Reduzieren Ihres Ransomware-Risikos

Wie VMware Sie beim Schutz Ihrer Multi-Cloud-Umgebungen vor Ransomware unterstützt

Erste Schritte

Die reale Ransomware-Bedrohung

Ransomware-Angriffe machten *im Jahr 2021 Schlagzeilen*, als sie in zahlreichen bekannten Unternehmen kritische Infrastrukturen lahmlegten und Betriebsunterbrechungen verursachten. Laut Prognosen von *Cybersecurity Ventures* wird alle 11 Sekunden ein Unternehmen Opfer eines Ransomware-Angriffs. In unserem eigenen *Global Security Insights Report 2021* identifizierten wir Ransomware als den „zweithäufigsten Vektor für Sicherheitsverletzungen“.

Durch den Erfolg von Ransomware wurden Cyberkriminelle ermutigt. Sie intensivieren ihre Bemühungen und erweitern ihre Fähigkeiten, um noch verheerendere Angriffe durchzuführen. Viele machen sich den wachsenden „Ransomware as a Service“ (RaaS)-Markt zunutze und steigern dadurch sowohl Geschwindigkeit als auch Reichweite, denn Angriffe können nun mit lediglich drei Klicks gestartet werden. In einem kürzlich von der Cybersecurity and Infrastructure Security Agency (CISA), dem Federal Bureau of Investigation (FBI) und der National Security Agency (NSA) gemeinsam veröffentlichten *Warnhinweis* internationaler Partner wurde bestätigt, dass die Bedrohung durch Ransomware-Angriffe aller Voraussicht nach in den kommenden Monaten weiter zunehmen und sich verschlimmern wird.

Angesichts der Unvermeidbarkeit von Ransomware ist es an der Zeit, sicherzustellen, dass sich Ihr Unternehmen verteidigen und die potenziellen Auswirkungen von Sicherheitsverletzungen auf den fortlaufenden Betrieb minimieren kann. In diesem E-Book wird erläutert, wie VMware Sie mithilfe von Carbon Black Cloud, NSX Security, VMware Cloud Disaster Recovery und Professional Services beim Schutz Ihrer Multi-Cloud-Umgebungen unterstützt, um das Ransomware-Risiko zu reduzieren und die Oberhand gegenüber Angreifern zu gewinnen.

Berücksichtigung des gesamten Lebenszyklus von Ransomware-Angriffen

Die Infiltration Ihres Unternehmens ist nur der erste Schritt eines Ransomware-Angriffs. Danach zielen Angreifer darauf ab, sich in Ihrer Umgebung einzunisten, sie zu analysieren und dadurch zu ermitteln, was Ihre wertvollsten Daten sind und wo sich diese befinden. In manchen Fällen stehlen Kriminelle die Daten (doppelte und dreifache Erpressung), bevor sie sie verschlüsseln. Anschließend fordern sie ein Lösegeld im Austausch für einen Entschlüsselungsschlüssel, der die Daten auf den Zustand vor dem Angriff zurücksetzt.

Um die Bedrohung dieser stetig zunehmenden und zerstörerischen Attacken tatsächlich zu minimieren, müssen Sie all die verschiedenen Schritte, Vektoren und Auswirkungen erkennen und unterbinden. Dazu ist es erforderlich, den gesamten Angriffslebenszyklus ganzheitlich zu betrachten und Fähigkeiten zu entwickeln, die die Risiken in jeder einzelnen Phase minimieren. Das National Institute of Standards and Technology (NIST) Cybersecurity Framework bietet eine Methode, um die für den kompletten Lebenszyklus benötigten Fähigkeiten zu erfassen und zu evaluieren:

Ermitteln und Nachvollziehen von Risiken für Ihre Systeme, Ressourcen, Daten und Funktionen

Abwehren bekannter Angriffe durch die Implementierung entsprechender Kontrollen und Schutzmaßnahmen

Erkennen von Angriffsaktivitäten

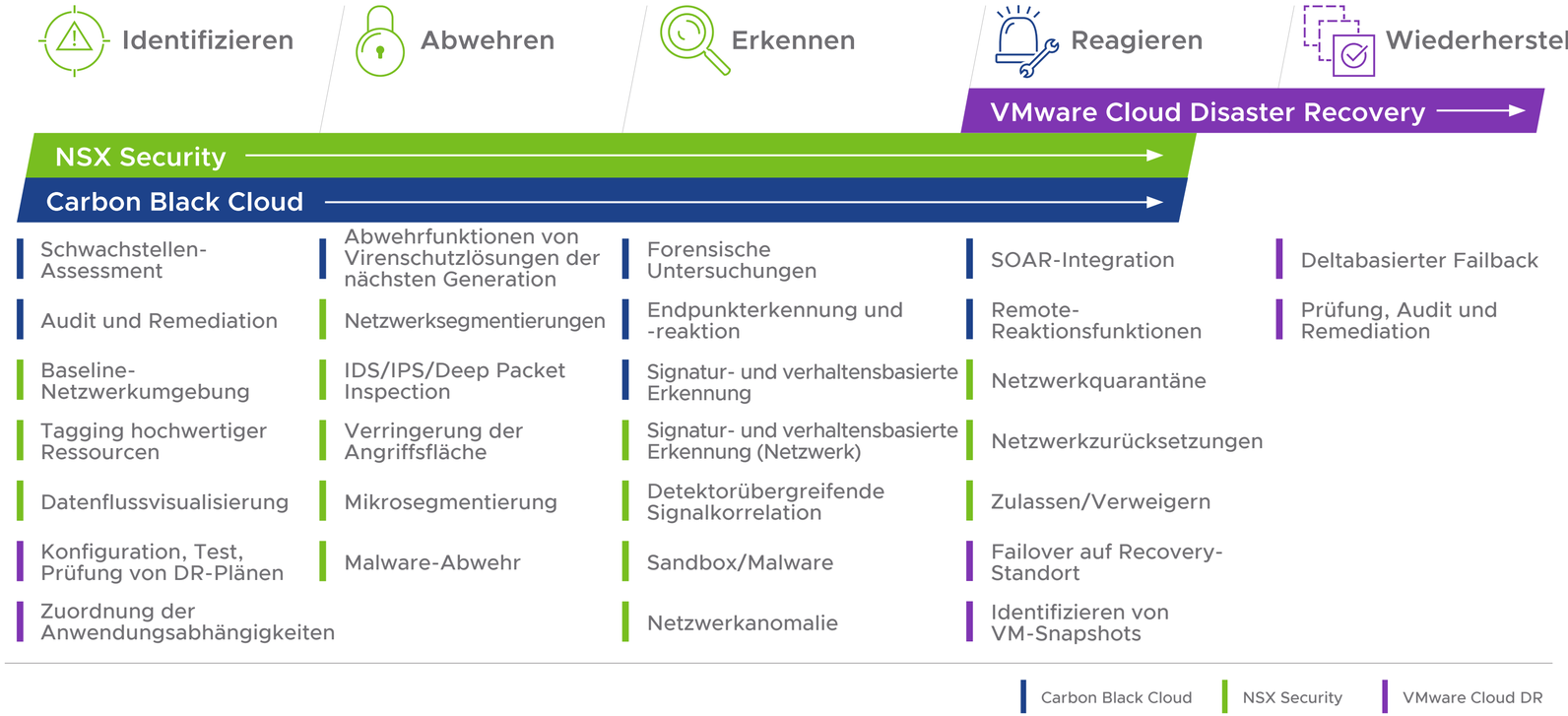
Reagieren, um Angriffe einzudämmen und abzuwehren

Recovery und Wiederherstellung auf den Betriebszustand vor dem Angriff

VMware hilft Ihnen dabei, Ihre Verteidigung über den gesamten Ransomware-Angriffslebenszyklus hinweg zu stärken und dadurch sowohl Ihre Resilienz zu verbessern als auch die Bedrohung zu minimieren.

VMware: Abdeckung des gesamten Ransomware-Lebenszyklus

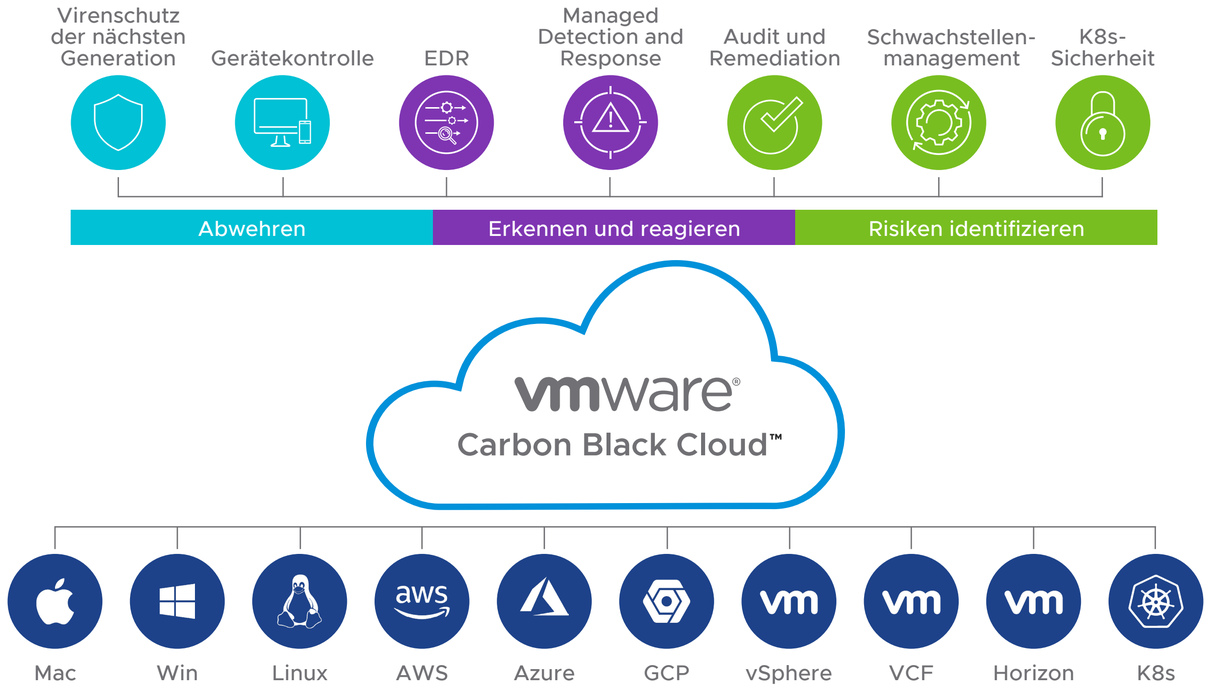
VMware-Lösungen (**VMware Carbon Black Cloud, NSX Security und VMware Cloud Disaster Recovery**) unterstützen Sie beim Entwickeln der im NIST-Framework beschriebenen Fähigkeiten, um Ransomware und andere Cyberrisiken umfassend zu bekämpfen. Beispielsweise können Sie all Ihre Workloads, Endpunkte, virtuellen Desktop-Infrastrukturen (VDIs), Netzwerke und Container schützen, sämtliche Pakete und Prozesse transparent gestalten und entsprechende Informationen für sich nutzen. Somit sind Sie in der Lage, Datenverkehr (z.B. East-West-Traffic, Command and Control, C2) und Nutzdaten zu identifizieren, die potenziell bösartig sind, und anschließend Maßnahmen zu ergreifen, um diese vollständig einzudämmen oder abzuwehren. Darüber hinaus können Sie schnelle, nahtlose Reaktions- und Recovery-Prozesse gewährleisten, sodass Ihr Unternehmen nur geringfügig oder überhaupt nicht beeinträchtigt wird.



VMware Carbon Black Cloud

VMware Carbon Black Cloud bietet u.a. Virenschutz der nächsten Generation (NGAV), Endpunkterkennung und -reaktion (EDR), erweiterte Bedrohungsbekämpfung, Schwachstellenmanagement sowie Rollback-Funktionen, sodass Sie Ihre Angriffsfläche verringern und Ihre kritischen Ressourcen vor Attacken schützen können. Mit Carbon Black Cloud profitieren Sie von mehreren Abwehrschichten, zuverlässiger Transparenz und Reaktionsfunktionen, um Ihre Umgebung vor Ransomware-Bedrohungen zu schützen.

Carbon Black Cloud-Plattform – Übersicht



Wichtige Vorteile für den Ransomware-Schutz:

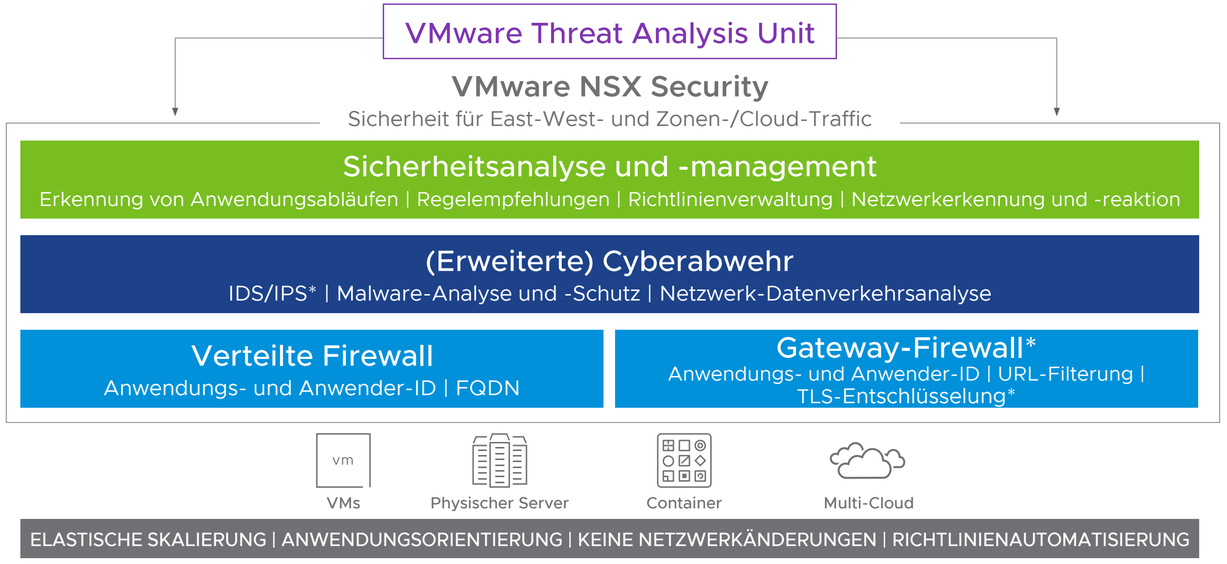
- Implementieren Sie einen **mehrschichtigen Abwehransatz**, der vor komplexen Bedrohungen (z.B. Ransomware) schützt und **bösartige Aktivitäten** in verschiedenen Angriffsphasen erkennt.
- Nutzen Sie **integrierte Reaktionsfunktionen, die die Problemlösung beschleunigen** und sämtliche Auswirkungen von Angriffen minimieren.
- **Suchen und filtern Sie nach allen Ereignissen** der letzten 30 Tage in Ihrer Umgebung, um sicherzustellen, dass Sie die erforderlichen Daten für Untersuchungen haben und Angriffe vollständig abwehren können.
- Erhalten Sie eine verständliche **Ereignisansicht mit visualisierten Benachrichtigungen**, die alle Aktivitäten anzeigen, sodass Sie Maßnahmen ergreifen und Kriminelle daran hindern können, sich in Ihrer Umgebung einzunisten.

VMware NSX Security

Mithilfe von VMware NSX Firewall können Sie die Netzwerksicherheit für Ihr gesamtes Netzwerk über eine zentrale Oberfläche verwalten und Anwendungen in Rechenzentrums-, Multi-Cloud- und Container-Infrastrukturen schnell schützen. Die Lösung bietet eine Software-Defined Layer 2-7-Firewall für jeden Workload. Dadurch gestaltet sich der detaillierte Schutz mit Netzwerk- und Mikrosegmentierung ganz einfach, d.h., falls (oder wenn) Angreifer in Ihr Netzwerk gelangen, sind sie in ihrem Bewegungs- und Aktivitätsradius extrem eingeschränkt. Sie können auch kontextbezogene Sicherheitsrichtlinien erstellen und erweiterte Funktionen für die Cybersicherheit nutzen, z.B. Systeme zur Erkennung und Abwehr von Eindringversuchen (IDS/IPS), Netzwerk-Datenverkehrsanalysen/Netzwerkerkennung und -reaktion (NTA/NDR) sowie Netzwerk-Sandboxing, um sich noch umfassender vor lateralen Bedrohungen zu schützen.

Transparenz und Durchsetzung über die gesamte Angriffskette hinweg

Zugriffskontrolle + ATP + Analyse und Management



* IDPS UND TLS-Entschlüsselung in GFW sind in NSX-T 3.2 nur als Tech Preview verfügbar.

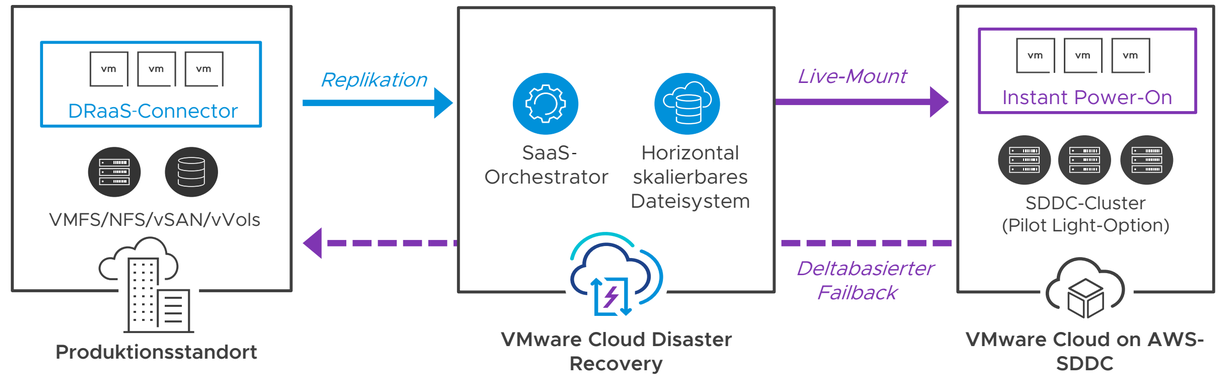
Wichtige Vorteile für den Ransomware-Schutz:

- Gewährleisten Sie eine **vollständige Sicherheitsabdeckung in Ihrem Netzwerk** für alle Datenverkehrsflüsse und Workload-Typen, sodass Ihnen nichts entgeht.
- Profitieren Sie von einer einfachen **Erstellung, Durchsetzung und Verwaltung detaillierter Mikrosegmentierungsrichtlinien**, um den East-West-Traffic zu schützen und es Angreifern schwer zu machen, sich in Ihrer Umgebung einzunisten.
- **Analysieren Sie komplexe Bedrohungen** mit einer Sandbox zur Emulation vollständiger Systeme, um zu ermitteln, mit was genau Sie es zu tun haben, und entsprechende Schritte zu unternehmen.
- **Stellen Sie infizierte Gastsysteme unter Quarantäne,** um **die laterale Ausbreitung** und Verbreitung von Angriffen zu verhindern.

VMware Cloud Disaster Recovery

VMware Cloud Disaster Recovery bietet eine bedarfsorientierte Ransomware- und Disaster Recovery, die als anwenderfreundliche SaaS-Lösung mit Cloud-Ökonomie bereitgestellt wird. Das Produkt kombiniert kosteneffizienten Cloud-Storage mit einfachem SaaS-basierten Management, um IT-Resilienz im erforderlichen Umfang durch einfache DR-Tests, Orchestrierung von Failover- und Failback-Plänen sowie optimierte Ransomware-Recovery sicherzustellen. Kunden profitieren von einem nutzungsbasierten Failover-Kapazitätsmodell für DR-Ressourcen.

VMware Cloud Disaster Recovery: Schutz Ihres Rechenzentrums in der Cloud



Blau: Betrieb im stabilen Zustand
Violett: aktiviert für Tests, Failover, Failbacks

Wichtige Vorteile für die Ransomware-Recovery:

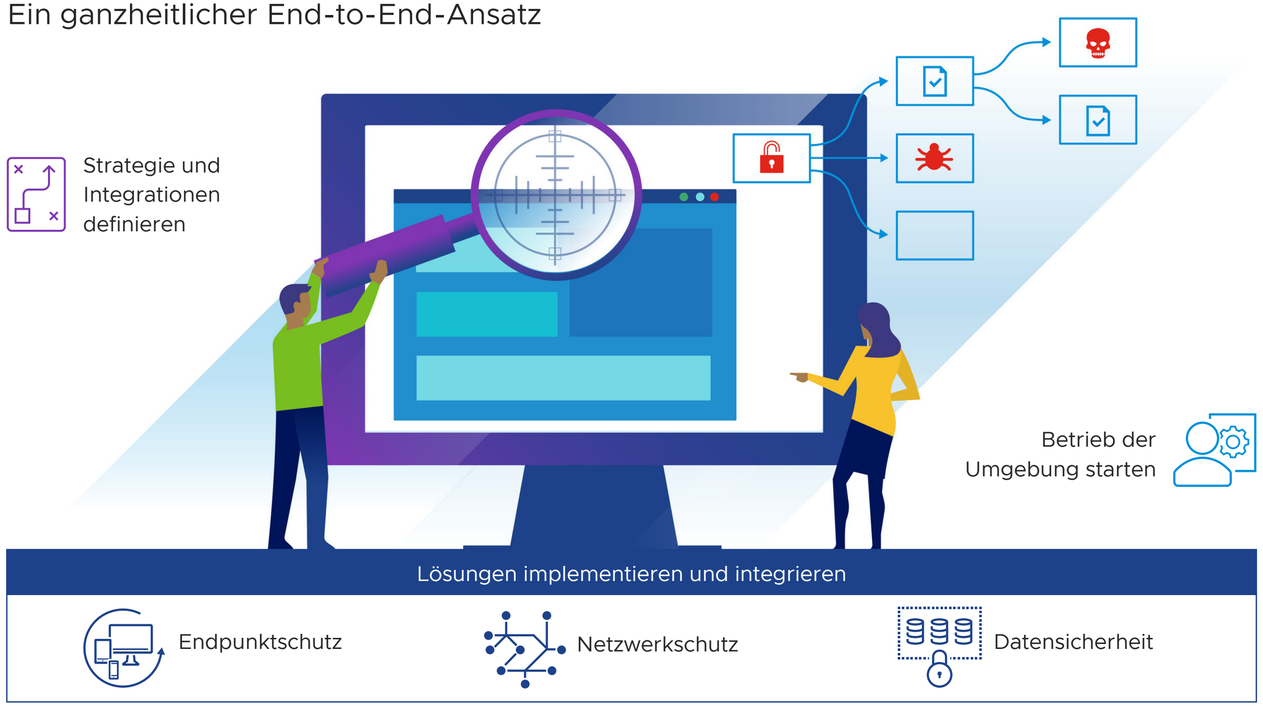
- Verwenden Sie **externe Air Gap-Backups**, um die direkten Auswirkungen eines Angriffs zu reduzieren.
- Stellen Sie mithilfe von **unveränderlichen VM-Snapshots und Datenintegritätsfunktionen** sicher, dass zuvor virenfreie Wiederherstellungspunkte nicht durch Malware verändert werden können.
- Erhalten Sie Recovery Point Objectives **(RPOs) von nur 30 Minuten** sowie einen **umfassenden Verlauf an Snapshot-Kopien**, um Ihre allgemeine Resilienz zu steigern.
- Verwenden Sie ein bedarfsorientiertes Software-Defined Datacenter (SDDC) in der Cloud, **um VMs sofort einzuschalten („Instant Power-On“)** und dadurch Unterbrechungen zu minimieren.
- Nutzen Sie **detaillierte Recovery-Funktionen**, um einzelne Dateien und Ordner von Wiederherstellungspunkten zu extrahieren, ohne dabei VMs einzuschalten. Führen Sie sie anschließend an einem endgültigen Wiederherstellungspunkt zusammen, um **Datenverlust bei der Recovery zu minimieren**.
- **Testen Sie** Ihre DR-Pläne **unterbrechungsfrei.**

VMware Professional Services

VMware Professional Services unterstützt Sie dabei, eine ganzheitliche Lösung zur Abwehr von Ransomware-Angriffen zu implementieren. Zunächst wird eine maßgeschneiderte Strategie definiert, die all Ihre Endpunkt-, Netzwerk- und Datensicherheitsanforderungen berücksichtigt. Sie erhalten Produktkonfigurationen und -integrationen sowie Hilfestellung bei sicherheitsrelevanten Gegenmaßnahmen und Betriebsverfahren, sodass Sie Produktimplementierung und -management optimieren können.

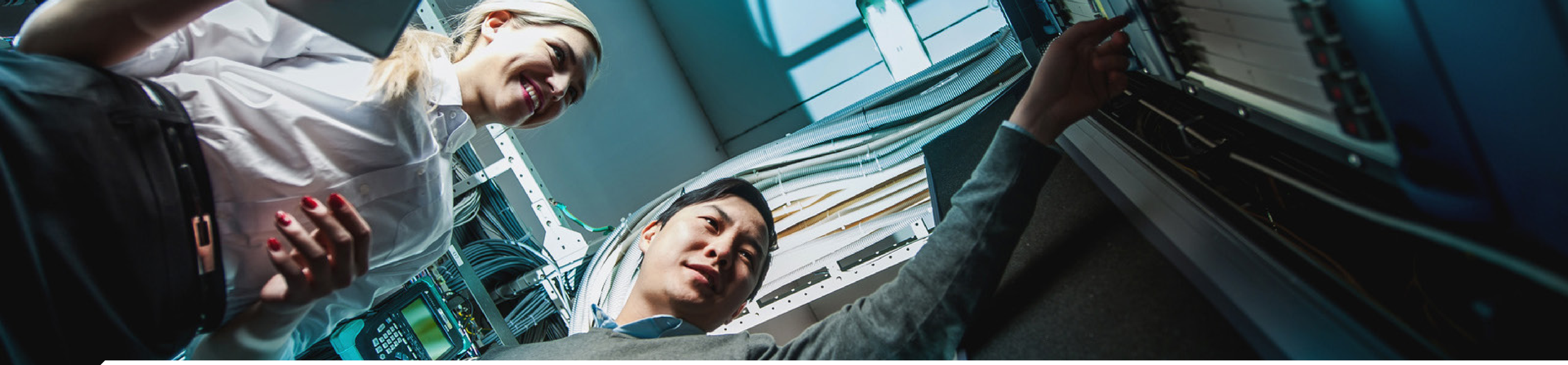
Ransomware-Risikominimierung – Implementierungsmethode

Ein ganzheitlicher End-to-End-Ansatz



Wichtige Vorteile für die Ransomware-Risikominimierung

- **Beschleunigen Sie die Implementierung** Ihrer Strategien und Lösungen für die Ransomware-Risikominimierung, um Risiken und Auswirkungen erfolgreicher Angriffe zu reduzieren.
- **Gewährleisten Sie eine bessere Recovery-Vorbereitung** für den Fall eines Angriffs, um Beeinträchtigungen im Hinblick auf vorhandene Ressourcen und Betriebsabläufe zu minimieren.
- **Verbessern Sie Sicherheitsprozesse** durch Wissenstransfer, betriebliche Hilfestellung und standardmäßige Betriebsverfahren, mit denen Sie Best Practices einführen und umsetzen können.
- **Minimieren Sie das Ransomware-Risiko** mit einem bewährten Ansatz und dem entsprechenden Fachwissen, um alle Phasen des Angriffslebenszyklus angemessen abzudecken.



Zusammenfassung: Schutz Ihres Unternehmens vor der Ransomware-Bedrohung

Ransomware-Attacken werden sich weiterhin ausbreiten und an Zerstörungskraft zunehmen, bis Unternehmen die Bedrohung ganzheitlich bekämpfen und Kriminellen das Leben in den einzelnen Angriffsphasen schwerer machen können. Dazu ist ein umfassender Ansatz wie der von VMware erforderlich, der Ihnen Folgendes bietet:

- **Identifizieren** und Bewältigen des Ransomware-Risikos in all Ihren Umgebungen
- **Unterbinden** bösartiger Aktivitäten mithilfe von detaillierten Kontrollen und Schutzmaßnahmen (z.B. Segmentierung/Mikrosegmentierung), die Angriffe im Keim ersticken
- **Erkennen** von Angriffsaktivitäten, einschließlich lateraler Ausbreitung und anderer ausgefeilter Taktiken, um diese abzuwehren und zu verhindern, dass sich Angreifer einnisten
- Schnelle **Reaktion**, um Angriffe vollständig einzudämmen und abzuwehren und aus Ihrer Umgebung zu beseitigen
- Schnelle **Recovery** und Wiederherstellung von Betriebsabläufen, um Auswirkungen auf Ihr Unternehmen zu minimieren

Weitere Informationen

VMware online:

Copyright © 2022 VMware, Inc. Alle Rechte vorbehalten. VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 Zweigniederlassung Deutschland Willy-Brandt-Platz 2 81829 München Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333
VMware und das VMware-Logo sind eingetragene Marken oder Marken von VMware, Inc. und dessen Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt. VMware-Produkte sind durch ein oder mehrere Patente geschützt, die auf der folgenden Webseite aufgeführt sind: vmware.com/go/patents.
Artikelnr.: Reducing Your Ransomware Risk ebook R2_DE 8/22