

Symantec DLP

Der neue Cybersecurity-Imperative: Kennen Sie Ihre Daten, kontrollieren Sie Ihre Risiken.



Lukas Zettl

Regional Sales Manager

So einfach passiert ein Data Leak



Symantec™
A Division of Broadcom

Product Brief

Symantec™ Email Threat Detection and Response

Stop targeted and advanced email attacks with powerful protection that includes complete visibility, prioritized response, and automated remediation.

Prevent the Most Advanced Email Attacks

Symantec™ Email Threat Detection and Response (ETDR) is a cloud-based service that uncovers and prioritizes advanced attacks, warning your organization through email by adding advanced detection techniques such as cloud-based sandboxing and ClickTime URL Protection to the Symantec Email Security cloud service. In addition, it helps accelerate your response to targeted and advanced threats with advanced email security analytics that provide the deepest visibility into targeted and advanced attack campaigns. This intelligence includes insights into both clean and malicious emails as well as more indicators of Compromised (IDCs) than any other vendor, with more than 60 data points such as URLs, file hashes, and targeted attack information.

You can export this data to your Security Operations Center (SOC) to quickly determine the severity and scope of any targeted or advanced attack. Furthermore, you can quickly remediate email attacks by automatically quarantining or blocking entire harmful threats. However, ETDR reduces the risk of phishing by preparing your users to recognize the latest phishing attacks with built-in security awareness training. Finally, when used alongside Symantec Endpoint Detection and Response and the Symantec Secure Web Gateway family to detect advanced threats, you can automatically correlate events across all control points.

Cloud-Based Sandboxing

ETDR customers can leverage cloud-based sandboxing capabilities to discover and prioritize today's most complex targeted and advanced attacks. This service uses advanced machine learning, network traffic analysis, and behavior analysis to detect even the most stealthy and persistent threats. In addition, it's critical email security visibility from the Symantec Global Intelligence Network, the world's largest clean threat intelligence network. The Symantec Global Intelligence Network provides comprehensive visibility into the threat landscape and delivers better security outcomes by correlating and analyzing security insights from more than 175 million endpoints, 80 million web proxy users, and 8 billion daily security requests across 121 countries. Our cloud-based sandboxing also provides you the details of malicious files and their execution actions, so that all relevant attack components can be quickly investigated and remediated. Today, many advanced attacks are virtual machine-aware, which means they don't reveal suspicious behavior when run in typical sandboxing systems. To combat this, we employ techniques to mimic human behavior and execute suspicious files both virtually and on physical hardware to uncover attacks that evade detection by traditional sandboxing technologies.

New chat

Previous 7 Days

New chat

Managing Screen Time.

Examples

Capabilities

Limitations

“Explain quantum computing in simple terms” →

Remembers what user said earlier in the conversation

May occasionally generate incorrect information

“Got any creative ideas for a 10 year old’s birthday?” →

Allows user to provide follow-up corrections

May occasionally produce harmful instructions or biased content

“How do I make an HTTP request in Javascript?” →

Trained to decline inappropriate requests

Limited knowledge of world and events after 2021

Send a message.

Free Research Preview: ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT May 3 Version](#)

Upgrade to Plus

OpenAI

OpenAI

New chat

ChatGPT Language Model

International Tensions Over S

Most Significant Change (MSC

Rick Davies Unknown Consulti

NAM coalition vs Western nati

Clear conversations

Dark mode

OpenAI Discord

Updates & FAQ

Log out

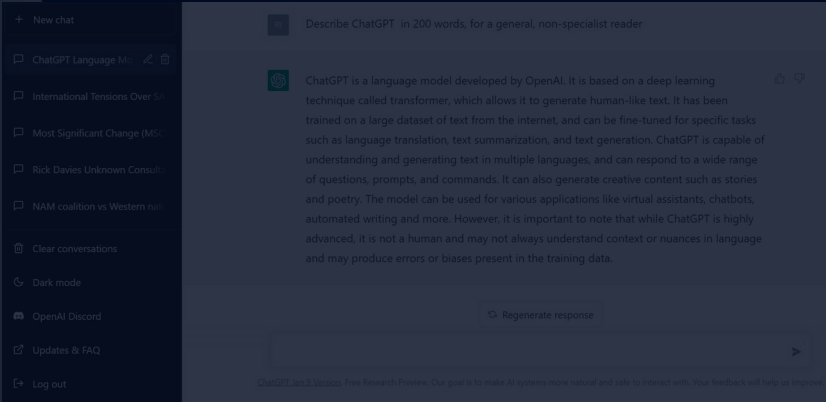
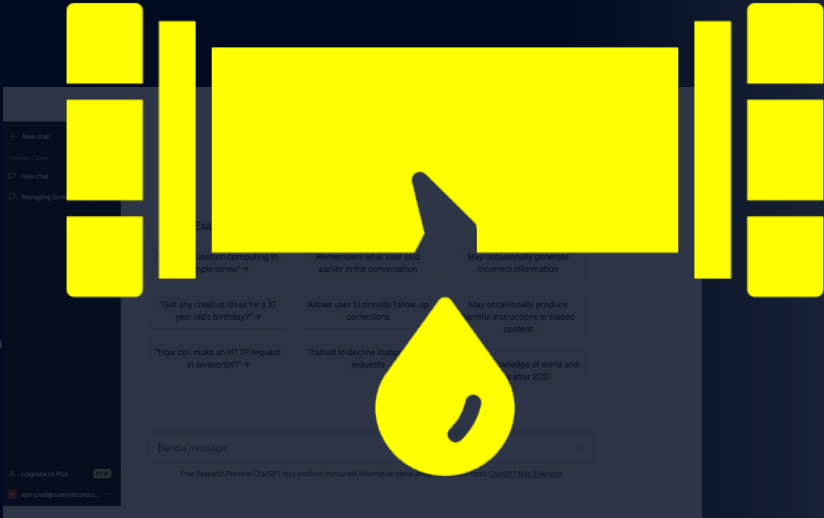
Describe ChatGPT in 200 words, for a general, non-specialist reader

ChatGPT is a language model developed by OpenAI. It is based on a deep learning technique called transformer, which allows it to generate human-like text. It has been trained on a large dataset of text from the internet, and can be fine-tuned for specific tasks such as language translation, text summarization, and text generation. ChatGPT is capable of understanding and generating text in multiple languages, and can respond to a wide range of questions, prompts, and commands. It can also generate creative content such as stories and poetry. The model can be used for various applications like virtual assistants, chatbots, automated writing and more. However, it is important to note that while ChatGPT is highly advanced, it is not a human and may not always understand context or nuances in language and may produce errors or biases present in the training data.

Regenerate response

ChatGPT Jan 3 Version, Free Research Preview. Our goal is to make AI systems more natural and safe to interact with. Your feedback will help us improve.

So einfach passiert ein Data Leak



Cybersecurity-Druck in Unternehmen



Third-Party Risk

- Unternehmen arbeiten zunehmend mit **externen Dienstleistern, Lieferanten und Partnern** zusammen.
- Partner haben **Zugriff auf kritische Systeme oder sensible Daten** (z. B. Kundentransaktionen, Authentifizierungsinformationen).
- **Fehlende Transparenz** über Zugriffe, Datenbewegungen und Sicherheitsvorfälle.
- Cloud-Provider erhöhen die Flexibilität, führen aber zu **Kontrollverlust über die physische Datenhoheit**.



Datenfragmentierung

- Daten liegen heute über zahlreiche Systeme verstreut: **On-Premises, Cloud, mobile Geräte, SaaS-Anwendungen**
- Unterschiedliche Speicherorte = **fehlende Übersicht und Kontrolle**
- **Erhöht das Risiko** von Datenverlust und Fehlklassifizierungen
- **Erschwert einheitliche Sicherheitsrichtlinien** und Compliance-Prüfungen
- **Besonders kritisch:** Schattenkopien, lokale Speicher und private Cloud-Dienste



Compliance- Druck

- Strengere Anforderungen durch **DSGVO, NIS2, ISO 27001, PCI-DSS** u.a.
- **NIS2-Richtlinie** verpflichtet Unternehmen zur systematischen Kontrolle und Absicherung ihrer Lieferketten (Third Party Risk Management).
- **Nachweispflicht:** Unternehmen müssen zeigen, *wie* Daten geschützt werden
- Fehlen konsistenter Schutzmechanismen **erschwert Audit-Readiness**



Schatten-IT

- Mitarbeitende nutzen Cloud-Dienste (z. B. Google Drive, Dropbox, WeTransfer), **ohne Freigabe der IT**.
- Unternehmensdaten landen in **unkontrollierten Umgebungen**.
- Fehlende Verschlüsselung oder **unzureichende Zugriffsbeschränkungen**.
- **Hohe Dynamik** – täglich entstehen neue SaaS-Dienste, oft unbemerkt.

Was bedeutet NIS2 für Unternehmen?

In Österreich sollen mit dem NISG 2026 rund **4.000 Unternehmen** und Einrichtungen ab mittlerer Größe aus **18 Sektoren** erfasst werden.

Fakten Check Österreich

- NIS2 ist auf EU-Ebene am **16. Jänner 2023** in Kraft getreten.
- Die EU-Mitgliedstaaten mussten NIS2 bis **17. Oktober 2024** in nationales Recht umsetzen.
- In Österreich erfolgt die Umsetzung über das **NISG 2026**.
- Laut WKO sollen **ab 1. Oktober 2026** für rund **4.000 Unternehmen und Einrichtungen ab mittlerer Größe** aus **18 gesellschaftlich relevanten Sektoren verpflichtende Sicherheitsmaßnahmen und Meldepflichten** gelten.

Key sectors

Energy
Mobility
Banking
Financial markets infra
Healthcare
Drinking water
Waste water
Digital infrastructure
ICT
Government
Space

Important sectors

Postal & courier services
Waste management
Chemical industry
Food
Manufacturing
Digital service provider
Research

Was Kunden bald gefragt werden

Neue Fragen in Ausschreibungen & Verträgen:

- Können Sie Sicherheitsvorfälle zeitnah erkennen und melden?
- Können Sie nachweisen, welche Daten betroffen sind?
- Haben Sie Prozesse für Incident Response und Business Continuity?
- Wie schützen Sie sensible Kundendaten?
- Welche Security-Kontrollen gelten für Ihre Subunternehmer?

NIS-2 Kontrolllandkarte: Wo DLP einzahl



Risikoanalyse & Security Policies

NIS2-Frage:

Welche kritischen Informationswerte müssen geschützt werden?

DLP-Beitrag:

- Identifikation sensibler Datenbestände
- Klassifikation von Daten nach Risiko
- Transparenz über Speicherorte und Datenflüsse
- Policy-Basis für Schutzmaßnahmen



Meldefähigkeit & Nachweisbarkeit

NIS2-Frage:

Können wir schnell belegen, ob sensible Daten betroffen sind?

DLP-Beitrag:

- Nachvollziehbarkeit von Datenabflüssen
- Dokumentation von Policy-Verstößen
- Unterstützung bei 24h-/72h-Bewertungen
- Faktenbasis für interne und externe Meldungen



Zugriffskontrolle & Asset Management

NIS2-Frage:

Wer darf auf kritische Informationen zugreifen und was passiert danach?

DLP-Beitrag:

- Sichtbarkeit über Datenzugriffe und Datennutzung
- Schutz bei Kopieren, Upload, E-Mail, Web und Endpoint
- Kontrolle riskanter Kanäle wie USB, private Cloud oder private E-Mail
- Ergänzung zu IAM, MFA und Endpoint Security



Incident Handling

NIS2-Frage:

Können Sicherheitsvorfälle erkannt, bewertet und eskaliert werden?

DLP-Beitrag:

- Erkennung ungewöhnlicher Datenbewegungen
- Kontext zu Benutzer, Datei, Kanal und Empfänger
- Priorisierung nach Kritikalität der betroffenen Daten
- Incident Evidence für Security- und Compliance-Teams



Lieferkettensicherheit

NIS2-Frage:

Wie kontrollieren wir Datenrisiken bei Partnern, Dienstleistern und Subunternehmern?

DLP-Beitrag:

- Kontrolle externer Datenweitergabe
- Monitoring von Datenbewegungen zu Dritten
- Policies für Partnerkommunikation
- Nachweise für Kunden, Audits und Vertragsanforderungen



Wirksamkeitsprüfung

NIS2-Frage:

Funktionieren unsere Sicherheitsmaßnahmen nachweisbar?

DLP-Beitrag:

- Policy-Verletzungen als messbare Kontrollindikatoren
- Reports zu Vorfällen, Trends und Risikobereichen
- Nachweis von Prävention, Blockierung oder User Coaching
- Grundlage für kontinuierliche Verbesserung

Data-Centric Cybersecurity

"Weg von der Infrastruktur – hin zum
eigentlichen Wert: den **Daten** selbst"

3 Grundprinzipien der Data-Centric Security



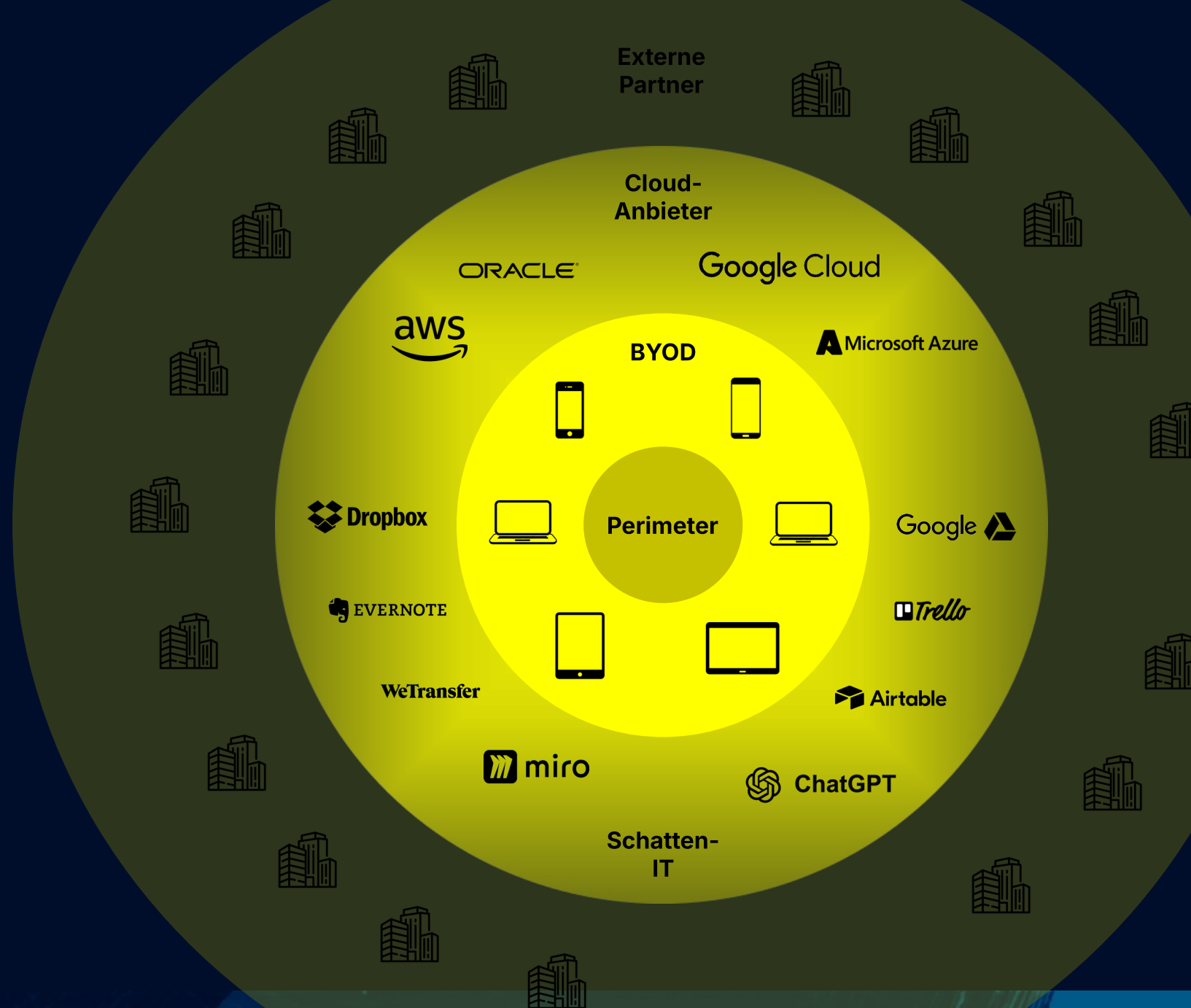
Sichtbarkeit



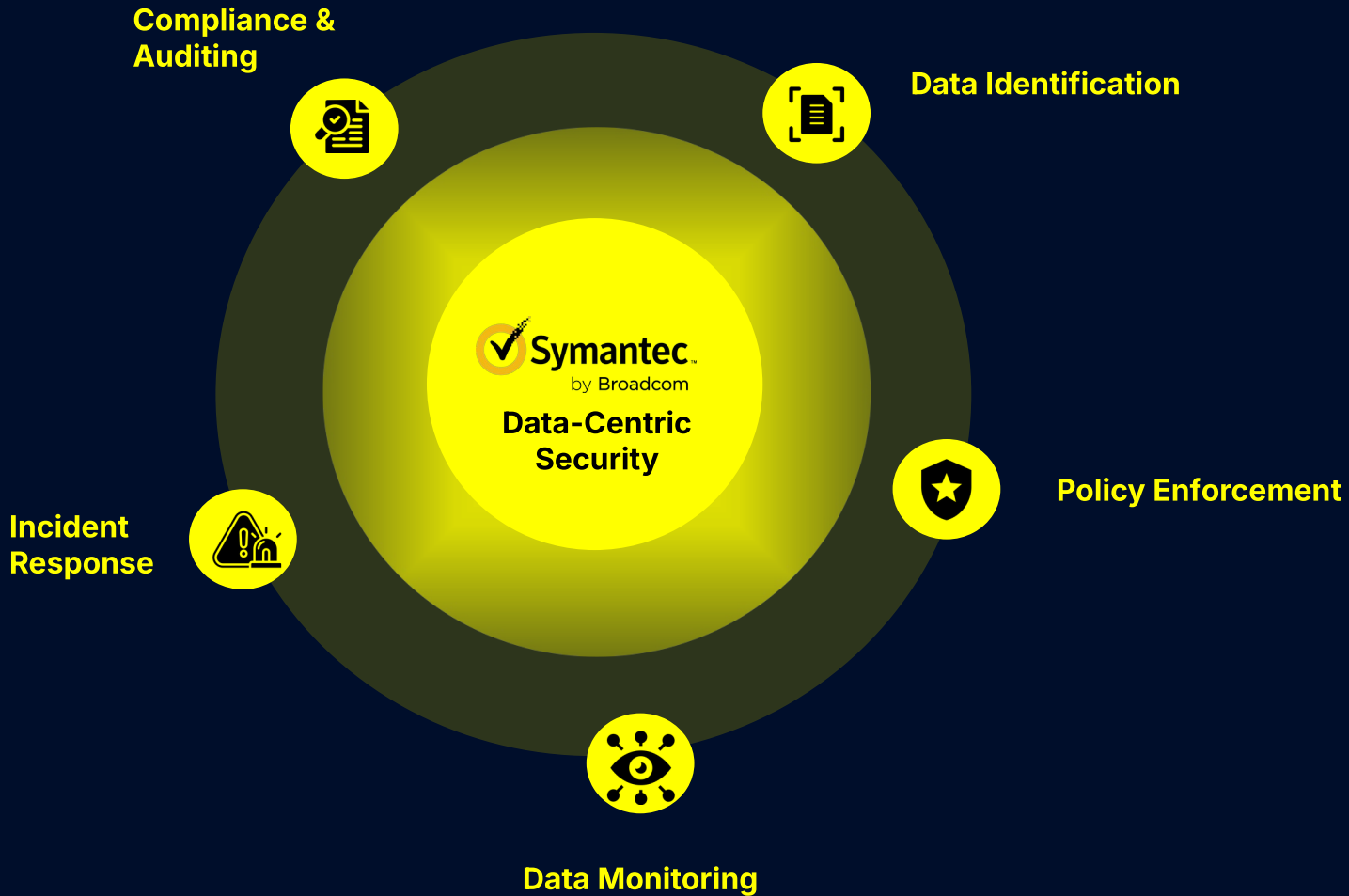
Klassifizierung



Kontrolle



Symantec Data-Centric Security Approach



Phase 1: Entdecken & Verstehen

- Automatisierte Scans von Endpoints, File-Shares, Datenbanken und Cloud-Speichern
- Identifikation vertraulicher Daten (personenbezogen, geistiges Eigentum, Finanzdaten etc.)
- Klassifizierung nach Sensitivität und Geschäftswert

Phase 2: Überwachen & Analysieren

- Monitoring aller Datenbewegungen – Endpoint, Netzwerk, Cloud, E-Mail
- Analyse von Benutzerverhalten und Nutzungsmustern
- Erkennung ungewöhnlicher oder riskanter Aktionen

Phase 3: Überwachen & Analysieren

- Durchsetzung von Sicherheitsrichtlinien in Echtzeit
- Automatische Aktionen bei Verstößen: blockieren, verschlüsseln, umleiten, warnen
- Dynamische Anpassung an Risiko-Level und Benutzerkontext

Herausforderungen lösen durch Data-Centric Security



Infrastruktur ≠ Daten

Schutz der Infrastruktur, aber nicht der Daten selbst



Externe Datenkanäle

Keine durchgängige Kontrolle über externe Datenkanäle



Sichtbarkeit & Auditability

Mangelnde Echtzeit-transparenz und Dokumentation



Vernetzte Ökosysteme

Third-Party & Insider bleiben Angriffsvektor Nr. 1



Mult-Kanal Abdeckung

- Kontrolle über Datenflüsse – unabhängig vom Kanal oder Akteur
- Endpoint, Email, Web, Cloud, API
- Einheitliches Policy-Enforcement über alle Kanäle



Daten-Klassifizierung

- Automatisierte Klassifizierung & Schützen sensibler Daten
- EDM/IDM, OCR, Machine Learning
- Automatisierte Schutzmaßnahmen



Compliance: NIS2/DORA/GDPR

- Integration in regulatorische Reportingpflichten (NIS2/DORA/GDPR)
- Belastbare Audit-Trails
- Automatisierte Dokumentation



Echtzeit-Transparenz

- Echtzeitüberwachung aller Datenflüsse
- Frühwarnsystem und forensische Untersuchung
- Erhöhte Resilienz



Carbon Black.
by Broadcom



Lukas Zettl

Regional Sales Manager

Symantec

lukas.zettl@arrow.com

+43 664 88699784