Modernisieren von SecOps mit Elastic Security

Dalibor Galić - Enterprise Account Executive

Matthias Holzgethan - Senior Solutions Architect

elastic

Meet Elastic

Elastic helps everyone find answers that matter.
From all data. In real time. At scale.

Founded in 2012

2800+
employees

40+
Countries with employees

4B+
downloads

54%
Of Fortune 500 companies
trust Elastic

elastic

One Data Analytics Platform
Two Out-of-the-Box Solutions
The Freedom to Build Anything

elastic

Elastic is Wherever Your Data Lives

- Public Cloud
- Hybrid
- On-Premises

aws Google Cloud Microsoft Azure
Alibaba Cloud Tencent Cloud

Amazon Web Services Google Cloud Microsoft Azure

50+ Cloud Regions Globally

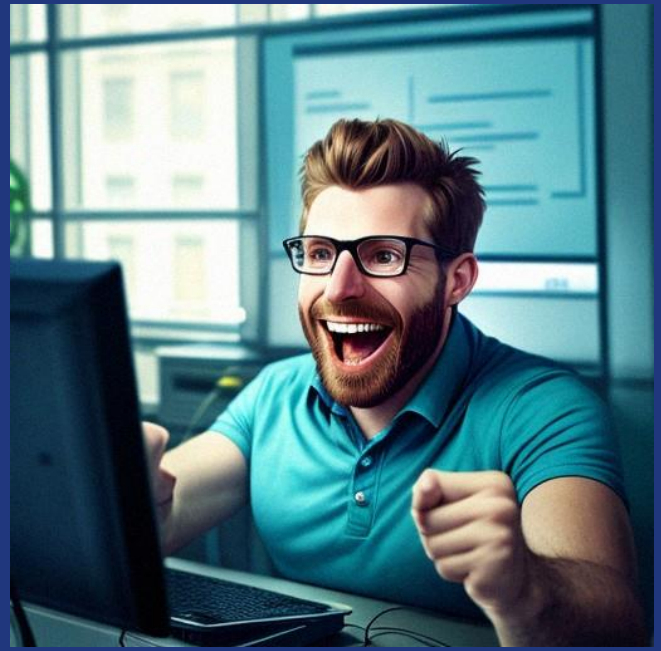
elastic

SIEM Installationen und Migrationen stellen Unternehmen vor große Herausforderungen

Elastic Security

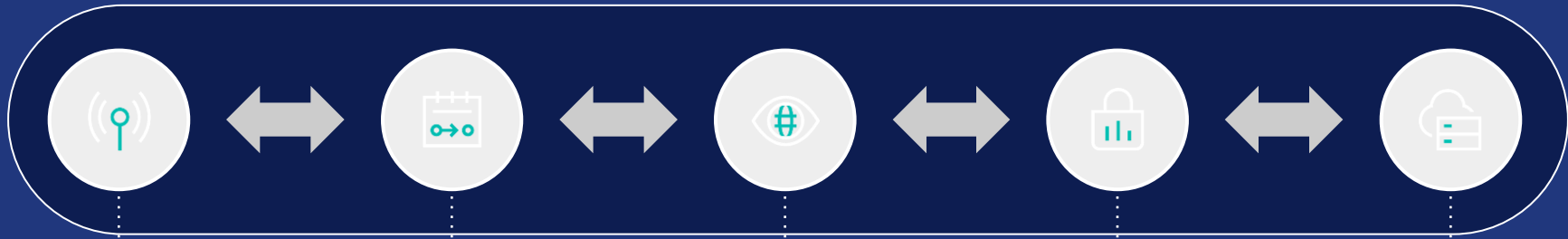
… hilft dabei Risiken zu reduzieren und das Budget zu optimieren:

- Dynamische Security Workflows helfen den Security Analysten
- Security Ausgaben können durch die flexiblen Lizenz-Optionen optimiert werden
- Zukunftssicherheit für Ihr SOC durch kontinuierliche Innovation



elastic

Typische Herausforderungen im Bereich Security



Zu viele Alarme

Security-Teams werden mit Alarmen “geflutet” - die wirklichen Vorfälle können dabei untergehen

Zu langsame Reaktion

Oft fehlt der Kontext zu einem Alarm. Dies erschwert die korrekte Einstufung von Alarmen und verzögert die korrekte Reaktion

Eingeschränkte Sicht

Silos, Skalierungs- und Kostenprobleme schränken die Transparenz ein und verlangsamen die Erkennung von Vorfällen

Geringe Flexibilität

SIEM, Endpoint und Cloud tools sind oft nicht flexible genug und um Kosten zu sparen wird dann oft nicht das gesamte Unternehmen abgedeckt

Komplexität in der Cloud

Hohe Kosten für Datentransfer und Datenhoheit sowie eine sehr dynamische und schnell wachsende Umgebung

elastic

Zukunftssicherheit für Ihr SOC

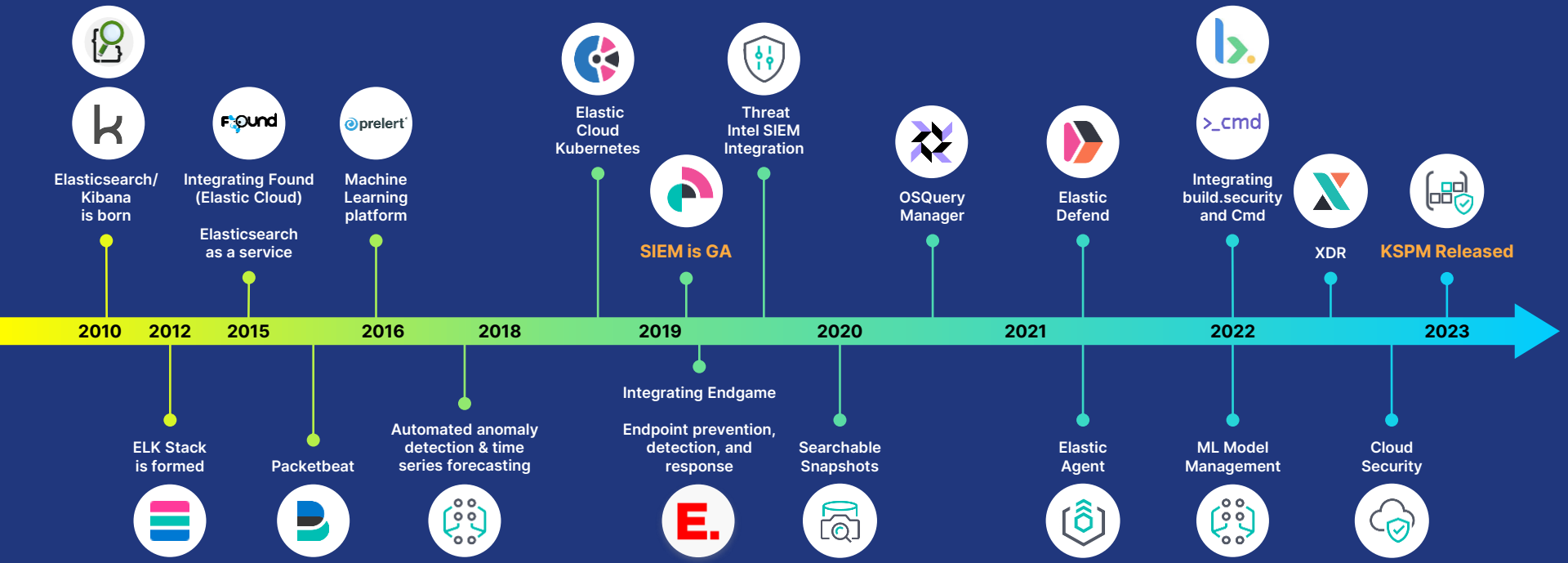
- On prem
- Containerized
- Cloud
- Multi Cloud
- Hybrid

- Custom Dashboards
- Graph Analysis
- Machine Learning
- Maps
- Canvas Presentations
- Open Source Community

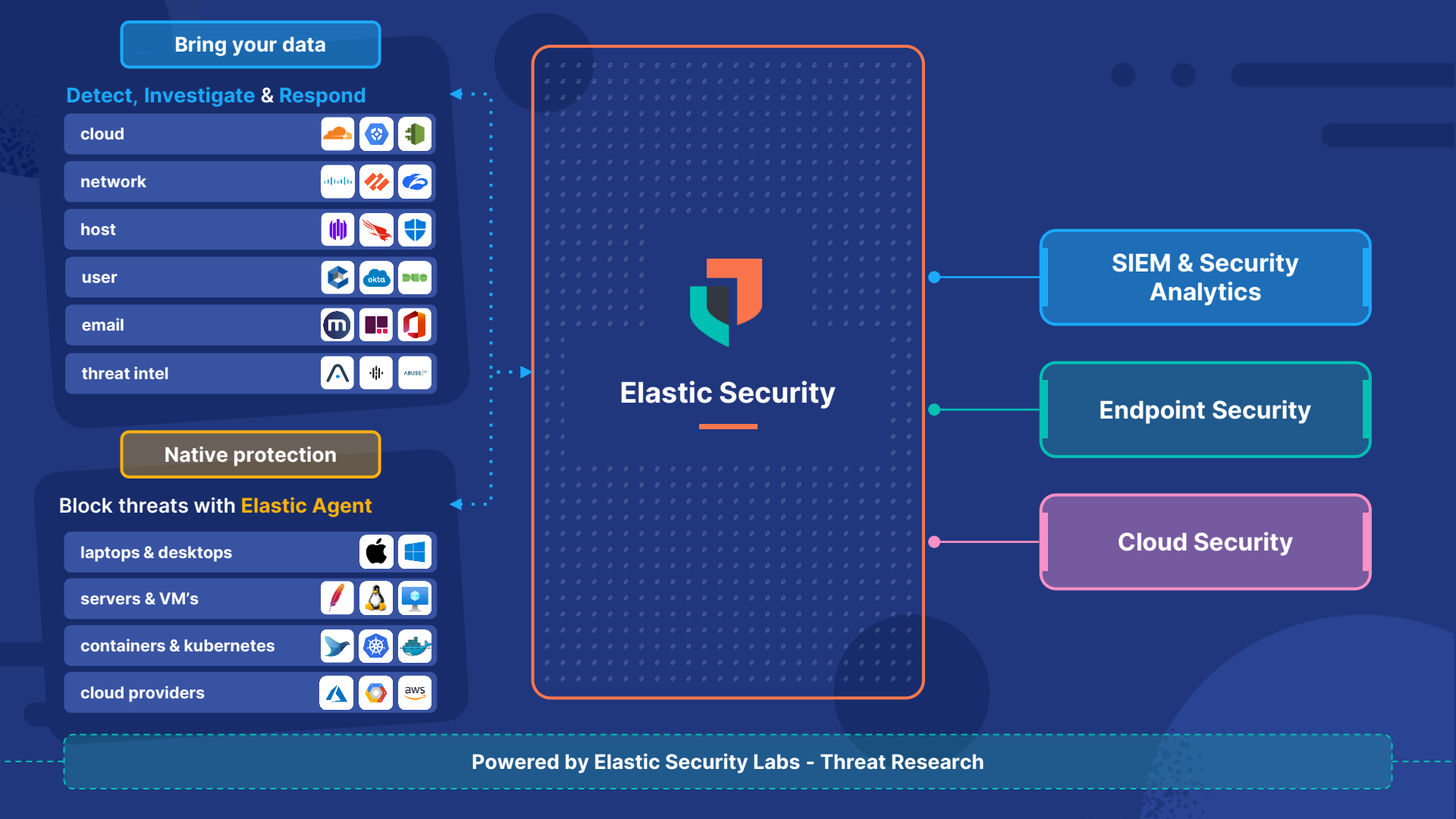
elastic

Zukunftssicherheit für Ihr SOC

Nachweisliche Erfolgsbilanz in Sachen Innovation



elastic


Bring your data
Detect, Investigate & Respond
cloud
network
host
user
email
threat intel
Native protection
Block threats with Elastic Agent
laptops & desktops
servers & VM's
containers & kubernetes
cloud providers
Elastic Security
SIEM & Security Analytics
Endpoint Security
Cloud Security
Powered by Elastic Security Labs - Threat Research

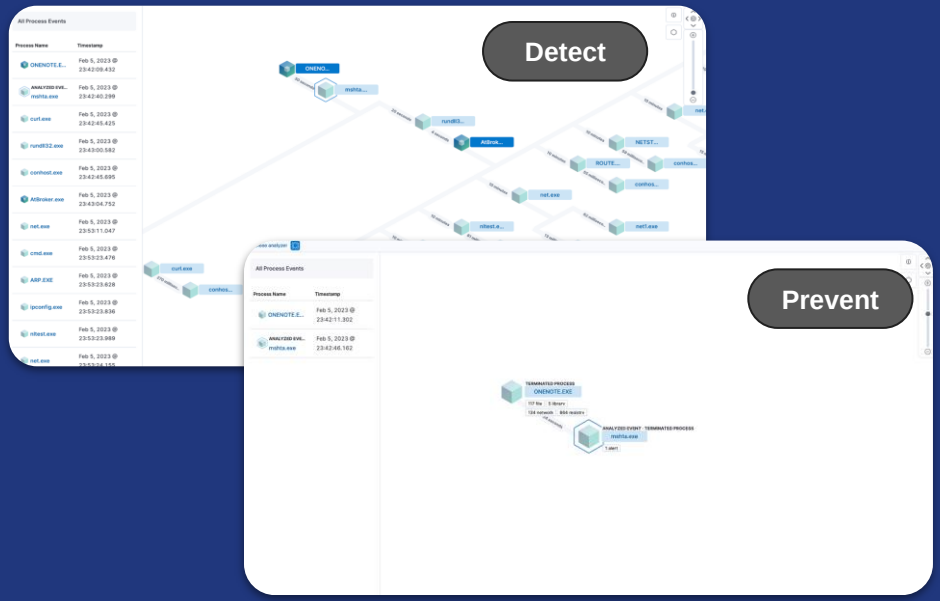
Das Werkzeug für Security Analysten

Protect → Investigate → Respond

Angriffe erkennen bevor diese starten

Automatisierung beim Threat Hunting

Bedrohungen (im gleichen Workflow) erfolgreich abwehren



elastic

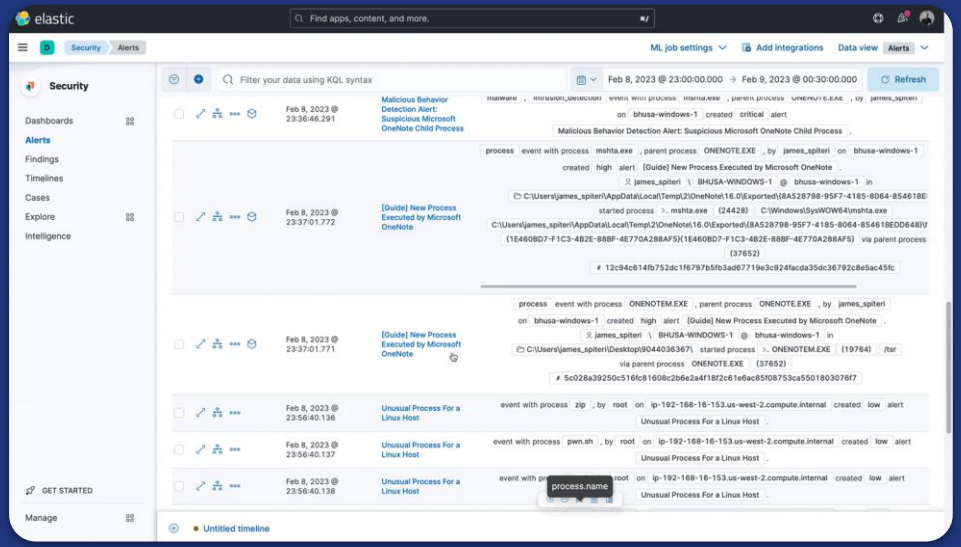
Das Werkzeug für Security Analysten

Protect → **Investigate** → **Respond**

Angriffe erkennen bevor diese starten

Automatisierung beim Threat Hunting

Bedrohungen (im gleichen Workflow) erfolgreich abwehren



elastic

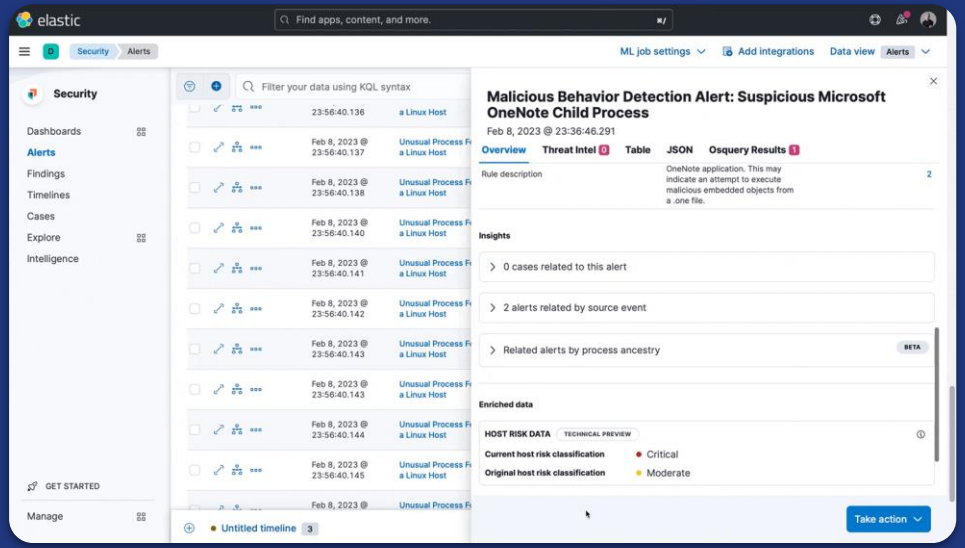
Das Werkzeug für Security Analysten

Protect → **Investigate** → **Respond**

Angriffe erkennen bevor diese starten

Automatisierung beim Threat Hunting

Bedrohungen (im gleichen Workflow) erfolgreich abwehren



elastic

Optimierung der Security-Ausgaben

Trotz hoher Aufbewahrungsdauer und hoher Verfügbarkeit

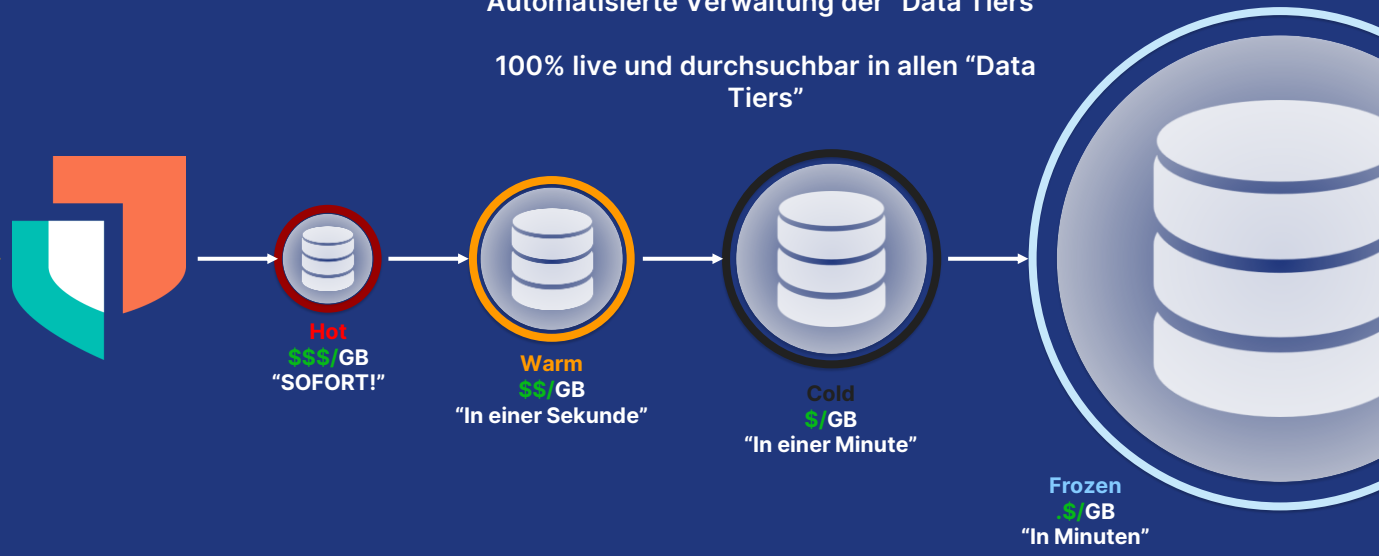
Konsolidierung

- SIEM
- Endpoint
- Cloud
- Container
- Soar
- Threat Intel
- *Observability*

Optimiertes Budget

Automatisierte Verwaltung der “Data Tiers”

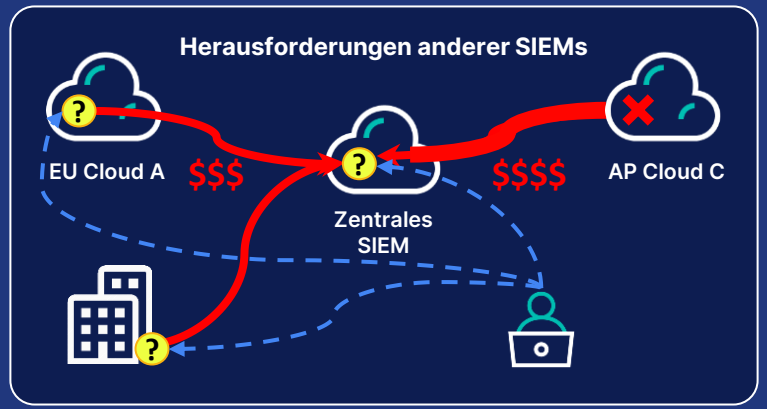
100% live und durchsuchbar in allen “Data Tiers”

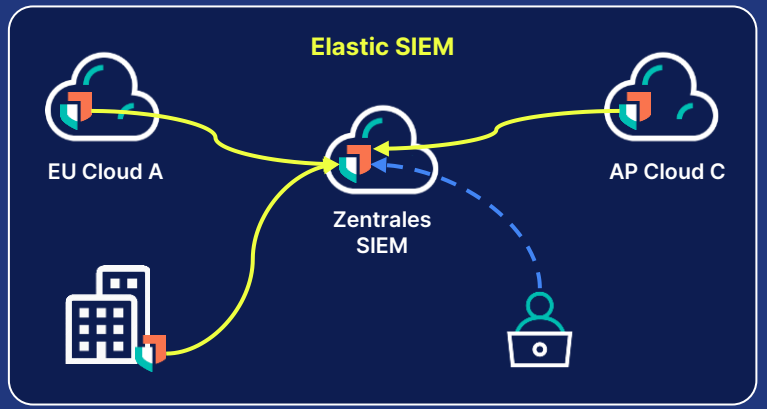


elastic

Optimierung der Security-Ausgaben

Hohe Flexibilität in hybriden und Multi-Cloud Umgebungen





Cloud Kosten

- Datentransferkosten sind hoch

Komplexität in hybriden Cloud-Umgebungen

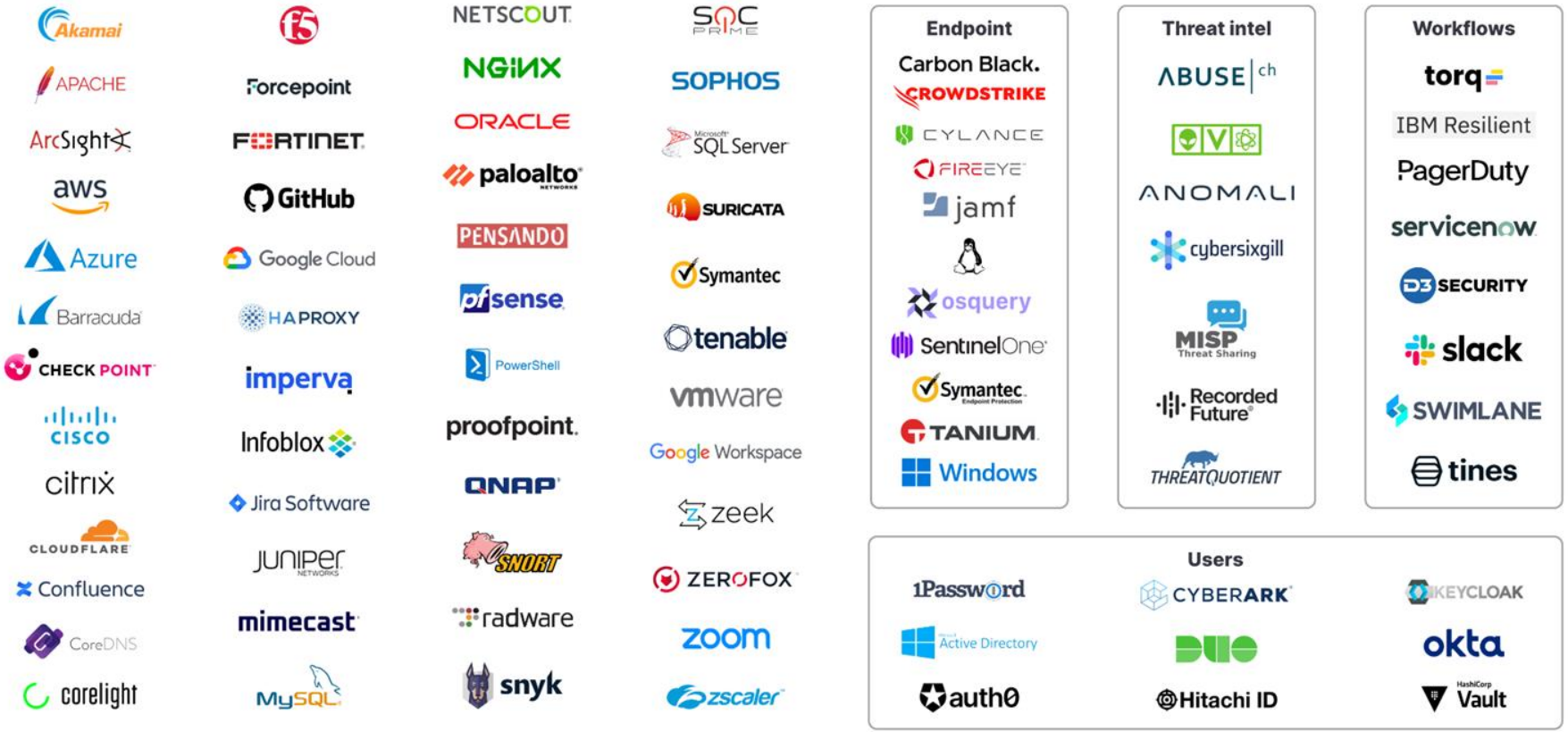
- Gleiche Funktionen?
- Wo sind meine Daten gespeichert?
- Verfügbarkeit der Cloud-Umgebungen?

Datenzugriff leicht gemacht

- Sicheres “Distributed Search”
  - Korrelation zwischen Cloud Instanzen
  - Datenhoheit sicherstellen
  - Vollständiges RBAC / ABAC
  - Datentransferkosten deutlich reduzieren
- Gleicher Funktionsumfang zwischen Cloud und self-managed
- 50+ Elastic Cloud Regionen

elastic

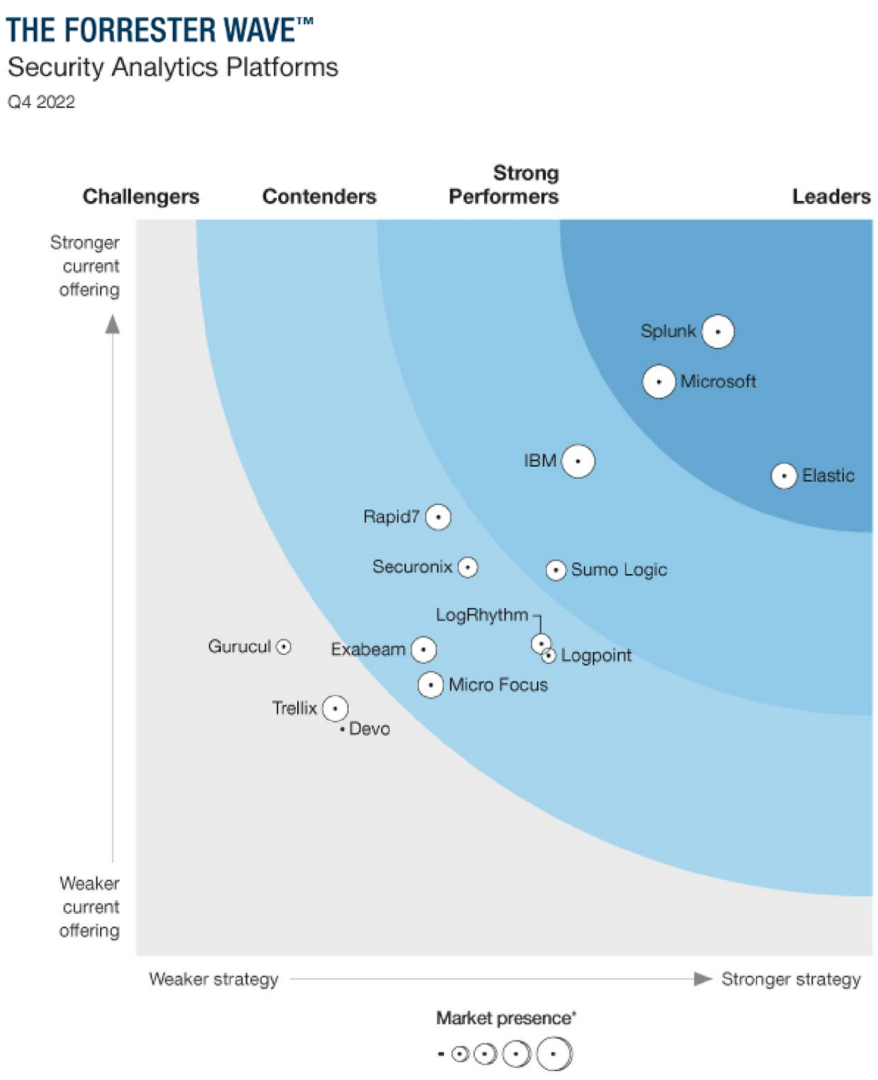
Integrationen mit wichtigen Partnern



Elastic named a Leader in The Forrester Wave™ Security Analytics Platforms Q4 2022

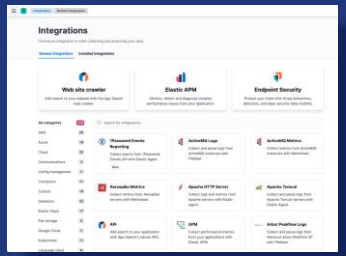
FORRESTER®
WAVE LEADER 2022
Security Analytics Platforms

- *"Elastic provides incredible flexibility and visualizations in an open offering."*
- *"Reference customers value the flexibility on pricing and subsequent cost savings that Elastic provides."*
- *"Elastic Security best suits clients comfortable with security engineering looking for an extremely customizable product."*

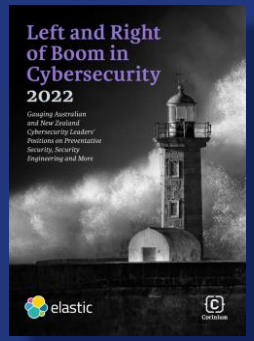


Wie können Sie mehr über Elastic Security erfahren?

Elastic's Research (z.B. Global Threat Report) ist verfügbar via Security Labs
elastic.co/security-labs



Elastic Security selbst ausprobieren
cloud.elastic.co



Lesen sie unser Paper "Left and Right of Boom in Cybersecurity"
elastic.co/left-right-boom-cybersecurity-2022

OH MY MALWARE!

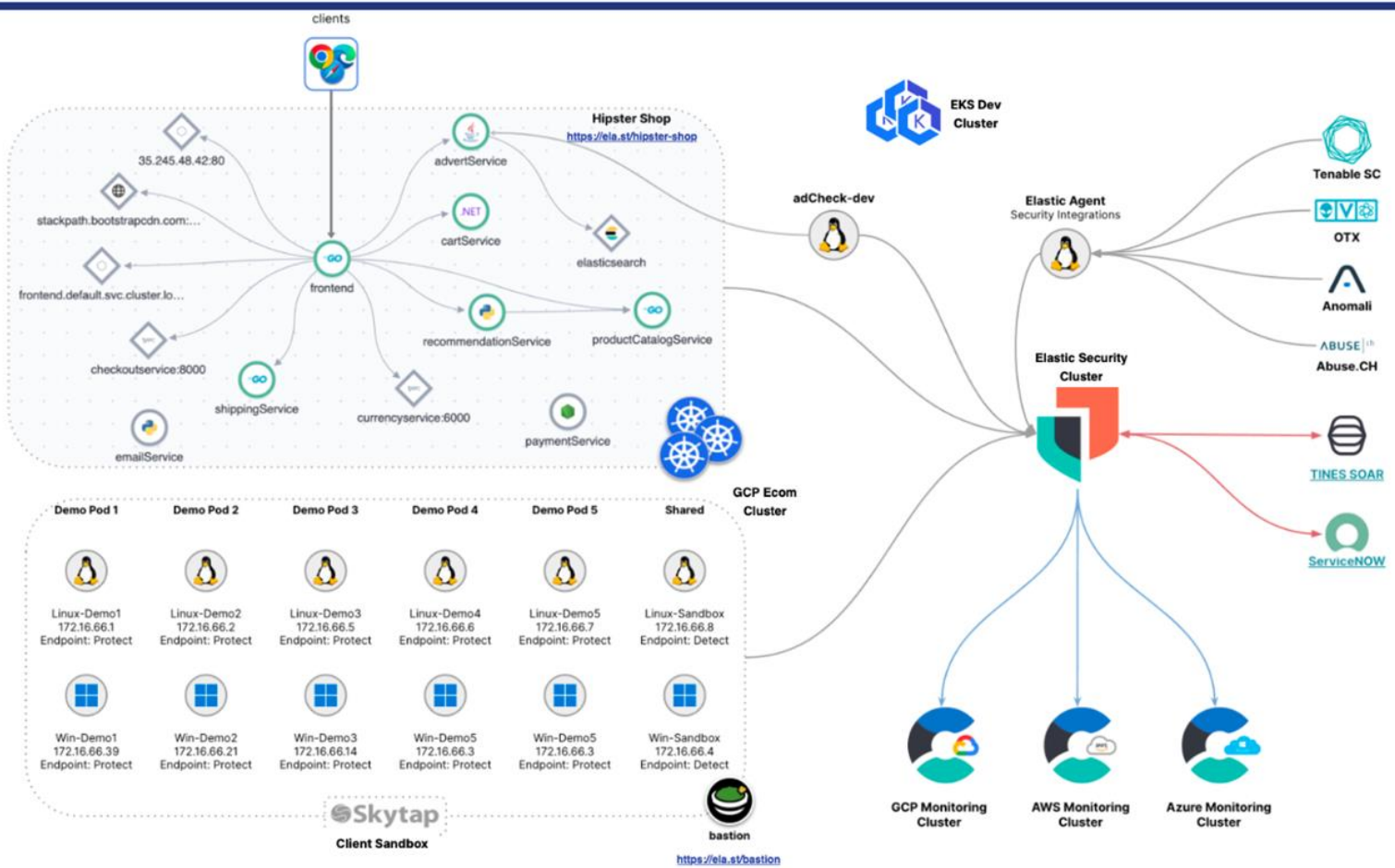
Schauen Sie sich eine Malware Demo an
ohmymalware.com

Sprechen Sie mit Ihrem Elastic Account Team

elastic

Demo

Architecture



elastic

Vielen Dank für die Aufmerksamkeit

elastic