DELL Technologies

# Mehr Sicherheit ohne zusätzliche Personalkosten

Ein großes County im Südwesten der USA entschied sich für Dell Managed Detection and Response, um seine Cybersicherheit deutlich zu verbessern.

Kundenprofil

**US-County**

Bundesstaatliche und kommunale Verwaltungen | USA

„Uns war klar, dass wir unseren Sicherheitsstatus verbessern mussten. Dell Managed Detection and Response erledigt das jetzt für uns, und das ganze ohne zusätzliche MitarbeiterInnen."

**Director of Information Systems**
Großes County im Südwesten der USA

## Geschäftsanforderungen

Angesichts der rasanten Zunahme von Ransomware und anderen Cyberbedrohungen, die sich gegen bundesstaatliche und kommunale Verwaltungen richten, wollte ein großes, aufstrebendes County im Südwesten der USA seinen Sicherheitsstatus und seine Fähigkeit verbessern, Bedrohungen zu erkennen und darauf zu reagieren. Kosten und Aufwand für die Einstellung und Schulung zusätzlicher SicherheitsexpertInnen sollten vermieden werden.

## Geschäftsergebnisse

- Verbesserter Sicherheitsstatus des Countys ohne Personalaufstockung
- Erweiterung der Kenntnisse, Kompetenzen und Skalierungsfähigkeit des IT-Teams
- Entlastung der MitarbeiterInnen durch Auslagern der 24x7-Bedrohungsüberwachung und -Reaktion
- Optimierte Erkennung und schnelle Korrektur einer Serververletzung
- Profitieren von erfahrenen ExpertInnen, auf die sich das County verlassen kann

## Lösungen auf einen Blick

- Managed Detection and Response

Ein großes, schnell wachsendes County im Südwesten der USA erfüllt Verwaltungsaufgaben für mehrere Hunderttausend EinwohnerInnen. Es ist für seine unterschiedlichen Unternehmen bekannt, die von dynamischen Medizin-, Biotech- und Produktionsfirmen bis hin zu wichtigen landwirtschaftlichen Betrieben reicht.

In den letzten Jahren haben die Cybersicherheitsbedrohungen, die sich gegen bundesstaatliche und kommunale Verwaltungen richten, drastisch zugenommen. In den USA wurden im Jahr 2020 landesweit 79 Ransomwareangriffe auf Regierungseinrichtungen aller Ebenen verübt. Diese Attacken verursachten Ausfallzeiten und Wiederherstellungskosten in Höhe von fast 19 Milliarden US-Dollar.[1]

Nach einer enttäuschenden Erfahrung mit dem Angebot eines anderen Anbieters entschied sich das County im Südwesten der USA für Dell Managed Detection and Response, das auf der Secureworks® Taegis™ XDR-Sicherheitsanalysesoftware basiert. Die Lösung ist ein vollständig verwalteter und umfassender 24x7-Service, der Bedrohungen in der gesamten IT-Umgebung des Countys überwacht, erkennt, untersucht und abwehrt.

„Uns war klar, dass wir unseren Sicherheitsstatus verbessern mussten“, sagt der Director of Information Systems des Countys. Dell Managed Detection and Response erledigt das jetzt für uns, und das ganze ohne zusätzliche MitarbeiterInnen.“

## Kombination von zwei wichtigen Funktionen

Die Lösung vereint die beiden wichtigsten Komponenten eines eindrucksvollen Sicherheitsstatus:

- Das Fachwissen der SicherheitsanalystInnen von Dell Technologies ergänzt das kleine Team des Countys, das aus einem einzigen Sicherheitsanalysten oder einer Sicherheitsanalystin, einem/einer SystemadministratorIn und einem/einer TechnikerIn besteht.

- Die umfassenden Funktionen von Secureworks Taegis XDR – einer cloudnativen Sicherheitsanalyseplattform, die dafür konzipiert wurde, Advanced Threats aufzuspüren – versetzen die MDR-AnalystInnen in die Lage, die Ermittlungen zu optimieren und mit dem County zusammenzuarbeiten, Letztendlich helfen sie dabei, die richtigen Maßnahmen zu ergreifen, um die Auswirkungen zu minimieren.

„Als wir die Hilfe der SpezialistInnen von Dell Technologies benötigten, waren sie quasi umgehend zur Stelle und blieben für eine Woche oder zehn Tage, und wir wussten, dass wir in guten Händen waren.

**Director of Information Systems**
Großes County im Südwesten der USA

[1] Bischoff, Paul, „Ransomware attacks on US government organizations cost $18.9bn in 2020“, Comparitech, 17. März 2021. https://www.comparitech.com/blog/information-security/government-ransomware-attacks/

„Sie haben uns bei der Installation von Software-Agents mit speziellen Auslösern zum Stoppen von Diensten oder zum Herunterfahren von Rechnern oder Schließen von Konten auf allen Servern und Workstations geholfen und benachrichtigen uns, wenn eine Bedrohung entdeckt wird“, erläutert der Director of Information Systems des Countys. „Die SpezialistInnen von Dell Technologies haben uns wertvolle Ratschläge gegeben und die in den 90 Tagen der Implementierung zu ergreifenden Maßnahmen priorisiert.“

## Schnelle Eindämmung eines Angriffsversuchs

Die Lösung umfasst außerdem bis zu 40 Stunden pro Quartal an klar formulierten Anleitungen zur Reaktion auf Bedrohungen und deren Abwehr selbst in den komplexesten Situationen sowie weitere 40 Stunden pro Jahr zur Untersuchung von Aktivitäten und zur Einleitung der Wiederherstellung nach schweren Sicherheitsvorfällen, falls erforderlich.

„Was uns wirklich von der Lösung überzeugt hat, war der Versuch eines tatsächlichen Angriffs“, erinnert sich der Director of Information Systems des Countys. „Eine Hackergruppe hat einen Exploit auf dem Microsoft Exchange-E-Mail-Server entdeckt. Nachdem wir von Microsoft und der Cybersicherheitsbehörde unseres Bundesstaates benachrichtigt worden waren, stellten wir fest, dass einer unserer drei Server kompromittiert worden war. Das Team von Dell Technologies hat die Sicherheitsverletzung sehr gründlich untersucht und uns bei der Wiederherstellung unseres Servers geholfen.“

Er fährt fort: „Ich kann allen County-CIOs nur empfehlen, sich für eine Sicherheitslösung der Enterprise-Klasse wie Dell Managed Detection and Response zu entscheiden, und nicht für die Lösung eines Anbieters von Virenschutzsoftware. Als wir die Hilfe der SpezialistInnen von Dell Technologies benötigten, waren sie quasi umgehend zur Stelle und blieben für eine Woche oder zehn Tage, und wir wussten, dass wir in guten Händen waren. Zusammen arbeiteten wir an einer intelligenten Lösung und zwischen unseren Teams gab es jede Menge Synergien.“



**Weitere Informationen** zu Dell Managed Detection and Response finden Sie hier.

**Wenden Sie sich an** ExpertInnen von Dell Technologies Lösungen.

DELL Technologies

**Auf Social Media** folgen