VECTRA
SECURITY THAT THINKS

# 5 Punkte zur erfolgreichen Threat Detection Strategie

Warum, wann und wie investiere ich in die eigene Angriffserkennung?

25 Oktober 2022

# Über mich


**David Lin**

RSM, Vectra AI

dlin@vectra.ai

# Agenda

- “Das Problem”
- “Das Ideal”
- Was GARTNER sagt
- Die 5 Punkte für erfolgreiche Threat Detection

# Das Problem

> Wir wissen nicht, ob wir im Augenblick kompromittiert sind.

*72 % der Sicherheitsverantwortlichen glauben, dass sie möglicherweise betroffen sind, wissen es aber nicht*

Knowledge Forum A

> Wir wissen nicht, wie wir mit modernen Angriffen Schritt halten sollen.

*83 % der Sicherheitsverantwortlichen sind der Meinung, dass traditionelle Ansätze für moderne Bedrohungen nicht funktionieren.*

> Wir wissen nicht, wie wir die Bedrohungen priorisieren sollen, die am wichtigsten sind.

*79 % der Sicherheitsverantwortlichen geben an, dass die Tools der Anbieter ihr Versprechen nicht einhalten*

**Das Unbekannte.**

Source: Vectra Research Study | Global : Fit for Purpose or Behind the Curve? - January 2022 - Based on interviews of 1800 IT security decision makers working at organizations with more than 1,000 employees across France, Italy, Spain, Germany, Sweden, Saudi Arabia and the US, and more than 500 employees across the Netherlands and Australia & New Zealand.

# Die einzige Konstante in der Sicherheit ist "mehr"

**Mehr** Angriffsfläche abzudecken

Weitere Tools & Datensätze

Mehr Komplexität

**weniger effizient**

**Mehr** gerissene Angreifer zu erkennen

Mehr Anomalien & Regeln

Mehr Lärm

**weniger effektiv**

**Mehr** Verteidiger, um Schritt zu halten

Mehr manuelle Aufgaben

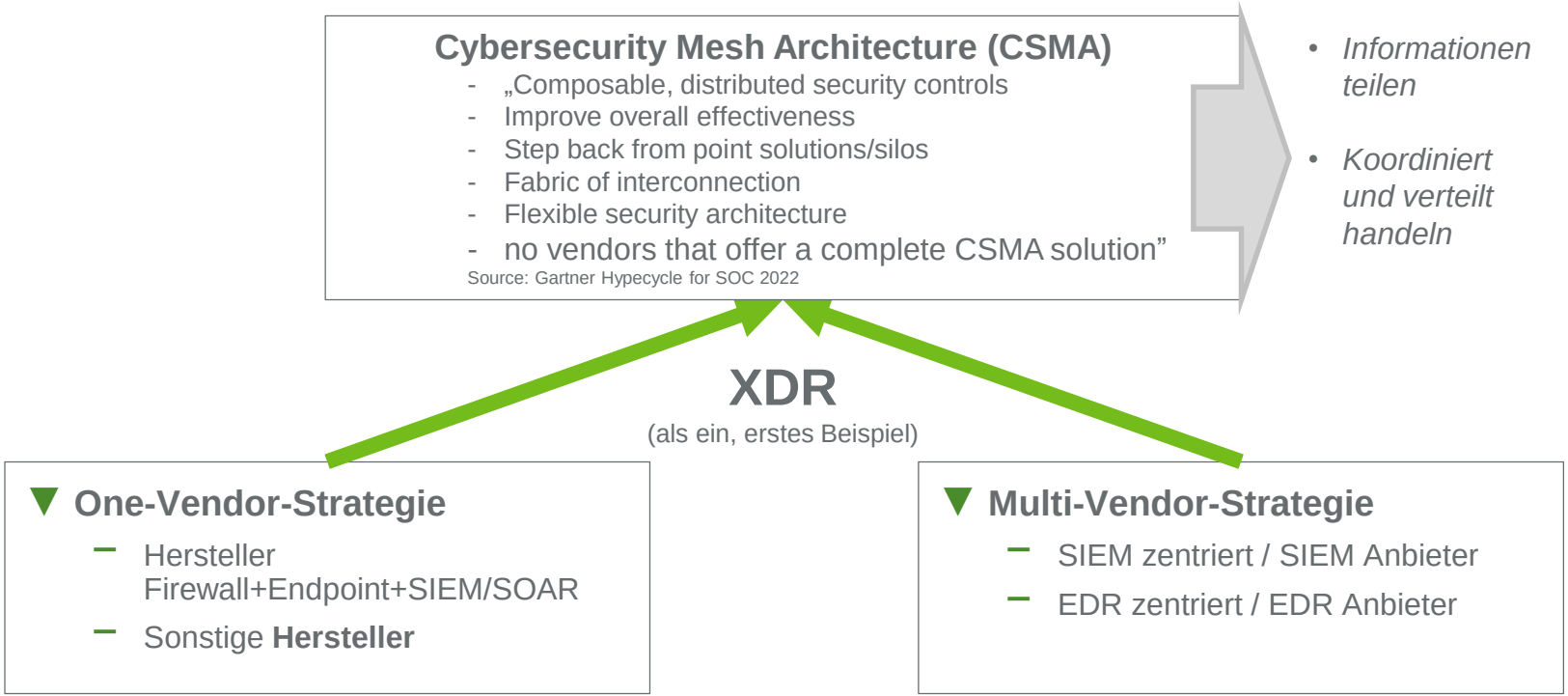
Mehr Burnout

**weniger belastbar**

**Die Antwort auf "mehr" ist NICHT mehr.**

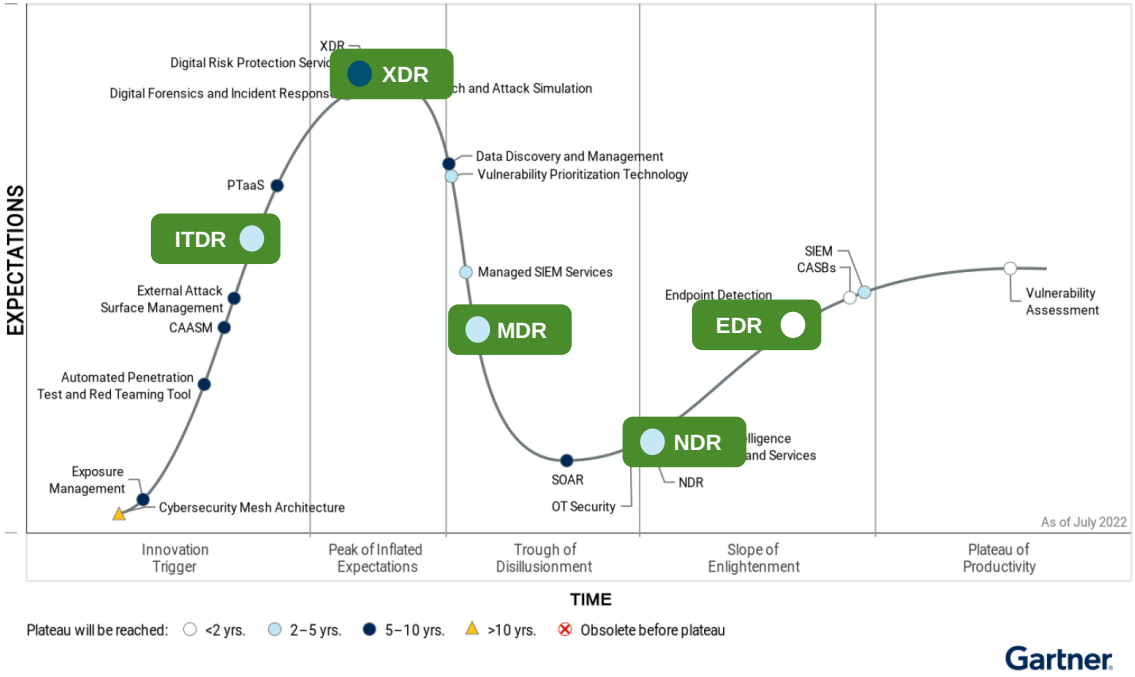
# Was wäre ideal?

Oder: Das Buzz-Word XDR



# Marktreife der xDR Technologien

Der Weg zu einem besseren TDR weist auf NDR, CDR, ITDR, MDR... XDR




## TDR Landscape

- Network Threat Detection & Response (**NDR + CDR**)
- Identity Threat Detection & Response (**ITDR**)
- Endpoint Threat Detection & Response (**EDR**)
- Managed Threat Detection & Response (**MDR**)
- Extended Threat Detection & Response (**XDR**)

Source: Gartner Hype Cycle for Security Operations, 2022 Published 5 July 2022 - ID G00770249

# Der Weg zu besserer Angriffserkennung

5 Punkte zur Realisierung von Mehrwerten

- #1 Coverage
- #2 Clarity
- #3 Control
- #4 Complexity
- #5 Competency

## Kriterien jedes Schlüssels

- **Schmerz**: Welche Schmerzen verursacht das Problem?
- **Pfad**: Welche Wege adressieren den Schmerz?
- **Kosten/Nutzen:** Was kommt unter dem Strich dabei heraus?

Da es im Deutschen keine vergleichbar schöne Alliteration gibt, haben wir es nicht übersetzt. ☺

# Technische Anforderungen

Security Operations-Teams verdienen eine bessere Threat Detection & Response (TDR)

Sicherheit braucht **höhere Abdeckung**

Coverage

Über Public Cloud, SaaS, Identität, Netzwerk, Endpunkt

Sicherheit braucht **klares Signal**

Clarity

Um wichtige Warnungen zu erkennen, zu selektieren und zu priorisieren

Sicherheit braucht **bessere Kontrolle**

Control

Um Angriffe schnell zu untersuchen und darauf zu reagieren

**Die Antwort auf "mehr" ist: besser.**

VECTRA SECURITY THAT THINKS.®

# #1: Coverage

## Problem: das Unbekannte

**Problem**: das Unbekannte

*"Wir wissen nicht, wo wir gerade kompromittiert sind."*

72 % der Sicherheitsverantwortlichen glauben, dass sie möglicherweise verletzt wurden, wissen es aber nicht

- **Schmerz:** *"Eine immer vielfältigere Reihe von Risiken und Risiken, über die Unternehmen einen besseren Überblick haben müssen."*
- **Pfad**:

| 2 to 5 years | 5 to 10 years |
|---|---|
| **Hoher kurzfristiger Nutzen für die Sicherheit** | **Hoher kurzfristiger Nutzen für die Sicherheit** |
| • **Identity Threat Detection and Response (ITDR)**<br>• **Digital Risk Protection Services (DRPS)**<br>• **Network Detection and Response (NDR + CDR)**<br>• Threat Intelligence Products and Services | • **Exposure Management**<br>• **Extended Detection and Response (XDR)**<br>• Automated Penetration Test & Red Teaming<br>• Cyber Asset Attack Surface Management (CAASM)<br>• External Attack Surface Management (EASM)<br>• Data Discovery and Management (DDAM) |

- **Nutzen**: **Einheitliche Angriffstransparenz in ITDR, NDR + CDR beantwortet: "Wie sieht meine Organisation aus der Sicht eines Angreifers aus?"**
  - *"Überwacht Angreifertechniken, um Identitäts- und Zugriffskontrollen zu schützen, zu erkennen, wenn Angriffe auftreten, und eine schnelle Behebung zu ermöglichen."*

Source: Vectra Research Study | Global : Fit for Purpose or Behind the Curve? - December 2021 – based on interviews of 1800 IT security decision makers working at organizations with more than 1,000 employees across France, Italy, Spain, Germany, Sweden, Saudi Arabia and the US, and more than 500 employees across the Netherlands and Australia & New Zealand.

Source: Gartner Hype Cycle for Security Operations, 2022 Published 5 July 2022 - ID G00770249

# #2: Clarity

## Problem: das Unbekannte

**Problem**: das Unbekannte

*"Wir wissen nicht, wo wir gerade kompromittiert sind."*

72 % der Sicherheitsverantwortlichen glauben, dass sie möglicherweise verletzt wurden, wissen es aber nicht

- **Schmerz:** *"Priorisierung von erkannten Problemen, um sicherzustellen, dass Ihr Security Operations-Programm auf Ihre Angriffsfläche abgestimmt ist."*
- **Pfad**:

| 2 to 5 years | 5 to 10 years |
|---|---|
| **Hoher kurzfristiger Nutzen für die Sicherheit** | **Hoher kurzfristiger Nutzen für die Sicherheit** |
| • **Identity Threat Detection and Response (ITDR)**<br>• **Digital Risk Protection Services (DRPS)**<br>• **Beach and Attack Simulation (BAS)**<br>• **Vulnerability Prioritization Technology (VPT)**<br>• **Network Detection and Response (NDR + CDR)**<br>• Threat Intelligence Products and Services<br>• Security Incident and Event Management (SIEM)<br>• Managed SIEM Services | • **Extended Detection and Response (XDR)**<br>• Data Discovery and Management (DDAM)<br>• Penetration Testing as a Service (PTaaS) |

- **Nutzen**: **Einheitlicher Angriffskontext** in ITDR, NDR + CDR beantwortet: "Wie sollte meine Organisation die Probleme finden und priorisieren, die Angreifer zuerst sehen werden?"
- *Verringern Sie das Alarmrauschen, erhöhen Sie die Wiedergabetreue der Warnungen, reduzieren Sie die Optimierung von Analysten, die Triage und das Burnout – verkürzen Sie die Zeit für die Erkennung, Untersuchung und Reaktion*

Source: Vectra Research Study | Global : Fit for Purpose or Behind the Curve? - December 2021 – based on interviews of 1800 IT security decision makers working at organizations with more than 1,000 employees across France, Italy, Spain, Germany, Sweden, Saudi Arabia and the US, and more than 500 employees across the Netherlands and Australia & New Zealand.

Source: Gartner Hype Cycle for Security Operations, 2022 Published 5 July 2022 - ID G00770249

VECTRA SECURITY THAT THINKS.®

# #3: Control

## Problem: das Unbekannte

**Problem**: das Unbekannte

*"Wir wissen nicht, wo wir gerade kompromittiert sind."*

72 % der Sicherheitsverantwortlichen glauben, dass sie möglicherweise verletzt wurden, wissen es aber nicht

- **Schmerz:** *"SRM-Führungskräfte haben Schwierigkeiten, Maßnahmen zur Risikominderung zu priorisieren, und hinterlassen Lücken, in denen sie das Gefühl haben, weniger Kontrolle zu haben"*
- **Pfad**:

| 2 to 5 years | 5 to 10 years |
|---|---|
| **High near-term benefit for security (Bold)** | **High near-term benefit for security (Bold)** |
| • **Identity Threat Detection and Response (ITDR)**<br>• **Digital Forensics and Incident Response**<br>• **Digital Risk Protection Services (DRPS)**<br>• **Network Detection and Response (NDR)**<br>• Security Incident and Event Management (SIEM)<br>• Managed SIEM Services | • **Extended Detection and Response (XDR)**<br>• **Security Orchestration and Automation (SOAR)**<br>• Cyber Physical Systems Security (CPS)<br>• Data Discovery and Management (DDAM) |

- **Nutzen: Einheitliche Angriffskontrolle** über ITDR hinweg ermöglicht NDR + CDR der Sicherheit die Antwort:
- "Was würde passieren, wenn ein Angreifer eine Kampagne gegen die Infrastruktur meines Unternehmens durchführen würde, wie würde seine Verteidigung zurechtkommen und wie würden Prozesse funktionieren" – welche Personen, Prozesse und Technologien zu verwalten, zu automatisieren und zu integrieren sind.

Source: Vectra Research Study | Global : Fit for Purpose or Behind the Curve? - December 2021 – based on interviews of 1800 IT security decision makers working at organizations with more than 1,000 employees across France, Italy, Spain, Germany, Sweden, Saudi Arabia and the US, and more than 500 employees across the Netherlands and Australia & New Zealand.

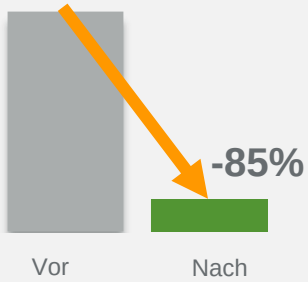
Source: Gartner Hype Cycle for Security Operations, 2022 Published 5 July 2022 - ID G00770249

# Wie eine bessere Angriffserkennung aussieht:

## Die Ergebnisse einer besseren Abdeckung, Klarheit, Kontrolle

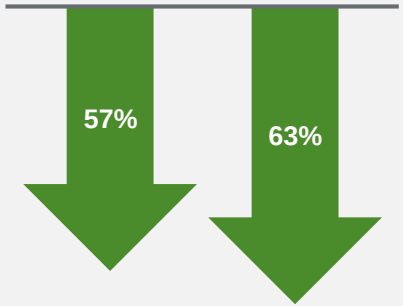

### Coverage

Gehen Sie über Signaturen und einfache Anomalien hinaus, um fast das 3-fache der Bedrohungen zu erkennen




### Clarity

85 % effizienter bei der Identifizierung realer Bedrohungen mit >2x höherer Analystenproduktivität




### Control

57 % weniger schwerwiegende Verstöße und 63 % geringeres Risiko einer größeren Geschäftsunterbrechung

Source: The Business Value of Cognito Network Detection and Response from Vectra, December 2020, Doc. #US47016020

# #4: Complexity

## Problem: das Unbekannte

**Problem**: das Unbekannte

*"Wir wissen nicht, wo wir gerade kompromittiert sind."*

72 % der Sicherheitsverantwortlichen glauben, dass sie möglicherweise verletzt wurden, wissen es aber nicht

- **Schmerz:** *"Effizienter und effektiver Einsatz von Sicherheitsbudgetierung und Ressourcen."*
- **Pfad**: Konzentrieren Sie sich auf kurzfristige Nutzenpfade, die Abdeckung, Klarheit und Kontrolle bieten

| 2 to 5 years | | | |
|---|---|---|---|
| **High near-term benefit for security** | **Coverage** | **Clarity** | **Control** |
| • Identity Threat Detection and Response (ITDR) | ✓ | ✓ | ✓ |
| • Digital Forensics and Incident Response | ✗ | ✓ | ✓ |
| • Digital Risk Protection Services (DRPS) | ✗ | ✗ | ✓ |
| • Breach and Attack Simulation (BAS) | ✗ | ✓ | ✗ |
| • Vulnerability Prioritization Technology (VPT) | ✗ | ✓ | ✗ |
| • Network Detection and Response (NDR + CDR) | ✓ | ✓ | ✓ |
| • Threat Intelligence Products and Services | ✗ | ✓ | ✗ |

- **Nutzen**: **Einheitliche TDR-Plattform** - Die Konsolidierung von ITDR, NDR + CDR mit vorhandenem EDR in einer Plattform beschleunigt die Bereitstellung, Implementierung und das Bedrohungsmanagement und liefert innerhalb von Wochen, nicht Monaten oder Jahren einen Mehrwert.

Source: Vectra Research Study | Global : Fit for Purpose or Behind the Curve? - December 2021 – based on interviews of 1800 IT security decision makers working at organizations with more than 1,000 employees across France, Italy, Spain, Germany, Sweden, Saudi Arabia and the US, and more than 500 employees across the Netherlands and Australia & New Zealand.

Source: Gartner Hype Cycle for Security Operations, 2022 Published 5 July 2022 - ID G00770249

# #5: Competency

## Problem: das Unbekannte

**Problem**: das Unbekannte

*"Wir wissen nicht, wo wir gerade kompromittiert sind."*

72 % der Sicherheitsverantwortlichen glauben, dass sie möglicherweise verletzt wurden, wissen es aber nicht

- **Schmerz:** *"Wie sich ein Angriff manifestieren kann, erfordert bestimmte Fähigkeiten, und Mitarbeiter mit den erforderlichen Fähigkeiten sind schwer zu rekrutieren und umzuschulen."*
  - *"Den meisten Unternehmen fehlen die Ressourcen, das Budget oder der Appetit, um ihre eigene 24/7 SOC-Funktion aufzubauen und zu betreiben"*
  - *"Die Anzahl der Mitarbeiter und Fähigkeiten, die erforderlich sind, um ein erstklassiges Portfolio unterschiedlicher Sicherheitstools zu integrieren und zu pflegen, ist hoch - anhaltende Komplexität, Personalausstattung und Kosten für die Unterstützung von SIEM-Bereitstellungen."*
- **Pfad**:

| 2 to 5 years | 5 to 10 years |
|---|---|
| **Hoher kurzfristiger Nutzen für die Sicherheit** | **Hoher kurzfristiger Nutzen für die Sicherheit** |
| • **Managed Detection and Response (MDR)**<br>• Threat Intelligence Products and Services<br>• Managed SIEM Services | • Automated Penetration Test & Red Teaming<br>• Penetration Testing as a Service (PTaaS) |

- **Nutzen**: **Skills und 24x7x365 Verstärkungen** – Aufbau und/oder Erweiterung des Know-hows zur Erkennung und Reaktion auf Bedrohungen im gesamten Team in den Bereichen Reaktion auf Vorfälle, Bedrohungssuche, Bedrohungsanalyse und Red Teaming.

Source: Vectra Research Study | Global : Fit for Purpose or Behind the Curve? - December 2021 – based on interviews of 1800 IT security decision makers working at organizations with more than 1,000 employees across France, Italy, Spain, Germany, Sweden, Saudi Arabia and the US, and more than 500 employees across the Netherlands and Australia & New Zealand.

Source: Gartner Hype Cycle for Security Operations, 2022 Published 5 July 2022 - ID G00770249

# Technologische Quickwins

## Problem: das Unbekannte

**Problem**: das Unbekannte

*"Wir wissen nicht, wo wir gerade kompromittiert sind."*

- **Schmerz:** *"effektive und messbare positive Auswirkungen auf das Risikoprofil des Unternehmens."*
  - 72 % der Sicherheitsverantwortlichen glauben, dass sie möglicherweise verletzt wurden, wissen es aber nicht
  - 79 % der Sicherheitsverantwortlichen geben an, dass die Tools der Anbieter ihr Versprechen nicht einhalten
  - 83 % der Sicherheitsverantwortlichen sind der Meinung, dass traditionelle Ansätze für moderne Bedrohungen nicht funktionieren.

- **Pfad**:

| 2 to 5 years | | | |
|---|---|---|---|
| **Hoher kurzfristiger Nutzen für die Sicherheit** | **Coverage** | **Clarity** | **Control** |
| • **Identity Threat Detection and Response (ITDR)** | ✓ | ✓ | ✓ |
| • **Network Detection and Response (NDR + CDR)** | ✓ | ✓ | ✓ |
| • **Managed Detection and Response (MDR)** | ✓ | ✓ | ✓ |

- **Nutzen:**
  - Vertrauen, dass das Unternehmen über die gesamte Angriffsfläche hinweg abgedeckt ist
  - Vertrauen Sie darauf, dass Sicherheitsteams ein genaues Bedrohungssignal erhalten, was am wichtigsten ist
  - Vertrauen Sie darauf, dass Sicherheitsteams die Kontrolle übernehmen, um voranzukommen und Angreifern einen Schritt voraus zu sein

# Summary

5 Punkte zu Ihrer Threat Detection & Response Strategie –
auch bekannt als Angriffserkennung (Threat Detection and Response)

| | |
|---|---|
| #1 Coverage | **Der Angreifer sieht eine miteinander verbundene Angriffsfläche – wir sollten wie ein Angreifer denken.** Nutzen Sie eine TDR Plattform, die Transparenz über Identität, Cloud, SaaS, Netzwerk und Endpunkt vereinheitlicht |
| #2 Clarity | **Angreifer sind flexibel und werden immer Löcher in Ihrer Angriffsfläche finden.** Eine TDR-Plattform sollte den einheitlichen Kontext von Angreifern sehen, um die Bedrohungen zu priorisieren, die am wichtigsten sind. |
| #3 Control | **Mehr Angriffsfläche + mehr Ausweichmethoden = Angreifer haben die Oberhand.** Eine TDR-Plattform gibt ihnen die Kontrolle, indem sie Prozesse und Workflows integriert und automatisiert. |
| #4 Complexity | **Mehr Angriffsfläche + mehr ausweichende Angreifer müssen NICHT mehr Komplexität bedeuten.** Eine einheitliche TDR-Plattform reduziert die Komplexität, um innerhalb weniger Wochen einen Mehrwert zu schaffen |
| #5 Competency | **Angriffe entwickeln sich ständig weiter - es ist nie einfach, Schritt zu halten.** Eine TDR-Plattform mit MDR-Services liefert SOC-Fähigkeiten und baut -Know-how auf und ermöglicht 24x7x365-Überwachung. |
| Confidence | **Eine bessere Bedrohungsabwehr sollte KEINE ständige Pflege erfordern** – Eine einheitliche TDR-Plattform hat sofort effektive und messbare positive Auswirkungen auf das Risikoprofil des Unternehmens |