Acronis

#CyberFit

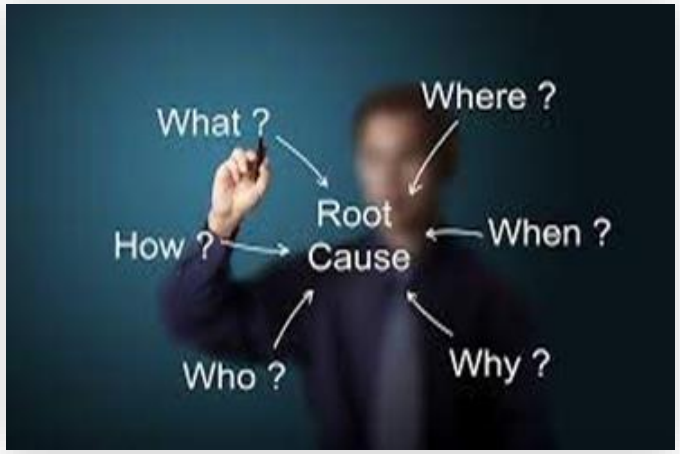
So machen Sie mit EDR Hackern das Leben schwer

Cybersicherheit optimieren: Warum EDR unverzichtbar ist

Marcel Henker – Acronis Germany GmbH – Juli 2023

Was ist EDR?

EDR (Endpoint Detection and Response = Endpunkterkennung und -reaktion**)** ist eine Plattform zur Korrelation von Sicherheitsereignissen, die **hochentwickelte Bedrohungen oder laufende Angriffe** erkennt und abwehren kann.



Primäre EDR-Funktionen laut Gartner:

- Erkennung von Sicherheitsvorfällen
- Eindämmung des Vorfalls auf dem Endpunkt
- Untersuchung von Sicherheitsvorfällen
- Bereitstellung von Anleitungen zur Behebung

Bedeutung von EDR

Hochentwickelte Angriffe lassen sich nur mit erweiterten Sicherheitsfunktionen abwehren

Mehr als 60 % aller Datenkompromittierungen **gehen auf die eine oder andere Form von Hacking zurück**.

Im Durchschnitt vergehen bis zur Identifizierung einer Sicherheitsverletzung ganze **207 Tage**.

Kompromittierungen sind unvermeidbar – Sie müssen sich darauf vorbereiten

70 Tage bis zur Eindämmung einer Sicherheitsverletzung

4,35 Millionen US-Dollar durchschnittliche Gesamtkosten einer Datenschutzverletzung

76 % der Sicherheits- und IT-Teams **fehlt ein einheitlicher Überblick** über Anwendungen und Assets

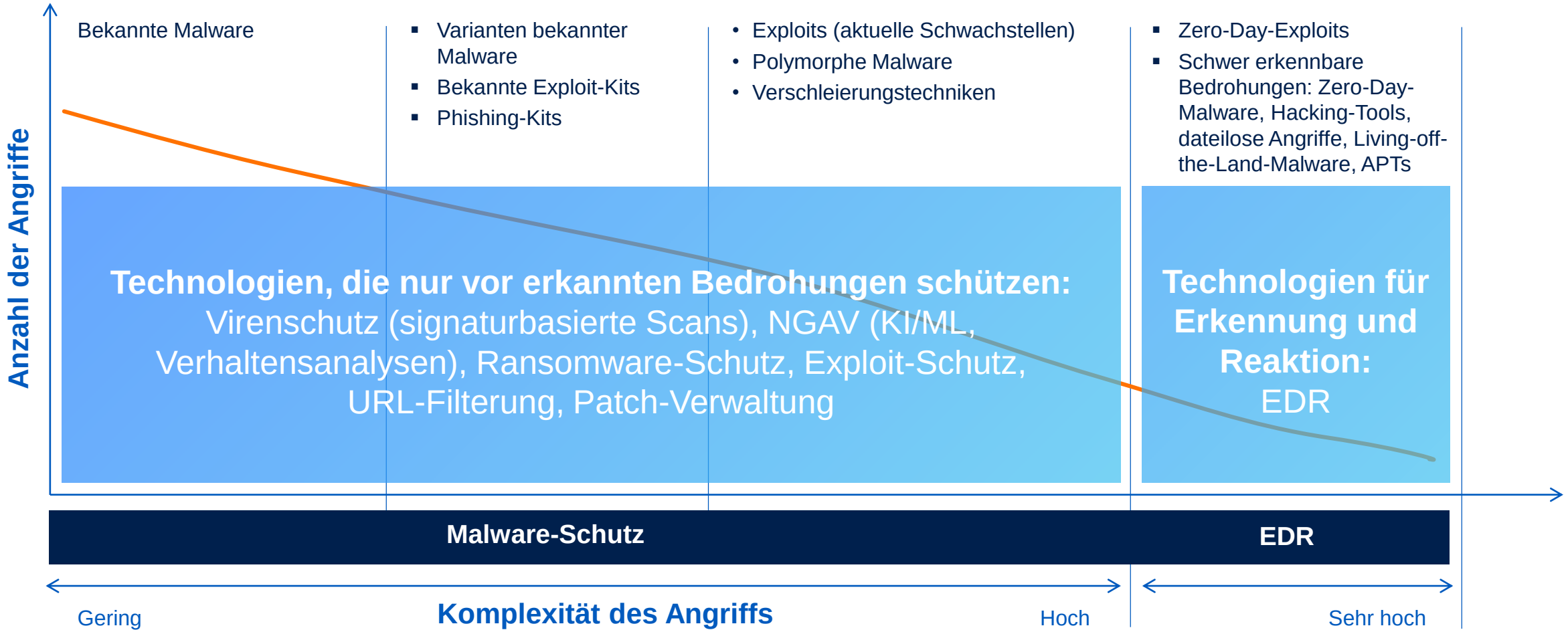
Für viele ist Compliance verpflichtend

Gesetze schreiben vor, dass Unternehmen **Sicherheitsverletzungen innerhalb eines knappen Zeitraums melden** müssen (z. B. laut DSGVO innerhalb von 72 Stunden)

70 % der Vorfälle betreffen personenbezogene Informationen (aufgrund gesetzlicher Vorgaben sind Analysen nach dem Zwischenfall erforderlich)

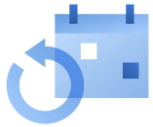
Quellen: Verizon: „Data Breach Investigations Report“, 2022; IBM Security und Ponemon Institute: „Cost of data breach report“, 2022; ServiceNow: „Costs and Consequences of Gaps in Vulnerability Response“, 2020; IDC: „Investigation or Exasperation? The State of Security Operations“

So schützt EDR vor mehr Bedrohungen



Die Einbindung eines EDR-Services war herausfordernd – bis jetzt!

Bestehende EDR-Lösungen sind mit hoher Komplexität, erheblichen Kosten und einem langen Zeitraum bis zur Amortisierung verbunden. Bieten Sie jetzt dank Acronis im Handumdrehen effektive und effiziente EDR-Services für Unternehmen aller Größen an.

Herausforderungen	 **Kosten und Komplexität**	 **Eingeschränkte Geschäftskontinuität & zahlreiche Lösungen**	 **Channel-Konflikt und Unterstützung für MSPs**	 **Verbesserung der Vorfallanalysen und Reaktionszeiten**	 **Begrenzte Sensibilisierung für Compliance-Fragen**
Vorteile von Acronis	**Innovation demokratisiert den EDR-Massenmarkt**	**Umfassende NIST-Abdeckung von der Identifizierung bis zur Wiederherstellung**	**Solution Provider-Partner orientierter Ansatz**	**Schnelle Analyse und Reaktion**	**Problemlose Einhaltung von Vorschriften**

Acronis
Cyber Protect Cloud

#CyberFit

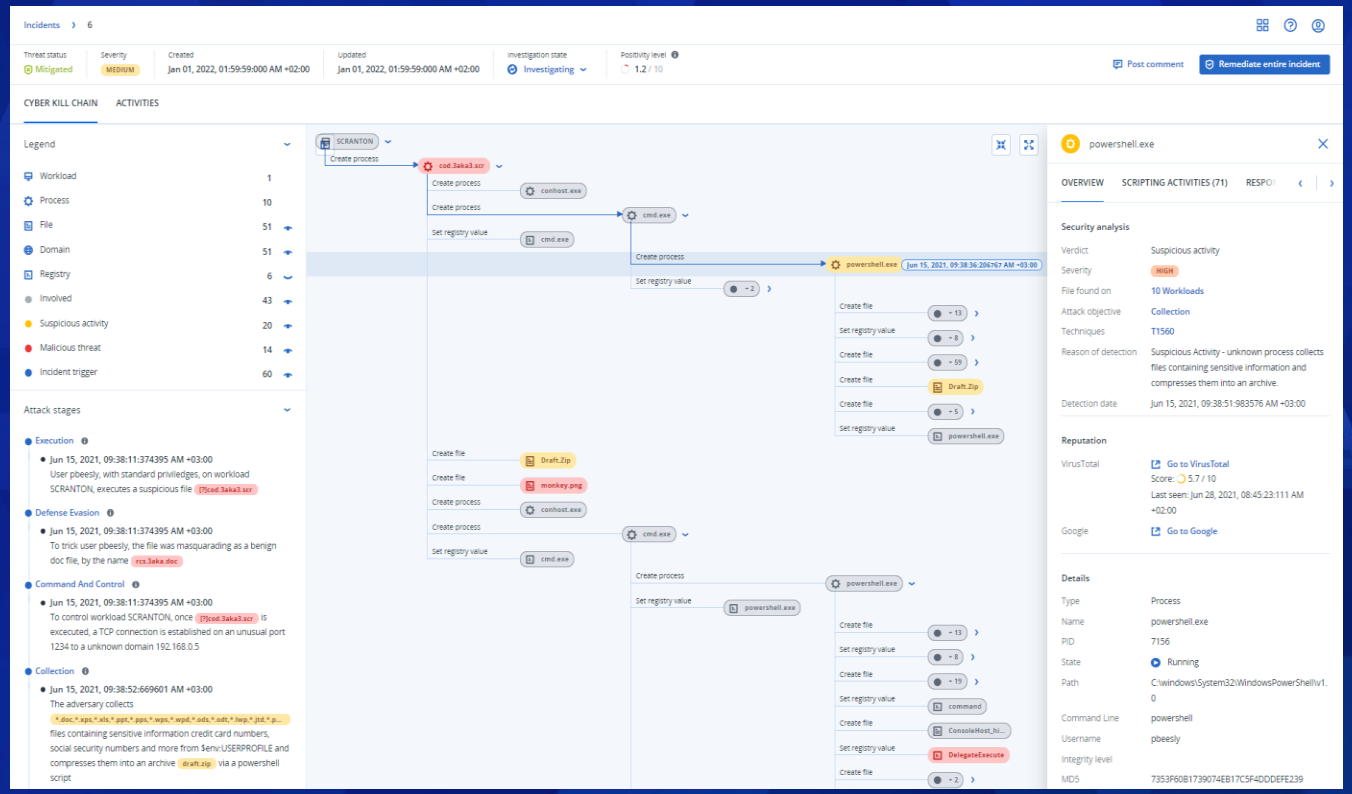
Advanced Security + Endpoint Detection and Response (EDR)

Speziell für Service Provider, um Endpunktsicherheit zu vereinfachen

1. **Schnelle Priorisierung und Analyse nach einem Angriff**

2. **Geschäftskontinuität** durch integrierte Funktionen für Backup und Recovery

3. **Einfache Einführung von Services** mit einer zentralen Plattform und einem einzigen Agenten – zur einfachen Bereitstellung, Verwaltung und Skalierung

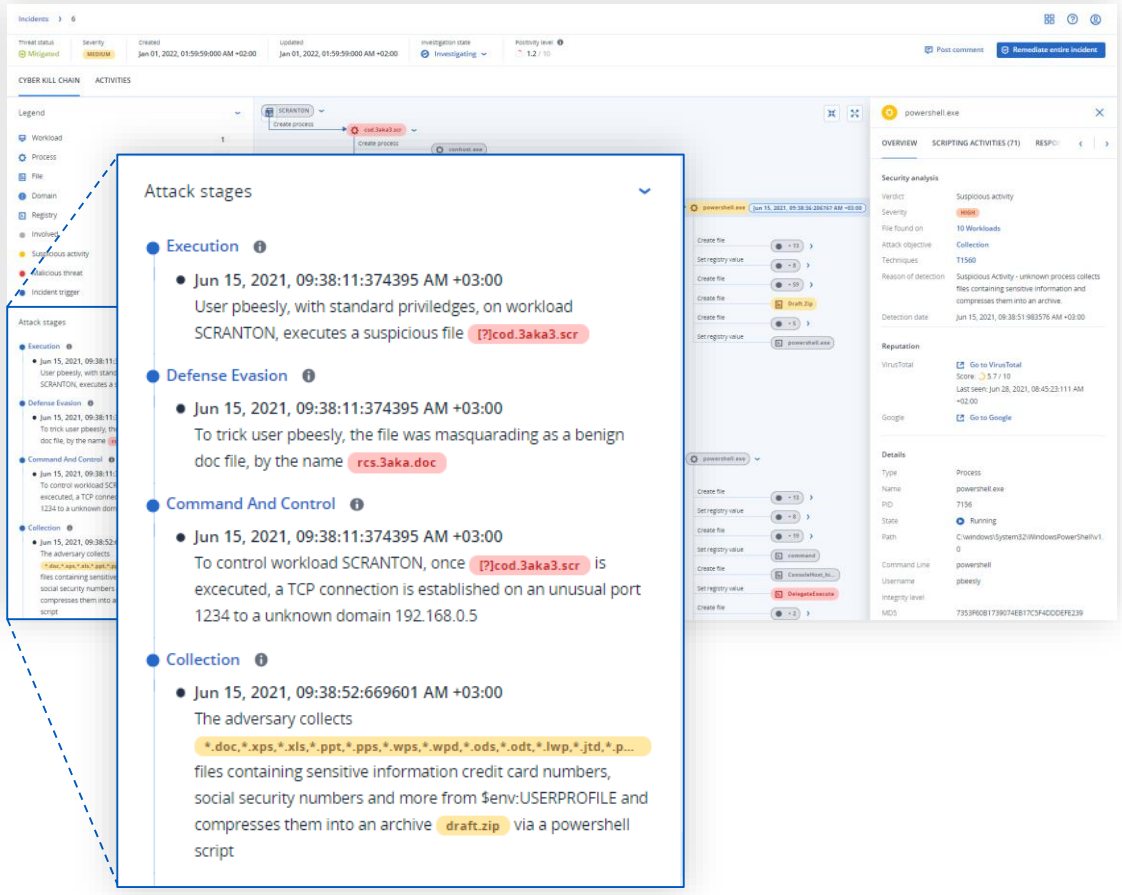


Analyse von Angriffen innerhalb von Minuten für schnelle Reaktionen

Profitieren Sie von KI-basierter, nutzerfreundlicher Auswertung von Angriffen und priorisierter Sichtbarkeit.

Ihr Team kann mühelos Angriffe analysieren sowie schnell und einfach folgende Aufgaben erledigen:

- **Vollständiger Überblick mit Priorisierung der verdächtigen Aktivitäten** auf allen Endpunkten statt einer einfachen Liste aller Warnmeldungen.
- **Vollständiger Überblick über die Angriffskette.** Die Entwicklung des Angriffs ist dem MITRE-Framework (Branchenstandard) zugeordnet.
  - Wie erfolgte der Erstzugriff?
  - Wie wurden die Spuren verwischt?
  - Wie ist Schaden entstanden?
  - Wie hat sich der Angriff ausgebreitet?
- **Sparen Sie Zeit und Geld**, da Sie keine strikten Schulungen oder Spitzenpersonal für die operativen Aufgaben benötigen.
- **Konzentration auf Wichtiges** dank eines Bedrohungsdaten-Feeds für neue Bedrohungen, sodass Sie nach Kompromittierungsindikatoren suchen können.

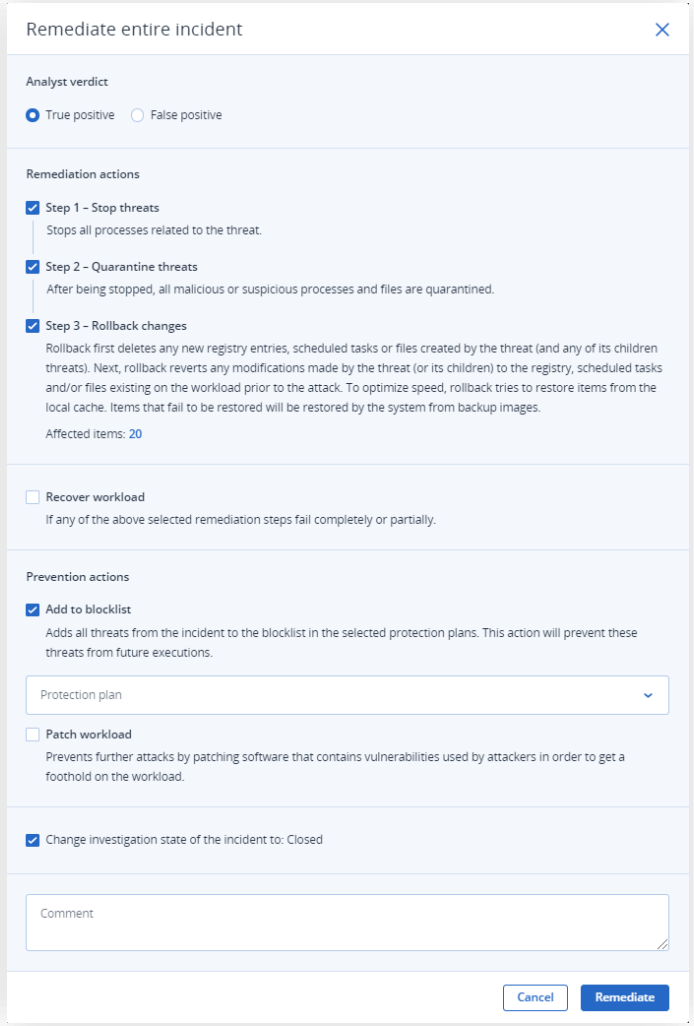


Stoppen von Angriffen und Gewährleistung der Geschäftskontinuität

Setzen Sie statt auf Einzellösungen auf eine integrierte Plattform für unübertroffene geschäftliche Resilienz.

- Weitere Untersuchungen mithilfe von Remote-Verbindungen und forensischen Backups
- Eindämmung von Bedrohungen, indem Sie betroffene Workloads vom Netzwerk isolieren
- Behebung durch Stoppen von Malware-Prozessen, Isolierung von Bedrohungen und Rollback von Änderungen
- Verhinderung des Wiederauftretens von Vorfällen – dank Software-Patch-Verwaltung und Blockierung erkannter Bedrohungen
- Gewährleistung einzigartiger Geschäftskontinuität mit integrierten Recovery-Funktionen, einschließlich angriffsspezifischer Rollbacks, Wiederherstellung auf Datei- oder Image-Ebene sowie Disaster Recovery

Wählen Sie aus, welche Maßnahmen Sie ergreifen möchten, und reagieren Sie mit einem Klick.



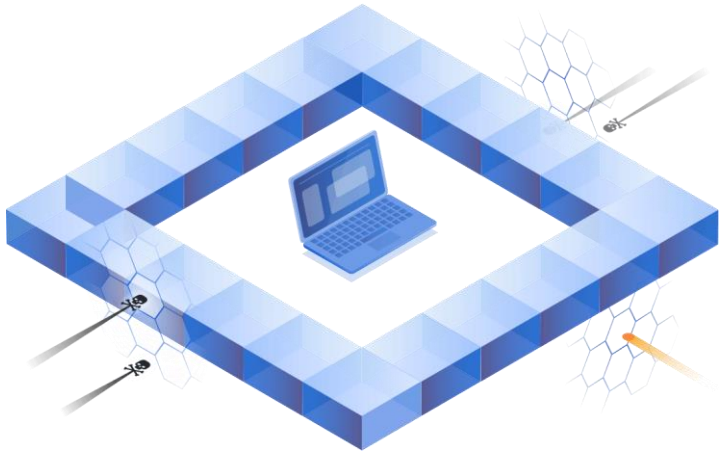
Umfasst alle Funktionen von Advanced Security

Stoppen Sie Bedrohungen, bevor sie zu schwerwiegenden Sicherheitsverletzungen werden.

Malware-Schutz der nächsten Generation: Verhinderung von Bedrohungen mit signatur- und verhaltensbasiertem Endpunktschutz

URL-Filterung: Ausweitung der Cyber Protection auf Web-Browser, um Angriffe von böswilligen Websites zu verhindern

Exploit-Schutz: Reduzierung des Risikos durch Exploits und Malware, die Software-Schwachstellen auszunutzen versuchen



Intelligente Schutzpläne: Automatische Anpassung von Patch-Installationen, Scans und Backups basierend auf Bedrohungsalarmen aus den Acronis Cyber Protection Operation Centers

Forensisches Backup: Forensische Untersuchungen durch Erfassung digitaler Beweise in Image-basierten Backups

Besserer Schutz mit weniger Aufwand: Malware-Schutz für Backups und gründlichere Scans, indem die Daten in zentralen Storage (z. B. die Cloud) ausgelagert werden

Sicheres Recovery: Verhinderung von Re-Infektionen durch Malware-Scans von Backups und Aktualisierungen der Virenschutz-Datenbank während des Wiederherstellungsprozesses

Globale und lokale Positivlisten: Basierend auf Backups für gründlichere Heuristik durch Vermeidung falscher Erkennungen

Acronis: Geschäftskontinuität für alle Bereiche des NIST-Frameworks

IDENTIFIZIERUNG

SCHUTZ

ERKENNUNG

REAKTION

WIEDER-HERSTELLUNG

	IDENTIFIZIERUNG	SCHUTZ	ERKENNUNG	REAKTION	WIEDER-HERSTELLUNG
Advanced Security + EDR	▪ Hardware-Inventarisierung ▪ Erkennung ungeschützter Endpunkte	▪ Schwachstellen-Bewertungen ▪ Exploit-Schutz ▪ Gerätekontrolle ▪ Verwaltung der Sicherheits-konfiguration	▪ Feed zu neuen Bedrohungen ▪ Suche nach Kompromittierungs-indikatoren neuer Bedrohungen ▪ Malware- und Ransomware-Schutz ▪ KI- und ML-basierte Verhaltenserkennung ▪ URL-Filterung	▪ Schnelle Vorfallanalyse ▪ Workload-Behebung mit Isolierung ▪ Forensische Backups	▪ Schnelles Rollback von Angriffen ▪ Massenwiederherstellungen per Mausklick ▪ Self-Service-Recovery
Acronis Cyber Protect Cloud	▪ Software-Inventarisierung ▪ Datenklassifizierung	▪ Patch-Verwaltung ▪ DLP ▪ Backup-Integration ▪ Cyber Scripting	▪ E-Mail-Schutz	▪ Untersuchungen per Remote-Verbindung	▪ Vorab mit Disaster Recovery integriert

Acronis als Service Provider-Partner

Gemeinsamer Erfolg statt Konkurrenz! Wir unterstützen Sie bei Ihrem Wachstum.

- **Schnelle Bereitstellung von Services** durch einen modularen Ansatz mit nur einer Konsole und einem Agenten
- Innovation ermöglicht **hochwertige Services mit gesunden Margen** bei Kund:innen aller Größen
- **Kontrolle der Gesamtbetriebskosten (TCO) und einfaches Service-Tiering und Management** mit einer einzigen, integrierten Plattform
- Zusammenarbeit mit einem Anbieter und Partner, **der sich auf Ihren Erfolg konzentriert und bei MDR-Services nicht mit Ihnen konkurriert**
- Acronis #CyberFit Partnerprogramm und Unterstützung – Assets, Schulungen, Marketing- und Vertriebs-Support

THE CHANNEL CO. CRN SECURITY 100 2022

ChannelPro SMB FORUM 2022 WINNER BEST REVENUE BOOSTER

1	Agent	Richtlinie	Konsole	Lizenz	Anbieter

Schnelle Service-Bereitstellung

Vollständige Abdeckung des NIST-Frameworks

Verbesserte Leistung

Preisgekrönte Endpoint Protection

Durch AV-Comparatives bestätigte Business-Sicherheit

Test des Schutzes unter realen Bedingungen – **0 False Positives**

Test des Malware-Schutzes – **0 False Positives**

AV-TEST-zertifiziert

Erkennung und Blockierung hochentwickelter Bedrohungen – **100 % Erkennungsrate**

0 False Positives

Zertifiziert durch ICSA Lab

0 False Positives

VB100-zertifiziert

0 False Positives

Goldmedaille für Endpunktschutz

4.5 Excellent

Mitglied der Microsoft Virus Initiative

Mitglied der Anti-Malware Testing Standard Organization

Mitglied der Anti-Phishing Working Group

Teilnehmer und Testsieger bei Anti-Malware Test Lab

VIRUSTOTAL-Mitglied

Mitglied der Cloud Security Alliance

Advanced Security + EDR: Vier wichtige Anwendungsfälle

Erkennung und Abwehr von Angriffen noch vor Kompromittierungen

- **Überwachung und Korrelation von Ereignissen** auf Endpunkten
- **Blockierung gängiger Bedrohungen** mit preisgekröntem Endpunktschutz
- **Erkennung hochentwickelter Bedrohungen** und Analyse innerhalb von Minuten

Reaktion, bevor Schaden entsteht

- **Zuverlässige Geschäftskontinuität** dank integrierter Recovery
- **Reduzierung der Auswirkungen** durch Isolierung von Prozessen und Workloads
- **Verringerte Angriffsfläche** zum Schutz vor zukünftigen Bedrohungen

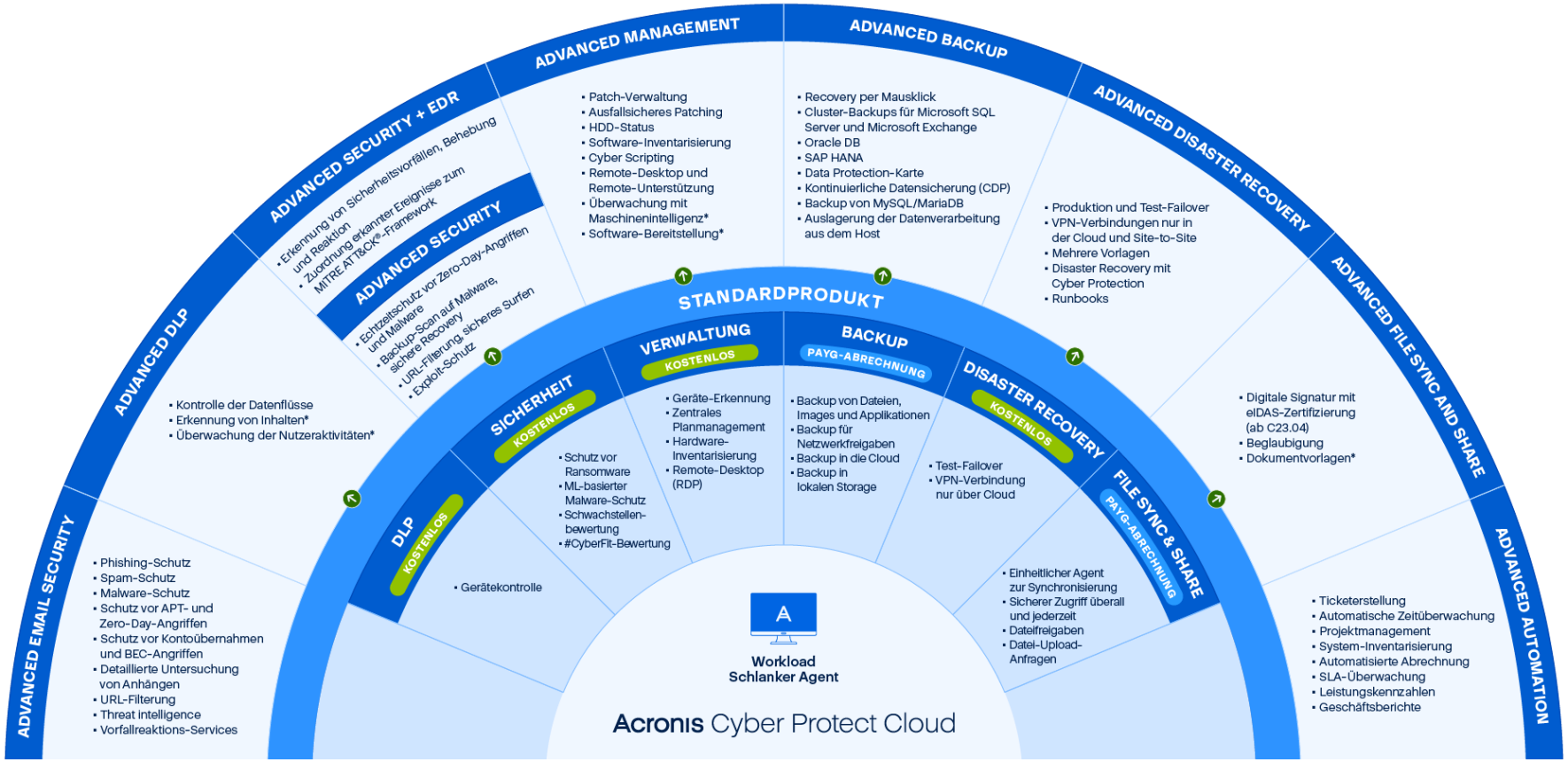
Unterstützung von Compliance und Cyberversicherungen

- **Meldung von Zwischenfällen auf Endpunkten** basierend auf MITRE ATT&CK®
- **Klassifizierung sensibler Daten**
- **Erfassung forensischer Daten** in Backups

Konsolidierung von Lösungen

- **Schnelle Einführung und Skalierung** über eine Plattform, die für MSPs entwickelt wurde
- **Senkung der Kosten** mit einheitlicher Service-Verwaltung

Zusätzliche Advanced-Pakete:
Security, Backup, Disaster Recovery, Email Security, File Sync and Share, Management, DLP und **jetzt auch EDR**



* Demnächst verfügbar

Optimiert für alle Workloads

Schnelle Service-Bereitstellung

Konsolidierung der Anbieter

Acronis

F&A

Partner-DE@acronis.com

Partner Success Center:

https://www.acronis.com/de-de/partners/success-center

#CyberFit

Acronis

Cyber Foundation

Program

Bildung für einen starken Start ins Leben

Wir möchten allen Menschen eine Chance geben, neues Wissen zu erschaffen und mit vielfältigen Erfahrungen und Stärken eine erfolgreiche Zukunft aufzubauen!

Seien Sie dabei!