

# Acronis Detection and Response



## VERHINDERN SIE ANGRIFFE IN ECHTZEIT UND VERSCHAFFEN SIE SICH TIEFE EINBLICKE IN JEDE CYBER-BEDROHUNG

Acronis Detection and Response ist eine letzte Verteidigungslinie, die Ihr Unternehmen auch vor solchen Bedrohungen schützen kann, die Ihre Antimalware-Abwehr sonst umgehen könnten. Die Lösung wurde mit einem Zero-Trust-Ansatz entwickelt, um alle Abweichungen vom regulären Verhalten des Betriebssystems zu erkennen und zu stoppen. Sie bietet zudem eine Echtzeit-Übersicht und ermöglicht automatische sowie manuelle Schadensbehebungsmaßnahmen.

| BEDROHUNGSUNABHÄNGIGE SICHERHEIT  | BEDROHUNGSABWEHR IN ECHTZEIT   | FOKUSSIERTE UND DETAILREICHE SICHTBARKEIT   |
|---|--|---|
| Steigern Sie Ihre Endpoint Security-Fähigkeiten mit einer Threat Detection & Response-Technologie. Verhindern Sie Angriffe, die sich konventionellen Abwehrmaßnahmen entziehen können – wie z.B. Angriffe durch neue bzw. bisher unbekannte Malware, Ransomware, Zero-Day-Exploits oder durch APT-Techniken und dateilose Angriffe. | Beschränken Sie sich nicht nur darauf, nachträglich auf Sicherheitsverletzungen zu reagieren. Stellen Sie eine bewährten Lösung bereit, die automatisch verhindern kann, dass es überhaupt zu Schäden kommt. Es ist keine manuelle Bedrohungssuche, keine kostspielige Infrastruktur und auch kein Cloud-Konnektivität erforderlich. | Verschaffen Sie Ihrem Sicherheitsteam detaillierte Einblicke in die Zeitabläufe, die Quelle sowie die Taktiken, Techniken & Prozeduren (TTPs) der Angriffe. Außerdem erhalten Sie Einschätzungen darüber, was die Angreifer zu erreichen versuchten. Mit all diesen Informationen können Sie anschließend die Sicherheitslage Ihres Unternehmens deutlich verbessern. |

## SCHÜTZEN SIE IHRE ENDPUNKTE UND DATEN VOR ANGRIFFEN, DIE ANDEREN VERBORGEN BLEIBEN


| MINIMIEREN SIE CYBER-RISIKEN / WEHREN SIE JEDE BEDROHUNG AB  | SORGEN SIE FÜR SCHNELLE REAKTIONEN AUF VORFÄLLE   | NUTZEN SIE IHRE VORHANDENEN RESSOURCEN IN VOLLEM UMFANG AUS   |
|--|---|---|
| <ul style="list-style-type: none"> <li>• Erkennen und verhindern Sie auch fortschrittliche Malware-Angriffe, die ihren bisherigen Abwehrmaßnahmen entgehen könnten – wie z.B. Angriffe durch neue bzw. bisher unbekannte Malware, Zero-Day-Exploits oder durch APT-Techniken und dateilose Angriffe</li> <li>• Fügen Sie eine letzte Verteidigungsebene hinzu, um Ihre derzeitigen Abwehrfähigkeiten zu verbessern und Sicherheitsverletzungen zu stoppen, bevor diese die digitalen Vermögenswerte Ihres Unternehmens schädigen können</li> <li>• Verfolgen Sie einen Zero-Trust-Ansatz und erfassen Sie jede Abweichung vom regulären Verhalten des Betriebssystems</li> <li>• Funktioniert auch in Air-Gap- und Offline-Umgebungen</li> </ul> | <ul style="list-style-type: none"> <li>• Verringern Sie Ihre Reaktionszeiten auf Bedrohungen durch automatische Präventionsfähigkeiten</li> <li>• Ermöglichen Sie Ihrem Security Operations Center-Team detaillierte Einblicke in jeden Angriff</li> <li>• Nutzen Sie automatische und manuelle Schadensbehebungsmaßnahmen</li> <li>• Überwachen Sie kontinuierlich die Endpunkt- und Netzwerk-Aktivitäten im gesamten Unternehmen</li> </ul> | <ul style="list-style-type: none"> <li>• Reduzieren Sie den Bedarf für zusätzliche Ressourcen durch fokussierte und detaillierte Einblicke in aktuelle Bedrohungen – ohne dass Ihr Team dabei mit unnötigen Informationen überfrachtet wird</li> <li>• Sie können Ihre bestehenden Antimalware-Lösungen einfach ergänzen, ohne diese auseinanderreißen oder ersetzen zu müssen</li> <li>• Die Endpunkt-Performance und der Bandbreitenverbrauch werden kaum beeinträchtigt</li> <li>• Optimieren Sie Ihre Gesamtbetriebskosten, ohne dass zusätzliches Personal oder eine kostspielige Infrastruktur erforderlich sind</li> </ul> |

## PROFITIEREN SIE VON EINEM MODERNEN ANSATZ ZUR BEDROHUNGSABWEHR (THREAT PREVENTION)

Acronis Detection and Response erweitert Ihre Sicherheitsfähigkeiten mit einer „Post-Breach Threat Detection & Response“-Technologie. Sie können damit auch solche Bedrohungen noch identifizieren und stoppen, die andere Abwehrmaßnahmen durchbrochen haben. Außerdem erhält Ihr Cyber Security-Team leistungsfähige Werkzeuge, um Vorfälle ausführlich und forensisch verwertbar zu analysieren.

| AUTOMATISCHER ECHTZEITSCHUTZ   | BEDROHUNGS-AGNOSTISCHER SCHUTZ  | ZERO-TRUST-ANSATZ   | KEINE DATENÜBERFLUTUNG   | GERINGE GESAMT-BETRIEBSKOSTEN  |
|--|---|---|--|--|
| Bedrohungen können automatisch bei Erkennung gestoppt werden – im Gegensatz zu herkömmlichen Lösungen, bei denen die Bedrohungssuche und Schadensbehebungsmaßnahmen noch immer manuell oder zumindest halbmanuell erfolgen muss. | Erkennen und unterbinden Sie fortschrittliche Angriffe (z.B. durch neue bzw. bisher unbekannte Malware, Ransomware, Zero-Day-Exploits oder durch APT-Techniken und dateilose Angriffe), die selbst Antiviren-Programme der nächsten Generation (NGAVs) übersehen. | Steigern Sie die Erkennungsgenauigkeit von Bedrohungen mit einem Zero-Trust-Ansatz, durch die Sie alle Abweichungen von regulären Verhaltensmustern beim Betriebssystem erkennen können. Dieser Ansatz ist besser, als immer wieder neue Angriffstechniken identifizieren zu müssen, die sich ständig weiterentwickeln. | Verschaffen Sie Ihrem Sicherheitsteam fokussierte und detaillierte Einblicke in aktuelle Bedrohungen und Vorfälle, ohne dass Sie manuell nach Bedrohungen suchen und riesige Datenmengen analysieren müssen. | Senken Sie Ihre Gesamtbetriebskosten durch eine automatische Bedrohungssuche und geringen Bandbreitenverbrauch. Nutzt vorhandene Ressourcen und Infrastrukturen. |

## ICSA LABS-ZERTIFIZIERTE LÖSUNG

| <br>ICSA Labs<br>Advanced Threat Defense<br>Certified | TESTDAUER | TESTDURCH-LÄUFE | GETESTETE MALWARE | ERKANNT (PROZENT) | HARMLOSE APPLIKATIONEN | FALSCH-POSITIVE (PROZENT) |
|--|-----------|-----------------|-------------------|-------------------|------------------------|---------------------------|
|  | 33 Tage   | 1162            | 441               | 100%              | 721                    | 0,1%                      |

### FLEXIBLE BEREITSTELLUNGSOPTIONEN

#### On-Premise-Bereitstellung

Nutzen Sie Ihre vorhandene IT-Infrastruktur und stellen Sie die Lösung in Ihrer lokalen Umgebung bereit

#### Cloud-Bereitstellung

Nutzen Sie ein Software-as-a-Service (SaaS)-Bereitstellungsmodell, um die Wartungs- und Betriebskosten zu senken

**WEITERE INFORMATIONEN**

