# Sicherer Umgang mit Dokumenten, ob E-Mail, Up- oder Download

Content Disarm & Reconstruction (CDR)

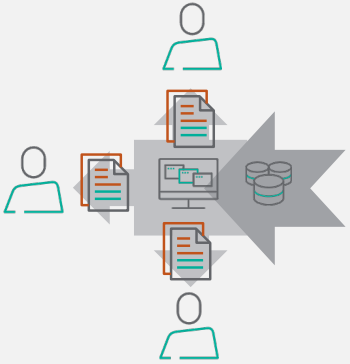
Matthias Senft
Senior Presales Consultant

Forcepoint

# Das Problem bei der gemeinsamen Nutzung von Daten

Um Informationen zu erhalten, müssen Sie Daten akzeptieren, …

… aber Daten können ***Schadsoftware*** enthalten.



Um Informationen auszutauschen, müssen Sie Daten senden, …

… aber Daten können auch ***zusätzliche Informationen*** enthalten.

Wie schützen Sie Ihr Unternehmen, wenn Sie nicht die neuesten Bedrohungen erkennen können?

# Umfrage – bitte geben Sie uns Feedback!

(1/3) Haben Sie es in der Vergangenheit erlebt, dass trotz unterschiedlicher Schutzmechanismen Schadcode ins Unternehmen gekommen ist?

Antwortmöglichkeiten:(JA / NEIN)

# Umfrage – bitte geben Sie uns Feedback!

(2/3) Durch wie viele Security-Technologien (Firewall, Proxy, AV, Sandbox etc.) geht eine Datei bis ein User damit arbeiten kann?

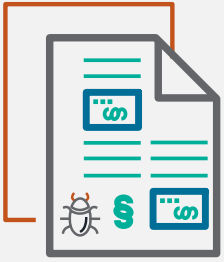
Antwortmöglichkeiten:(0/1/3/5+)

# Umfrage – bitte geben Sie uns Feedback!

(3/3) Können Dokumente in Echtzeit geprüft und zugestellt werden?

Antwortmöglichkeiten: (JA / NEIN)

# Der neue Zero-Trust-Ansatz für Malware:
# **Entschärfung und Rekonstruktion von Inhalten**



UNSICHERE DIGITALE INHALTE

SICHERE DIGITALE INHALTE

**EXTRAHIEREN**

von Inhalten aus den Originaldaten, Verwerfen unerwünschter Inhalte

**ÜBERPRÜFEN**

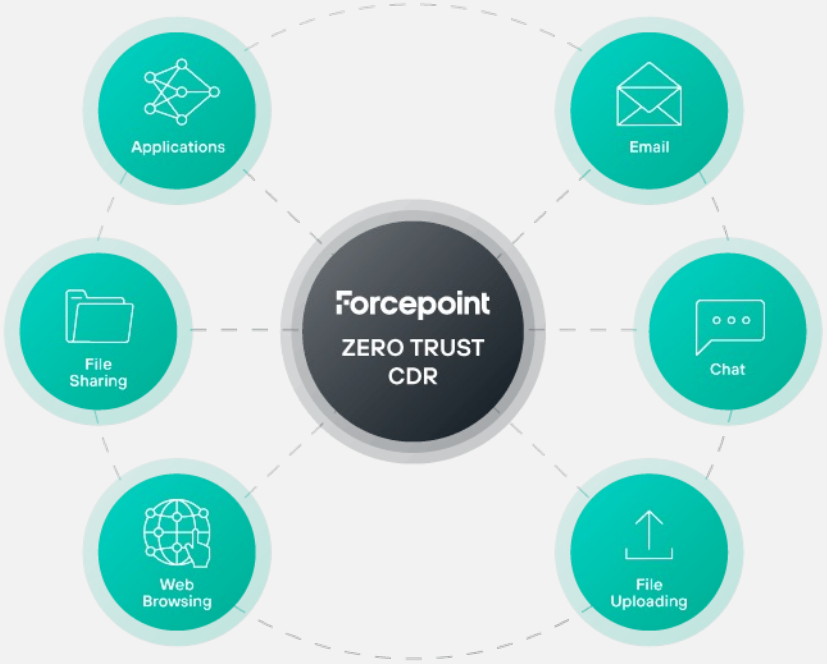
ob die Informationen sicher sind

**ERSTELLEN**

100% sicherer Informationen und Daten

- **Extrahieren** Sie nur die Nutzinformationen - sonst nichts
- **Transformieren und normalisieren** Sie alles, vertrauen Sie keinen Daten, die in einen Prozess eingespeist werden
- **Stoppen Sie Schadsoftware,** ohne sie erkennen zu müssen

# Zero Trust CDR Use Cases




100% malware-free

Pixel perfect, fully revisable files

No false positives

No latency

# Zero Trust CDR Use Cases

## Die häufigsten Use Cases unserer Kunden

- Web-Download

  „Mitarbeiter lädt sich Dateien von einer Webseite herunter“

- Portal-Upload

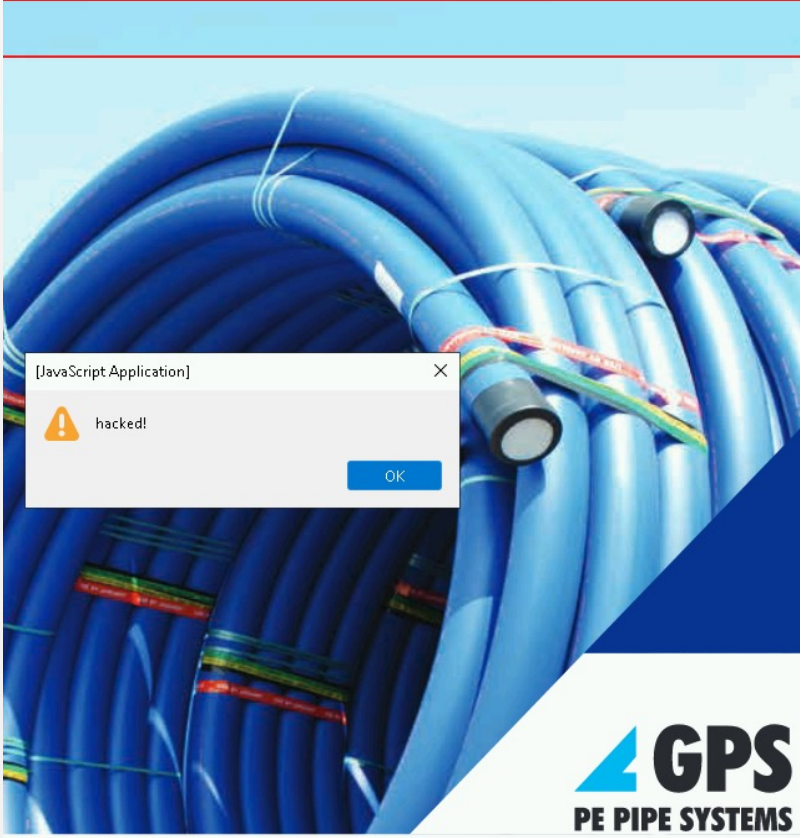
  „Externe laden Dokumente oder Bilder in Portal hoch, ein Mitarbeiter öffnet die Datei“

- E-Mail-Kommunikation

  „Sender und Empfänger tauschen Anhänge per E-Mail aus“

Live-Demo

# Content Disarm & Reconstruction



# Die Vorteile von Zero Trust CDR

| Sicherheit | Investitionsschutz | Flexibilität | Leistungsstark |
|---|---|---|---|
| • Beseitigt alle Malware<br>• Umgehungssicher<br>• Zukunftssicher | • Keine Falschmeldungen<br>• Keine zu verteilenden Updates<br>• Keine Notwendigkeit, Patches übereilt zu verteilen<br>• Keine unmittelbare Notwendigkeit, anfällige Legacy-Anwendungen zu ersetzen | • Cloud-Service<br>• Vor-Ort-Installation<br>• Virtuelle Umgebungen | • Schnelle zustandslose Verarbeitung<br>• Skalierbarer, unterbrechungsfreier Betrieb<br>• Nahezu in Echtzeit |

Wir nennen unsere Lösung **Zero Trust CDR.**
**Vertraue nichts** und **transformiere alles!**

# Bereitstellungsoptionen für Zero Trust CDR

## On- Premise

- Software only
- High assurance appliance

## Cloud

Private Cloud

Public Cloud

- VMs - Software
- APIs – Software

# Der Vergleich

| Bedrohung | Traditionelles CDR | Forcepoint Zero Trust CDR |
|---|---|---|
| **Ausführbarer Code** | Versucht, bekannten ausführbaren Code zu erkennen und zu entfernen | ✓ Liefert nie ausführbaren Code aus |
| **Ausnutzung von Dateiformaten** | Versucht, bekannte Exploits zu erkennen und zu entfernen, und rekonstruiert die Originaldateien so, dass sie mit den Standards übereinstimmen. | ✓ Quelldaten sind nicht vertrauenswürdig - Daten werden nie von einem zum anderen Ende transportiert, alle Informationen werden extrahiert, überprüft und als neue Dateien erstellt |
| **Manipulierte Dateistrukturen** | Versucht, bekannte fehlerhafte Strukturen zu erkennen und zu korrigieren und rekonstruiert die Originaldateien so, dass sie den Standards entsprechen | ✓ Keine Erkennung - wir extrahieren nur Informationen, die wir verstehen, selbst wenn sie fehlerhaft sind, und erstellen neue Daten, die immer korrekt aufgebaut sind. |
| **Steganographie** | Nur Abwehr von eingehenden Angriffen | ✓ Stoppt eingehende Malware und verdeckte Exfiltration, zudem verbessert es DLP durch Hinzufügen von „Anti-Steganografie“ für ausgehende Bilddaten |

# Zusammenfassung

- Zero Trust-Technologie, die **Malware-freie Daten** liefert und eine **verdeckte Exfiltration verhindert**
- **Flexible** Bereitstellungen in der Cloud, vor Ort und virtuell
- Wesentliche **wirtschaftliche Vorteile** und **verbesserte Nutzererfahrung**
- Eine hochwirksame Lösung für eines der schwierigsten Probleme der Welt: **sicherer Austausch von Informationen**