhöhten Risiken führen.

	HYBRID CLOUD-BETRIEB	SICHERHEITS-HERAUSFORDERUNGEN	HERKÖMMLICHER IT-BETRIEB	LÜCKEN IN DER HERKÖMMLICHEN IT-SICHERHEIT
Designarchitektur	Vernetzte Services	• Keine Transparenz in Bezug auf die Kommunikation und Verbindung von Workloads • Flache, unsegmentierte Netzwerke erhöhen das Risiko.	Monolithisch und isoliert	• Herkömmlicher Virenschutz (AV) ist nicht für eine Cloud-Workload-Umgebung konzipiert. • Bei einer auf das Rechenzentrum konzentrierten Überwachung fehlt das grundlegende Verständnis für normales Netzwerkverhalten.
Betriebsmodell	Dezentrales Eigentum und Management	• IT-Ops ist für Status, Management und Verfügbarkeit von Workloads verantwortlich, jedoch nicht in der Lage, Schwachstellen zu erkennen. • Technologie- und Prozess-Silos tragen zu Fehlkonfigurationen, nicht ausreichend geschützten Konfigurationen und sonstigen menschlichen Fehlern bei.	Zentralisiert	• Kommen Kernsicherheitsprodukte hinzu, müssen zusätzliche Agents installiert werden, was die System-Performance verschlechtert und Abläufe verkompliziert. • Durch fehlende einheitliche Transparenz in Bezug auf Workloads sowie bei verschiedenen Workloads und Clouds wird die teamübergreifende Koordination komplexer.
Skalierbarkeit	Hochdynamisch, automatisch	• Das Fehlen einer Änderungskontrolle führt zu Fehlkonfigurationen, wie z.B. ungesichertem Daten-Storage, einer zu hohen Anzahl an Berechtigungen, Standard-Anmeldeinformationen und Konfigurationseinstellungen, sowie zur Deaktivierung von Sicherheitskontrollen. • Die Unfähigkeit, Sicherheitsrichtlinien für Workloads in Private und Public Clouds zu standardisieren, erhöht das Risiko.	Statisch, manuell	• Herkömmliche Suchen sind nicht dafür konzipiert, häufige Cloud-Fehlkonfigurationen (die Hauptursache Cloud-basierter Datenschutzverstöße) zu erfassen.[2] • Müssen für jede einzelne Cloud-Umgebung Einzelsicherheitslösungen bereitgestellt werden, wird das skalierbare Management von Governance und Richtlinien erschwert.

TABELLE 1: Sicherheitsherausforderungen entstehen bei Hybrid Cloud-Workloads dann, wenn die wesentlichen Unterschiede zwischen Cloud Computing und herkömmlicher IT nicht erkannt werden.

2. Cloud Security Alliance, „Top Threats to Cloud Computing: Egregious Eleven Deep Dive“, September 2020.

IT-Ops, DevOps und SecOps sind gemeinsam dafür verantwortlich, die Sicherheit und Verfügbarkeit kritischer Workloads in der Cloud zu gewährleisten.

Drei Schritte zur Neudefinition des Risikos

Sie machen das Beste aus der digitalen Transformation, wenn Sie akzeptieren, dass es sich um einen erheblichen Paradigmenwechsel handelt. Ältere Risikomanagement-Modelle sind bei laufenden Veränderungen und einer großen Zahl an Mitwirkenden nicht mehr angemessen.

Zum Schutz von Cloud-Workloads müssen Unternehmensteams auf Folgendes achten:

1. Transparenz erhöhen: Unbekannte oder nicht erkannte Risiken in Workloads müssen identifiziert werden.
2. Recovery verkürzen: Die Risiko-Recovery muss durch entsprechende Resilienz in Cloud-Workloads beschleunigt werden.
3. Sicherheit vereinfachen: Die Risikominimierung muss für alle Workloads, Endpunkte und Container vereinheitlicht werden.

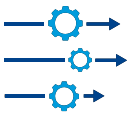
Schritt 1: Transparenz erhöhen: Unbekannte oder nicht erkannte Risiken in Workloads müssen identifiziert werden

- **Warum ist dies schwierig?** Sie können nicht mit Risiken umgehen, die Sie nicht kennen. Leider ist den meisten Administratoren von virtuellen Maschinen (VMs) nicht bewusst, dass die auf ihren VMs laufenden Anwendungen und Workloads potenziell für Angriffe anfällig sind. Während Angreifer nur eine einzige Schwachstelle identifizieren und ausnutzen müssen, um unbefugten Zugriff zu erhalten, müssen die für den Schutz des Systems Verantwortlichen alle Schwachstellen kennen und beheben. Nach der Identifizierung von Schwachstellen ist es zudem nicht immer einfach, einen Konsens zwischen IT-Ops und SecOps darüber zu erzielen, welche Schwachstellen mit höchster Priorität zu beheben sind, wann und aus welchen Gründen.
- **Ein Beispiel:** Joe ist Site Reliability Engineer (SRE) für ein großes Dienstleistungsunternehmen im Gesundheitswesen. Er ist für das Management der Private Cloud-Infrastruktur zuständig, zu der Server, Workloads und Anwendungen gehören, die sensible Gesundheitsdaten verarbeiten. Joe weiß, dass er alle Schwachstellen, die die Compliance beeinträchtigen oder Patientendaten preisgeben könnten, identifizieren und beseitigen muss. Dennoch haben Service-Performance, Verfügbarkeit und Betriebszeit für Joe und die anderen SREs in seinem Team höchste Priorität. Schließlich ist die Versorgung der Patienten unternehmenskritisch.

  Derzeit erwartet Joe von Sarah, einer Sicherheitsanalystin, dass sie ihn darauf hinweist, wenn bei einem geplanten Scan eine große Schwachstelle erkannt wird, die behoben werden muss. Da die beiden unterschiedliche Tools verwenden, sind sie sich in Bezug auf die zu treffenden Maßnahmen häufig nicht einig. Ohne gemeinsames Aufzeichnungssystem kann ein Konsens in Bezug auf diese kritischen Probleme nur schwer erreicht werden: Welche Schwachstellen haben die höchste Priorität? Reichen die zusätzlichen Maßnahmen aus? Wer sind die Angreifer? Und so weiter.
- **Anforderung: Domänenübergreifende Risikoerkennung:** Ermitteln Sie sämtliche Cloud-Workload-Risiken – aus allen Perspektiven sowie im Zusammenhang mit allen Angriffsvektoren – und verwenden Sie ein einheitliches Aufzeichnungssystem für deren Management. Kann ein Patch aufgrund des Ausfallrisikos nicht implementiert werden, stimmen Sie sich über eine zusätzliche Sicherheitsmaßnahme ab oder richten Sie eine Watchlist für die entsprechende Schwachstelle ein.

Schritt 2: Recovery verkürzen: Die Risiko-Recovery muss durch entsprechende Resilienz in Cloud-Workloads beschleunigt werden

- **Warum ist dies schwierig?** Für die meisten Unternehmen lautet die Frage nicht, ob es zu einem Datenschutzverstoß kommt, sondern wann. Bei einem Angriff sind Informationen über das Ausmaß der Gefährdung bzw. den eigentlichen Schaden von kritischer Bedeutung, um ähnliche Sicherheitsverletzungen in Zukunft zu verhindern. Außerdem sind solche Informationen für eine schnelle und vollständige Recovery maßgeblich. Schwierig gestaltet sich die Abwägung von Prioritäten. Für DevOps- und IT-Ops-Teams hat die möglichst schnelle Wiederherstellung der Services oberste Priorität, auch wenn dabei forensische Beweise und Artefakte vernichtet werden, die das SecOps-Team eigentlich benötigt, um die Ursache und den vollen Umfang des Angriffs zu ermitteln.
- **Ein Beispiel:** Die Recovery von einem Ransomware-Angriff innerhalb Ihrer Cloud-Umgebung ist womöglich kostspielig, kompliziert und aufwändig. Solche Angriffe können von Workloads auf die Server übergehen, auf denen sie gehostet werden, und dann auf die von den Mitarbeitern für den Zugriff auf diese Workloads



verwendeten Endpunkte. Ziel ist es, der Ransomware die Angriffsfläche zu nehmen, indem der Angriff gleich im Frühstadium – bei der Ausführung des Codes im Workload – unterbunden wird, ehe das Toolset vollständig bereitgestellt oder die Befehls- und Kontrollverbindungen (C2) aufgebaut sind und die Daten für die Erpressung herausgeschleust oder verschlüsselt werden können.

- **Anforderung: Risikoresilienz:** Beides – schnelle Wiederherstellung von Services nach einer Sicherheitsverletzung oder einem Malware-Angriff sowie Speicherung der für forensische Untersuchungen erforderlichen Daten – kann in der Cloud erfolgen, sofern Sie über die richtige Workload-Sicherheitsplattform verfügen. Die Überwindung dieser Kluft ist sogar ein wesentlicher Aspekt des Aufbaus von Risikoresilienz in Ihren Cloud-Workloads. Wenn Sie Workload- und Endpunktsicherheit auf ein und derselben Plattform verwalten, können Ihre Teams Risiken an allen Kontrollpunkten identifizieren und eine resilientere Recovery-Strategie entwickeln.

Schritt 3: Sicherheit vereinfachen: Die Risikominimierung muss für alle Workloads, Endpunkte und Container vereinheitlicht werden

- **Warum ist das schwierig?** Risikomanagement in Cloud-Workloads mit herkömmlichen Punktlösungen führt zu „Stovepipe"-Prozessen, die Gesamtkosten und Risiken erhöhen. Durch Verwendung unterschiedlicher Sicherheitstools je nach Public Cloud-Anbieter, Host-Betriebssystem oder Art der Cloud (Private oder Public) wird eine konsistente Strategie zur Risikominimierung in der Praxis unerreichbar. Wenn es in Bezug auf die Sicherheit keine Single Source of Truth gibt, können sich Teams nicht darauf einigen, wie sie Malware-Ausbrüche verhindern, Fehlkonfigurationen finden und beheben oder schnell voranschreitende Bedrohungen eindämmen.
- **Ein Beispiel:** Um die Betriebsresilienz zu erhöhen, entscheiden sich manche IT-Ops-Teams für mehrere Cloud-Anbieter oder kombinieren Private und Public Cloud-Infrastrukturen. Ohne eine wirklich agnostische Sicherheitsrichtlinie, die über diese Umgebungen hinausgeht, müssen Teams entweder einen Flickenteppich an Kontrollen nutzen oder bei einem einzigen Cloud-Serviceanbieter oder einer Cloud-Architektur (Private oder Public) bleiben.
- **Anforderung: Einheitliche Sicherheit:** Ziel ist es, einheitliche Sicherheitsmaßnahmen zu implementieren, die für die Cloud konzipiert sind und einheitlich angewendet werden, unabhängig davon, wo sich Workloads befinden (Public oder Private Cloud). Durch zentrales Lebenszyklusmanagement über Clouds, Workloads und Container hinweg kann eine konsistente und umfassende Strategie für Sicherheitsrichtlinien und Risikominimierung umgesetzt werden. So vereinfacht die Verwendung einer einzigen Plattform für Schwachstellenmanagement, Audit und Remediation sowie Endpunkterkennung und -reaktion (EDR) die Workload-Sicherheit und unterstützt die Zusammenarbeit zwischen IT-Ops, SecOps und DevOps.

Intrinsic Security für Cloud-Workloads

Wie in diesem White Paper erörtert, erhöht die Verwendung unterschiedlicher Technologien zum Verwalten von Cloud-Workloads das Risiko. Dies ist schlicht und einfach keine skalierbare Lösung. Zugleich muss jedes Team, von IT-Ops bis DevOps und SecOps, unbedingt die Konsole seiner Wahl nutzen können. Das soll nicht heißen, dass die Migration in die Cloud die Einführung eines völlig neuen Prozesses, einer neuen Benutzeroberfläche oder einer Managementkonsole erfordert. Schließlich sind diese Teams bereits mehr als ausgelastet.

Mit dem Intrinsic Security-Ansatz von VMware werden umfassende Überwachungsfunktionen und Verhaltensanalysen an jedem Kontrollpunkt – Cloud, Workload, Endpunkt, Netzwerk und Identität – implementiert und dann für ein vollständiges kontextbezogenes Bewusstsein vereinheitlicht. Wie eine Videokamera, die jede Bewegung an jedem Kontrollpunkt aufzeichnet, ermöglicht Intrinsic Security ein umfassendes kontextbezogenes Bewusstsein. Da die Telemetriedaten von verschiedenen Kontrollpunkten nicht mehr manuell zusammengefügt werden müssen, können Teams Bedrohungen schnell ab dem Eintrittspunkt und jedem Schritt dazwischen aufspüren.

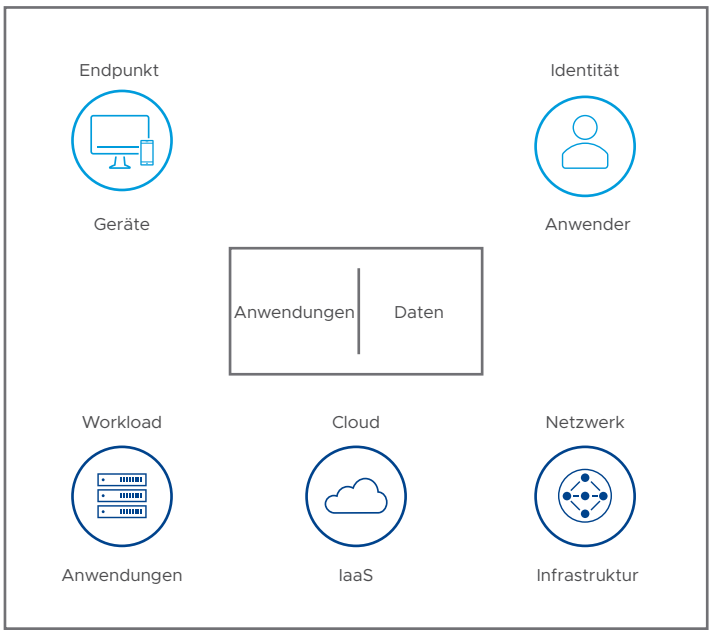


ABBILDUNG 1: Die fünf Kontrollpunkte von Intrinsic Security

Skalierbarer Schutz von Workloads in der Cloud

VMware Carbon Black Cloud bietet alle Funktionen für einen skalierbaren Cloud-Workload-Schutz sowie native Integration in vSphere und NSX. Dank dieser nahtlosen Integration können vSphere- und NSX-Administratoren auf alle relevanten Bedrohungsdaten im Kontext ihrer jeweiligen Domänen und innerhalb derselben, für ihre jeweiligen Rollen optimierten Konsole zugreifen.

VMware Carbon Black Cloud bietet nicht nur ein vollständiges kontextbezogenes Bewusstsein innerhalb von sowie über Clouds, Workloads, Endpunkte, Netzwerke und Identitäten hinweg, sondern auch ein gemeinsames System für IT-Ops, DevOps und SecOps, um Bedrohungen, die sich auf kritische Anwendungen und Workloads auswirken, zu verhindern, zu erkennen und zu beseitigen.

Die grundlegenden Komponenten von Intrinsic Security:

- VMware Carbon Black Cloud
- VMware vSphere
- VMware NSX

VMware Carbon Black Cloud

VMware Carbon Black Cloud ist eine cloudnative Plattform zum Schutz von Cloud-Workloads, die intelligente Systemhärtung und Verhaltensprävention kombiniert, um aufkommende Bedrohungen mithilfe eines einheitlichen Lebenszyklusmanagements und einer einfach zu bedienenden Konsole in Schach zu halten.

VMware vSphere

vSphere ist die branchenführende Plattform für Computing-Virtualisierung und wurde mit nativem *Kubernetes* neu gestaltet, damit Kunden Workloads, die auf vSphere ausgeführt werden, modernisieren können.

VMware NSX Advanced Threat Prevention™

Die auf maschinellem Lernen basierende VMware NSX Service-defined Firewall™ bietet Analysen des Netzwerkdatenverkehrs, Erkennung und Abwehr von Eindringversuchen sowie erweiterte Malware-Analysen mit umfassenden Netzwerkerkennungs- und Reaktionsfunktionen.

Cloud-Workload-Schutz von VMware: Funktionsweise

Mit dem Intrinsic Security-Ansatz von VMware können Unternehmen Cloud-Workloads schützen, indem sie die bestehende Infrastruktur dazu nutzen, Risiken proaktiv zu identifizieren, das Ausnutzen von Sicherheitslücken und Gefährdungen zu verhindern sowie neue Bedrohungen schnell zu erkennen und zu beseitigen.

Das dreistufige Verfahren basiert auf wesentlichen Sicherheitskontrollen und läuft wie folgt ab.

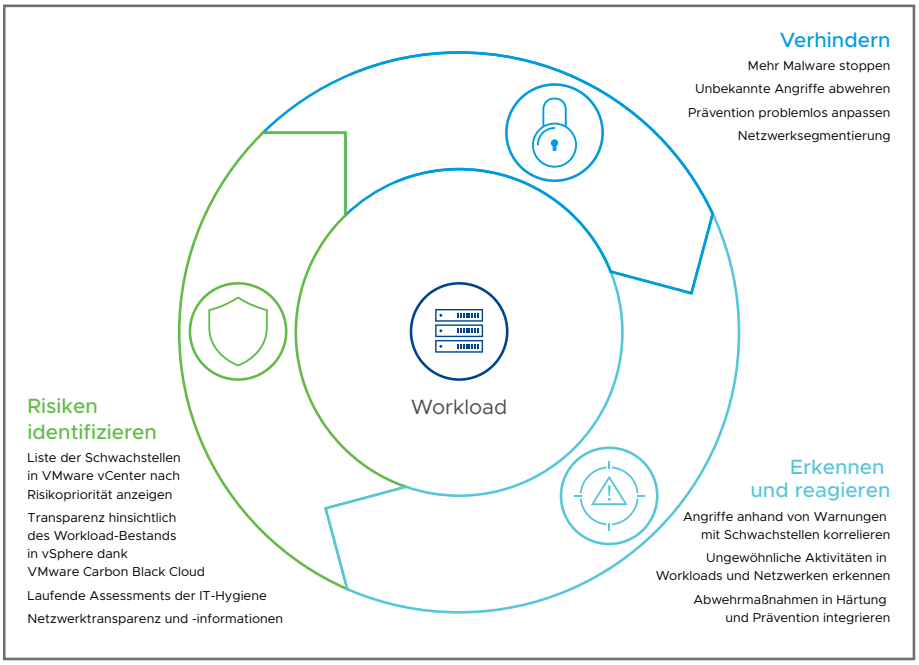


ABBILDUNG 2: Intrinsic Security für Cloud-Workloads bietet umfassenden Schutz für vSphere-Workloads.

Schritt 1: Risiken identifizieren

- **Anfängliche Zustandsintegritätsprüfung:** VMware Carbon Black Cloud führt eine anfängliche Zustandsintegritätsprüfung durch. Dabei wird ermittelt, ob das System, auf dem Sie den Workload installieren, fehlerfrei, konform und für die Art des Workload geeignet ist. Außerdem werden die Patch-Level des Betriebssystems erfasst und analysiert sowie Schwachstellen und Fehlkonfigurationen beurteilt. Darüber hinaus wird ermittelt, ob eine zusätzliche Systemhärtung erforderlich ist.
- **Durchgängige Transparenz in Bezug auf den Systemzustand:** VMware Carbon Black Cloud identifiziert Konfigurationsabweichungen und stellt fest, ob unbekannte oder nicht autorisierte Anwendungen, Schwachstellen oder andere dynamische Aktivitäten vorhanden sind, die die Angriffsfläche der Umgebung vergrößern. Unter anderem bietet es Folgendes:
  - Überwachen auf Änderungen, die auf schändliche Aktivitäten hindeuten (z.B. das Löschen von Kennwörtern, Änderungen der BitLocker-Konfiguration)
  - Audit und Remediation zur Abfrage von 1.500 Artefakten für jeden Workload und Endpunkt in Private und Public Clouds
  - Administratoren können benutzerdefinierte SQL-Abfragen ausführen, um nach bestimmten bösartigen Verhaltensweisen oder Aktivitäten Ausschau zu halten.
- **Durchgängige Transparenz in Bezug auf Schwachstellen und Netzwerkaktivität:** VMware Carbon Black Cloud bietet vSphere-Administratoren die Möglichkeit, nach Risiko eingestufte Workload-Schwachstellen in VMware vCenter® anzuzeigen und ohne Scan regelmäßig Schwachstellen in verschiedenen Workloads zu beurteilen. NSX bietet eine integrierte verteilte Firewall. So können IT-Ops-Teams die Kommunikation von Workloads über Private und Public Clouds hinweg überwachen, ermitteln, welche Workloads Teil einer Anwendung sind, sowie festlegen, wie nicht zusammenhängende Workloads segmentiert werden sollen.

Schritt 2: Eskalation von Risiken verhindern

- **Verhindern der Nutzung von Schwachstellen im Workload:** VMware Carbon Black Cloud bietet Virenschutz der nächsten Generation (NGAV) für einen Schutz, der über punktuelle Indikatoren für Malware, Ransomware, Zero-Day, schnelle Varianten, verdächtige Dateien und potenziell unerwünschte Prozesse (PUPs) hinausgeht, die für Workloads in Private und Public Clouds spezifisch sind. Die VMware-Plattform kombiniert Ablenkungsmanöver für Ransomware, dynamische Analysen und maschinelles Lernen für laufende Analysen, die verdächtige Dateien daran hindern, ausgeführt zu werden.
- **Verhindern von Nicht-Malware-Angriffen:** VMware Carbon Black Cloud blockiert nicht nur Malware-Angriffe, sondern schützt auch vor den neuesten persistenten Angriffen mit dateiloser Malware, speicherbasierten und Living-off-the-land(LotL)-Taktiken. Diese gefährlichen Angriffe nutzen vorhandene Software und Anwendungen auf Positivlisten (z.B. PowerShell) sowie autorisierte Protokolle, um bösartige Aktivitäten auszuführen. Im Gegensatz zu Legacy-Ansätzen auf der Grundlage von bekannten Bedrohungen kann die VMware-Plattform neue Varianten und Zero-Day-Schwachstellennutzungen durch Zusammenführen vernetzter Verhaltensweisen erkennen.
- **Vermeiden netzwerkbasierter Angriffe:** Die NSX Service-defined Firewall schützt Workloads durch Eingrenzen lateraler Ausbreitung und Blockieren der Nutzung von Schwachstellen bei empfindlichen Anwendungen und Services. Mit diesem Grad an Transparenz können Sie nachvollziehen, wie sich LotL-Angriffe durch das Netzwerk bewegen, Indicators of Compromise (IOCs) identifizieren und diese Netzwerkverbindungen sperren, um Workloads von Angreifern zu isolieren.
- **Maßgeschneiderte Prävention:** Jede Umgebung hat unterschiedliche und oft in Widerspruch stehende Betriebseinschränkungen. VMware bietet Kunden die Möglichkeit, Sicherheits- und Betriebsrisiken mit präziser Granularität auszugleichen. Mit der Richtlinien-Engine von VMware können Sie anhand der spezifischen Art eines Workload, dessen Funktion, Bedeutung und Nähe zu anderen kritischen Workloads bestimmen, wie Bedrohungen abgewehrt werden sollen. Um beispielsweise einen unternehmenskritischen Workload zu isolieren, kann ein Systemadministrator PowerShell daran hindern, den Arbeitsspeicher eines anderen Prozesses zu durchsuchen oder eine nicht vertrauenswürdige Anwendung zu starten.

Schritt 3: Laufende Risiken erkennen und minimieren

- **Der richtige Moment und Ausgangspunkt für eine Ermittlung:** Erkennen Sie betroffene Systeme mithilfe der einsatzbereiten automatisierten Bedrohungserkennung von VMware mit aktualisierter Threat Intelligence aus der VMware Threat Analysis Unit™ und isolieren Sie sie für die Remediation. Mit APIs von VMware können Sie eigene Feeds und Watchlists von Drittanbietern integrieren und die gemeinsame Nutzung von Bedrohungsdaten aus dem soliden VMware-Anwenderaustausch abrunden.
- **Voller Umfang und Zeitrahmen des Angriffs:** Mit der Plattform von VMware können Ermittler das Band sozusagen zurückspulen und nachvollziehen, wie ein bestimmter Angriff zustande gekommen ist, welche Systeme betroffen sind und wie sich der Angriff im Laufe der Zeit entwickelt hat. Da VMware die Gesamtheit der Daten erfasst (z.B. ausführliche Prozessaktivitäten, Interaktion zwischen Prozessen, Beziehungen zwischen über- und untergeordneten Prozessen usw.), können für Vorfälle zuständige und forensische Teams auch im Nachhinein eine ausführliche Zeitachse ohne tote Winkel erstellen und dem Angriff so auf den Grund gehen.
- **Schneller Detect-to-Prevent-Workflow:** In drei einfachen Schritten können Sie mit VMware Carbon Black Cloud Bedrohungserkennung in standardisierte Präventionsrichtlinien für Ihre Workloads umsetzen. Wenden Sie zunächst automatisierte Richtlinien an, die auf früheren auf Ihre Workloads zugeschnittenen Erkennungen basieren. Erstellen Sie als nächstes eine Vorschau der weiteren Auswirkungen der Präventionsrichtlinie, ehe sie umgesetzt wird. Wenden Sie dann mit einem einzigen Mausklick die aktualisierte Richtlinie auf Workloads in einer beliebigen Umgebung an.

Der Schutz von Cloud-Workloads vor einer Vielzahl von Bedrohungen erfordert einen mehrgleisigen Ansatz mit granulärer und gleichzeitig einheitlicher Transparenz in Bezug auf alle Aspekte der Computing-Umgebung. IT-Ops, DevOps und SecOps tragen die gemeinsame Verantwortung für den Schutz kritischer Workloads in der Cloud. Unternehmen, die Hybrid Clouds mit herkömmlichen Ansätzen zu schützen versuchen, sehen sich einer Vielzahl von Herausforderungen gegenüber, wie mangelnder Transparenz darüber, wie Workloads miteinander verbunden sind, fragmentierten Prozessen und Fehlkonfigurationen. Wie in diesem White Paper erörtert, sind größere Transparenz, beschleunigte Recovery und vereinfachte Sicherheit drei wichtige Strategien, die Unternehmensteams umsetzen müssen, um Risiken zu minimieren.

VMware ist hervorragend für den Schutz von Workloads in Hybrid Clouds positioniert. Insbesondere können Teams mit VMware-Lösungen aufkommende Risiken für Workloads genau identifizieren, eine weitere Eskalation dieser Risiken verhindern und Ausbrüche schnell und ohne Betriebsunterbrechungen eindämmen. Während andere Endpunkt- und Workload-Sicherheitsprodukte nur einen Datensatz erfassen, der sich auf bekannte böswillige Akteure bezieht, sammelt VMware Carbon Black Cloud kontinuierlich umfassende Workload-, Endpunkt- und Netzwerkdaten und analysiert die Verhaltensmuster von Angreifern, um Angriffe proaktiv zu stoppen, bevor sie Schaden anrichten können. Dieser Grad an erhöhter Betriebstransparenz vereinfacht die Sicherheit und beschleunigt die Systemwiederherstellung.

Zwar offerieren etliche Anbieter auf dem Markt Schutz für Cloud-Workloads, aber nicht alle Lösungen sind gleich. Unternehmen müssen wichtige Anforderungen wie Designarchitektur, Betriebsmodelle und Skalierbarkeit berücksichtigen und die richtigen Fragen stellen, um zu ermitteln, wie gut die Plattform ihren Anforderungen entspricht. Verwenden Sie bei der Suche nach einer geeigneten Plattform für den Cloud-Workload-Schutz die Checkliste in Tabelle 2. Sie haben 100 Punkte zu vergeben – weisen Sie jeder Kernfrage je nachdem, wie sie auf Ihr Unternehmen zutrifft, entsprechend Punkte zu. Die Summe der Punkte in der Spalte „Gewichteter Wert“ sollte 100 ergeben. Füllen Sie diese Checkliste aus, um ein Gefühl dafür zu bekommen, wo Ihre wichtigsten Prioritäten liegen.

Checkliste für die Evaluierung einer Plattform zum Schutz von Cloud-Workloads

	WICHTIGSTE ANFORDERUNG	WICHTIGE FRAGEN	GEWICHTETER WERT
Designarchitektur	Beschreiben Sie, wie die Plattform zum Schutz von Cloud-Workloads die Kommunikation und Verbindungen zwischen Workloads darstellt.	Kann sie Telemetriedaten cloud-, workload-, netzwerk- und endpunktübergreifend konsolidieren?	
		Unterstützt sie jede Anwendung, ungeachtet von Betriebssystem, Konfiguration und Cloud, oder ist sie von einem dieser Aspekte abhängig?	
		Kann sie feststellen, was normales Verhalten innerhalb eines Workload oder zwischen verschiedenen Workloads ist?	
		Welche Verhaltensmodelle setzt sie ein, um Angriffe mit Malware und Nicht-Malware-Angriffe (dateilos) innerhalb von Workloads und zwischen den einzelnen Workloads zu erkennen?	
Betriebsmodell	Beschreiben Sie, wie die Plattform zum Schutz von Cloud-Workloads die Ausrichtung und reibungslose Koordination zwischen IT-Ops, DevOps und SecOps gewährleistet, um Risiken zu senken, die Compliance zu vereinfachen und die Resilienz zu erhöhen.	Wie viele Agents müssen auf den jeweiligen Workloads, Containern und Betriebssystemen installiert werden?	
		Können IT-Ops, DevOps und SecOps bei der Überwachung und Reaktion auf Vorfälle denselben Datensatz nutzen?	
		Welche Governance-Rahmenbedingungen unterstützt Ihre Plattform (z.B. NIST 800-53)?	
		Wie würde ein typischer Workflow zwischen IT-Ops, DevOps und SecOps ablaufen, sobald eine Bedrohung, Schwachstelle oder Fehlkonfiguration identifiziert ist?	
Skalierbarkeit	Beschreiben Sie, wie die Plattform zum Schutz von Cloud-Workloads sichere und dennoch schnelle Programme zur Änderungskontrolle unterstützt, um die Standardisierung von Sicherheitsrichtlinien zu erhöhen und das Risiko von Fehlkonfigurationen und anderen menschlichen Fehlern in großem Umfang zu reduzieren.	Wie hoch ist der durchschnittliche CPU-Verbrauch pro Agent für den Schutz von Cloud-Workloads?	
		Ist er in der Lage, mehrere Sicherheitsfunktionen, wie EDR, NGAV und Schwachstellenmanagement, in einem einzigen Agent und einer einzigen Managementkonsole zu konsolidieren?	
		Kann die Plattform zum Schutz von Cloud-Workloads eine standardisierte, konsistente Sicherheitsrichtlinie in Private, Public und Hybrid Cloud-Umgebungen durchsetzen und entsprechende Reports erstellen?	
		Wie werden regelmäßige Schwachstellenprüfungen durchgeführt, ohne dass Verfügbarkeit und Performance beeinträchtigt werden?	

TABELLE 2: Checkliste zur Evaluierung von Cloud-Workload-Schutz

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Willy-Brandt-Platz 2 81829 München Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de