VERITAS

Cyber Resilience auf den Punkt gebracht

Veritas 360 Defense bietet eine Blaupause im Kampf gegen die modernen Cyberbedrohungen.

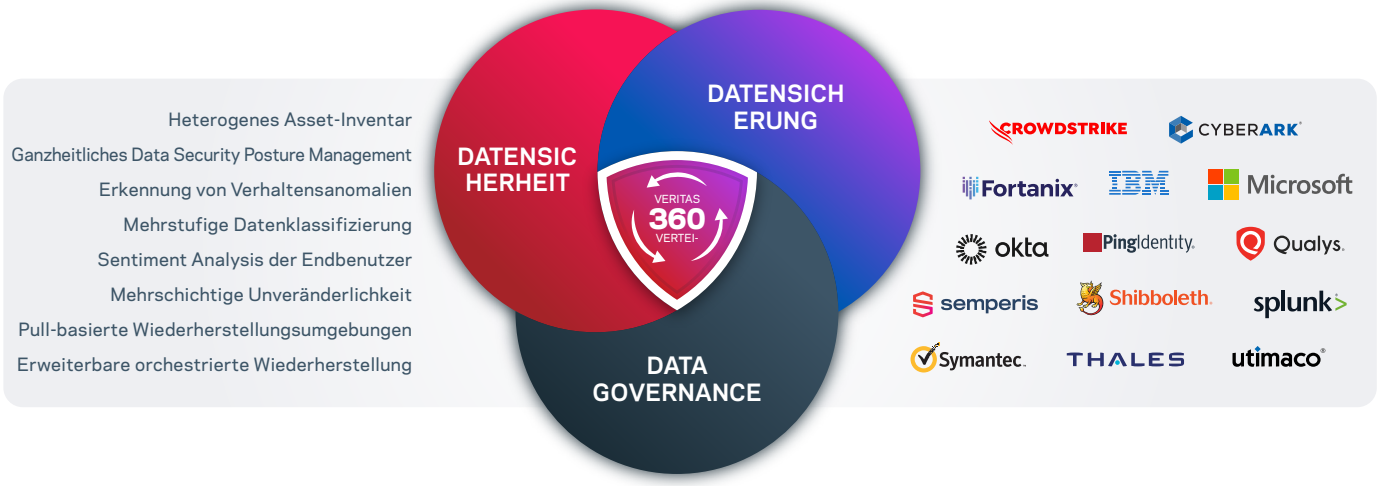
73 TAGE
Durchschnittliche Zeit bis zur Eindämmung eines Verstoßes nach der Identifizierung.[1]

Ausgeklügelte Ransomware-Angriffe erfordern einen ganzheitlichen Ansatz, um die Auswirkungen einer Sicherheitsverletzung zu mindern. Veritas 360 Defense vereint die traditionell getrennten Disziplinen Datensicherung, Datensicherheit und Data Governance, um zu gewährleisten, dass Ihre Daten sicher sind, schnell wiederhergestellt werden können und konform bleiben.

Angesichts der sich ständig weiterentwickelnden Bedrohungslandschaft müssen Teams an verschiedenen Standorten zusammenarbeiten, um Angriffe zu bekämpfen, die sich auf den Betrieb, den Umsatz und die Marke auswirken können. In funktionalen Silos kommen unterschiedliche Tools – oft in Verbindung mit benutzerdefiniertem Code – für die Angriffserkennung und -abwehr zum Einsatz, wodurch die Wiederherstellung verlangsamt wird. Solche DIY-Ansätze können zu Schwachstellen führen, die dann von Kriminellen ausgenutzt werden.

Veritas 360 Defense vereint Kernfunktionen aus dem Veritas-Portfolio mit vorintegrierten Lösungen aus unserem Ökosystem von Cybersicherheitspartnern, um Folgendes zu erreichen:

- Verstärken Ihrer Sicherheitslage
- Reduzieren der Auswirkungen von Ransomware-Angriffen mit einfacher und doppelter Erpressung
- Schnelle und zuverlässige Wiederherstellung, wie sie für eine erhöhte Resilienz erforderlich ist



Veritas 360 Defense ist die erste erweiterbare Architektur in diesem Bereich, die Datensicherung, Data Governance und Datensicherheit vereint. Es bietet eine breite Palette differenzierter Cyber-Resilience-Funktionen, die wir mit unserem Ökosystem führender Cybersicherheitsanbieter integriert und validiert haben. Anhand der Prinzipien „Von Grund auf sicher“ und „Standardmäßig sicher“ testen wir die Funktionen von Veritas 360 Defense rigoros anhand echten Ransomware-Varianten im Veritas REDLab (weitere Informationen zu REDLab finden Sie weiter unten).

Acht Merkmale, die Veritas 360 Defense auszeichnen

DATENSICHERHEIT

1. Heterogenes Asset-Inventar

Vollständige Transparenz gewährleistet das richtige Maß an Schutz für sämtliche Daten, um eine zuverlässige und genaue Wiederherstellung zu erreichen. Nutzen Sie die Berichterstellung für IT-Systeme, einschließlich Server, Speicher, Netzwerke, Hypervisoren, Cloud-Infrastruktur, hybride Cloud und herkömmliche Infrastruktur. Veritas bietet detaillierte Berichte zu Backups, auch bei anderen Anbietern. Sie können auch Rückbuchungsberichte, SLA-Berichte und Workflows für Warnungen und Ticketing erstellen.

2. Ganzheitliches Data Security Posture Management

Die Kontrolle und Klassifizierung unstrukturierter Daten schützt vor Diebstahl. Die Überwachung von Metadaten und Aktivitäten verhindert Insider-Bedrohungen, indem Benutzerverhalten, Zugriffsprobleme sowie anomales und böswilliges Verhalten erkannt und analysiert werden. Veritas ist einzigartig in Bezug auf die Breite der Datenabdeckung, die umfassende Klassifizierung und die Fähigkeit, über Inhaltsquellen hinweg zu korrelieren, einschließlich Sprache und Bildern.

Mit Veritas wissen Sie, über welche Art von Daten Sie verfügen und wo sie gespeichert sind. Im Falle eines Angriffs wissen Sie genau, ob sensible Daten kompromittiert wurden. Wir benachrichtigen die relevanten Stakeholder schnell und schaffen Klarheit über Zugangsprobleme, potenzielle Insider-Risiken und die wesentliche Art des Vorfalls.

3. Mehrstufige Datenklassifizierung

Veritas verwendet vordefinierte Richtlinien für den Datenschutz und branchenspezifische Richtlinien zur Klassifizierung von Inhalten. Die Klassifizierung geht über REGEX und Schlüsselwörter hinaus und umfasst auch den Vorlagenabgleich, die Dokumentähnlichkeit und die Stimmungsanalyse. Schnelle und gezielte Scans ermöglichen eine rasche Analyse großer Datenbestände. Dies reduziert die Zeit, die benötigt wird, um breite Datenquellen zu bewerten und tiefer in die riskantesten Sätze einzudringen.

DATA GOVERNANCE

4. Erkennung von Verhaltensanomalien

Erstellen Sie Benutzerprofile auf der Grundlage von sozialen Interaktionen und Rollen und identifizieren Sie fragwürdige Beziehungen und Aktionen – selbst von IT-Administratoren mit vollem Berechtigungsnachweis. Sie können Benutzerrisikobewertungen nutzen, um potenzielle Bedrohungen zu bewerten, Daten mit hohem Risiko zu priorisieren und Diebstahl und Zerstörung von Daten zu verhindern. Frühindikatoren liefern Kontext und bereichern Exfiltrationswarnungen, sodass Sie Nachforschungen anstellen können, bevor Schäden entstanden sind.

5. Sentiment Analysis der Endbenutzer

Erfassen und klassifizieren Sie Daten aus mehr als 120 Inhaltsquellen, um Verstöße gegen Unternehmensrichtlinien und Branchenvorschriften zu erkennen. Die Sentiment Analysis verwendet die Verarbeitung natürlicher Sprache, um subjektive Informationen aus Quellmaterialien zu identifizieren und zu extrahieren. Identifizieren Sie Einstellungen, Gefühle oder Emotionen auf der Grundlage von transkribierten Audio- oder schriftlichen Inhalten, um Einblicke in Insider-Risiken zu erhalten, und kennzeichnen Sie Inhalte zur manuellen Überprüfung auf regulierte Daten.

DATENSICHERUNG

6. Mehrschichtige Unveränderlichkeit

Veritas bietet End-to-End-Datenunveränderlichkeit für die branchenweit höchste Zahl an Speicherplattformen. Dieser mehrschichtige Ansatz ist im Backup-Katalog, in den Speicher-APIs und in der Sicherheit rund um die Zugriffskontrolle aus Netzwerk-, Benutzer- und Systemperspektive vollständig vorhanden. Unsere Lösungen unterstützen die Unveränderlichkeit in der Cloud für Cloud- und On-Prem-Backups. Somit kann eine Air-Gap-Kopie erstellt werden, die von einem Drittanbieter mit strengen Zugriffskontrollen verwaltet wird. Erfüllen Sie Branchenvorschriften und erfassen Sie Unternehmensdatensätze, indem Sie die Kommunikation in einem unveränderlichen Speicher protokollieren.

Veritas-Appliances verfügen über eine sichere Storage-Compliance-Uhr und Kontrollen, um unbefugten Datenzugriff zu verhindern, selbst durch vollständig privilegierte Administratoren. Cohasset Associates hat Veritas-Geräte auf die Einhaltung von SEC-, FINRA- und CFTC-Vorschriften geprüft.

7. Pull-basierte Wiederherstellungsumgebungen

Die Pull-basierte Replikation verhindert, dass Angreifer Daten in eine isolierte Wiederherstellungsumgebung verschieben. Es wird ein virtueller Air-Gap erstellt, in den nur autorisierte Daten eindringen dürfen, die aus der isolierten Umgebung angefordert werden. Für die Implementierung sind keine Tools von Drittanbietern oder teure Berater erforderlich.

8. Erweiterbare orchestrierte Wiederherstellung

Die orchestrierte Wiederherstellung für komplexe Anwendungen unterstützt die Zuordnung von Abhängigkeiten und benutzerdefinierte Aktionen mit einem einzigen Klick. Profitieren Sie von unterbrechungsfreien Proben Ihrer Produktionsumgebung und der Wiederherstellung von Backups und replizierten Systemen. Wenn es zu einem Cybervorfall kommt, können Sie eine schnelle Wiederherstellung durchführen.

VERITAS REDLab

Praxistests in Veritas REDLab

REDLab ermöglicht es Veritas, Ransomware- und Malware-Angriffe aus erster Hand zu untersuchen. In diesem isolierten Labor simulieren und führen wir regelmäßig echte Ransomware- und Malware-Angriffe auf unsere Produkte aus. Das REDLab-Team bewertet Funktionen, die bei der Erkennung von Cyberangriffen, dem Schutz von Backup-Repositories und der Infrastruktur sowie der Beschleunigung der Wiederherstellung helfen. REDLab hat sich als äußerst wertvoll erwiesen, um die Zuverlässigkeit der Lösung zu gewährleisten und eine Roadmap für zukünftige Innovationen zu erstellen. Darüber hinaus werden Partnerintegrationen auch in realen Angriffsszenarien validiert.

Implementieren Sie Veritas 360 Defense noch heute

Die Kombination von Datensicherungs-, Datensicherheits- und Data-Governance-Lösungen mit unserem Ökosystem von Cybersicherheitspartnern bietet die einheitliche 360-Grad-Sicht, mit der sich gewährleisten lässt, dass Daten sicher sind, die Wiederherstellung schnell erfolgt und Compliance-Anforderungen erfüllt werden. Erfahren Sie mehr über Veritas 360 Defense und wie es die Blaupause für vollständige Cyber Resilience bildet.

1. IBM 2023 Cost of a Data Breach Report

Über Veritas

Veritas Technologies ist ein weltweit führender Anbieter im Bereich Multicloud-Datenmanagement. Über 80.000 Kunden – darunter 95 Prozent der Fortune 100 – vertrauen darauf, mit Lösungen von Veritas den Schutz, die Wiederherstellbarkeit und Compliance ihrer Daten zu gewährleisten. Veritas steht für skalierte, zuverlässige Produkte, welche die Widerstandsfähigkeit bieten, die seine Kunden im Fall von Cyberangriffen wie Ransomware benötigen. Kein anderer Anbieter erreicht die Leistungsfähigkeit von Veritas mit Unterstützung für mehr als 800 Datenquellen, über 100 Betriebssysteme, über 1.400 Speicherziele und über 60 Clouds im Rahmen eines einzigen, einheitlichen Ansatzes. Mithilfe der Cloud Scale Technology setzt Veritas heute seine Strategie für autonomes Datenmanagement um, die den betrieblichen Aufwand reduziert und gleichzeitig einen größeren Mehrwert bietet. Weitere Informationen finden Sie unter veritas.com/de/de und folgen Sie uns auf Twitter unter @veritastechllc.

VERITAS

Veritas (Deutschland) GmbH
Theatinerstr. 11, 8. Etage
80333 München
Tel.: 0800-724 40 75
veritas.com/de/de

Die weltweiten Kontaktinformationen finden Sie hier:
veritas.com/de/de/company/contact

V2014 11/23