# Schutzstrategien gegen gezielte Angriffe

## Vor, Während und Nach einem Angriff

Roland Müller, Cisco Systems GmbH
System Engineer

Februar 2016

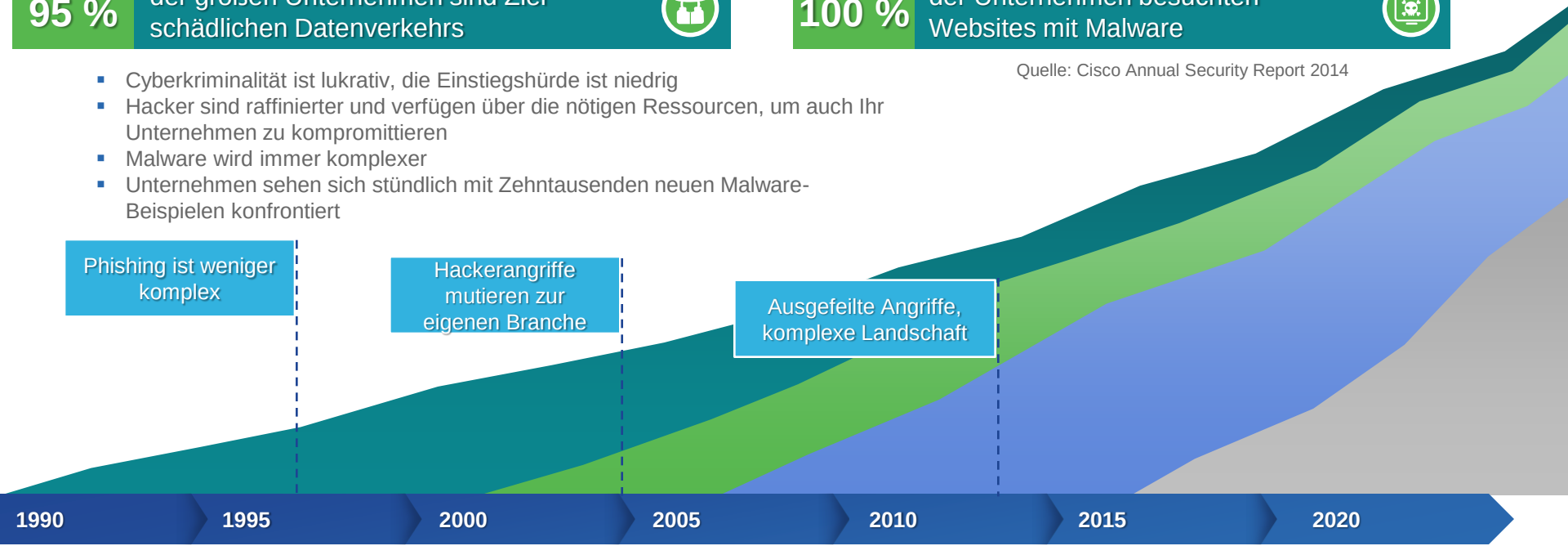
# Die Realität:
## Unternehmen sind Angriffsziele

**95 %** der großen Unternehmen sind Ziel schädlichen Datenverkehrs

**100 %** der Unternehmen besuchten Websites mit Malware

Quelle: Cisco Annual Security Report 2014

- Cyberkriminalität ist lukrativ, die Einstiegshürde ist niedrig
- Hacker sind raffinierter und verfügen über die nötigen Ressourcen, um auch Ihr Unternehmen zu kompromittieren
- Malware wird immer komplexer
- Unternehmen sehen sich stündlich mit Zehntausenden neuen Malware-Beispielen konfrontiert




**Viren**
1990-2000

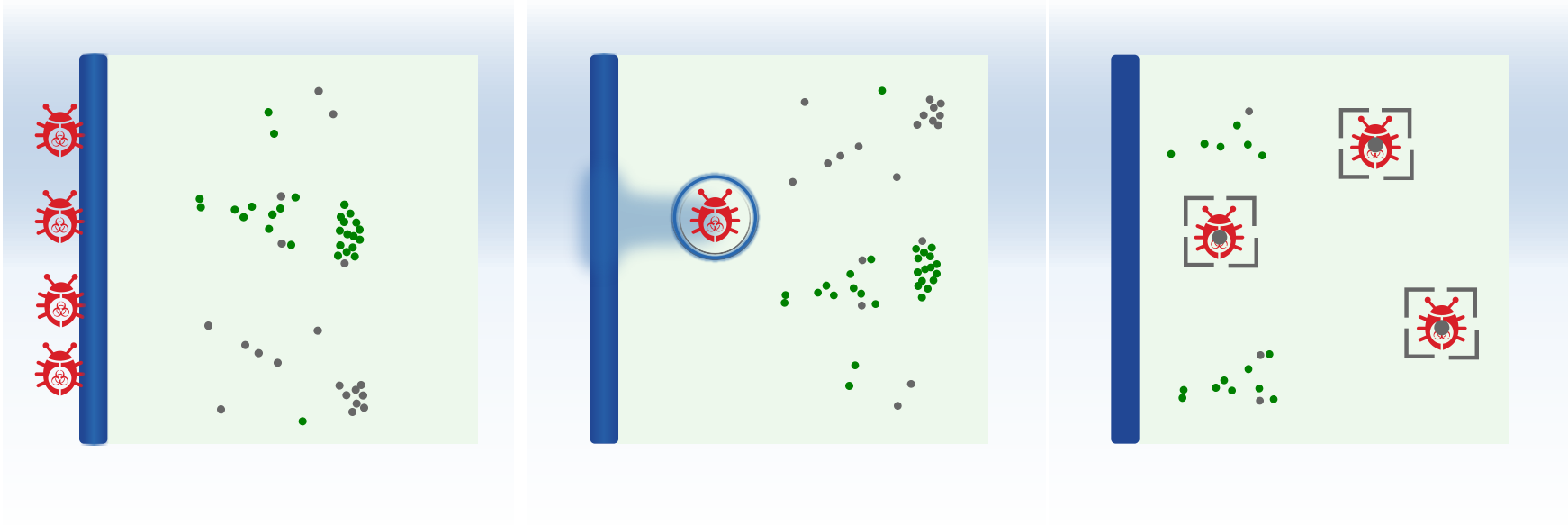
**Würmer**
2000-2005

**Spyware und Rootkits**
2005 bis heute

**APTs Cyberware**
Heute und in Zukunft

# Umfassende Sicherheit bedeutet heute mehr als nur Policy Control

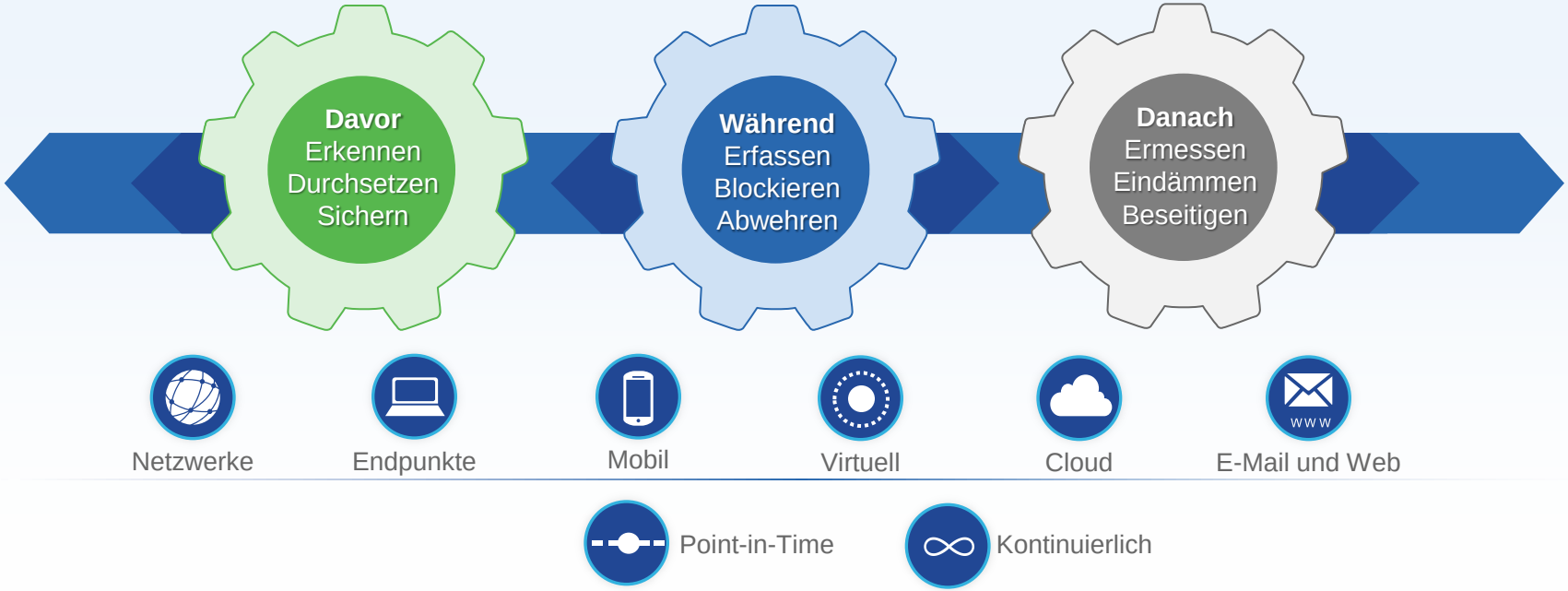
| Schutz vor Sicherheitsverletzungen | Schnelle Erkennung, Reaktion, Beseitigung | Threat Intelligence |
| --- | --- | --- |



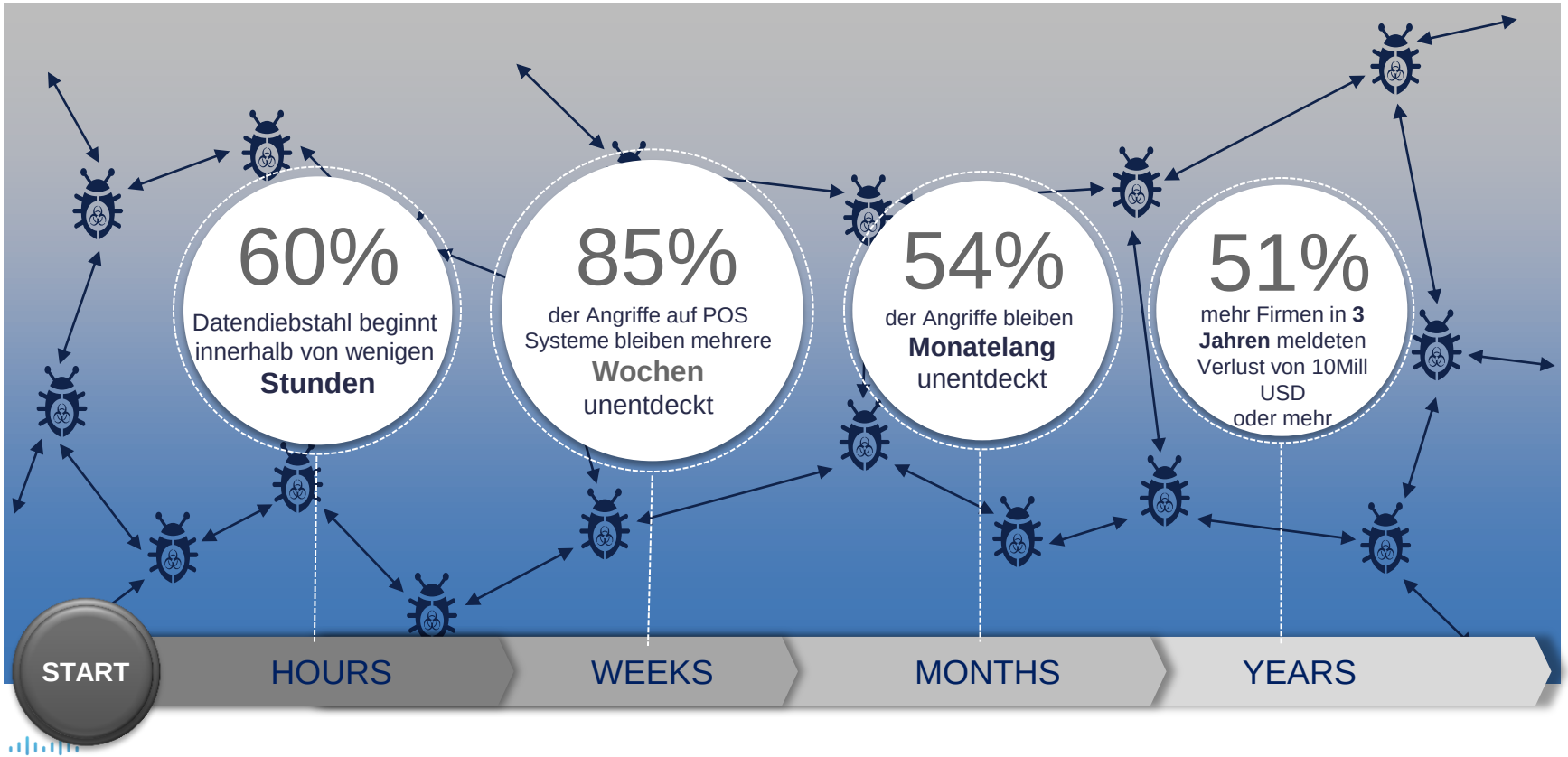
Quelle: http://www.pcworld.com/article/2109210/report-average-of-82-000-new-malware-threats-per-day-in-2013.html

# Schutz vor diesen komplexen Bedrohungen erfordert umfassende Transparenz und Kontrolle über das gesamte Angriffskontinuum

## Angriffskontinuum



# Schnelle Angriffserkennung ist Essentiell



# Cisco IT hat seine Angriffserkennung optimiert

Juni 2015 (Median)

**35.3**

**STUNDEN**

VS

Oktober 2015 (Median)

**17.5**

**STUNDEN**

Cisco ist somit wesentlich schneller als der Industriedurchschnitt (geschätzt zwischen 100 und 200 Tagen)

# Wie kommt’s???? Warum ist Cisco so viel schneller?

Cisco arbeitet mit „**Retrospective Security**“

Mittels Retrospective Security lassen sich Angriffe, welche die alle Verteidigungslinien durchbrochen haben, im **Nachhinein** identifizieren, die Ausbreitung lokalisieren und automatisch oder manuell auflösen.

Retrospective Security ist eine kritische Komponente um die Zeit bis zur Angriffserkennung zu reduzieren.

# Der Wert von Retrospective Security

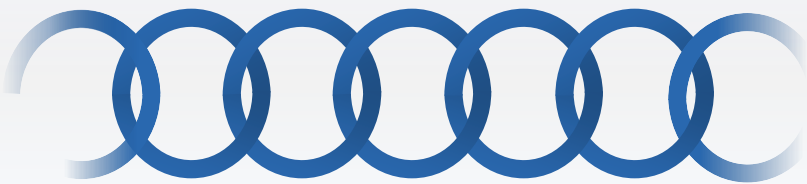
- Wenn Malware trotz aller Sicherheitsmechanmismen durchschlüpft…
- ... weil sie gänzlich **neu** ist und als solche zunächst nicht zu erkennen ist...

# Der Mehrwert von Retrospective Security

- Wenn Malware trotz aller Sicherheitsmechanmismen trozdem durchschlüpft…
- ... weil sie gänzlich **neu** ist und als solche zunächst nicht zu erkennen ist...
- … und am nächsten Tag weiss ich, das ist Malware
- Dann möchte ich wissen
  - Woher es kam, wie kam es durch?
  - Was macht es genau?
  - Und wo ist’s noch überall?

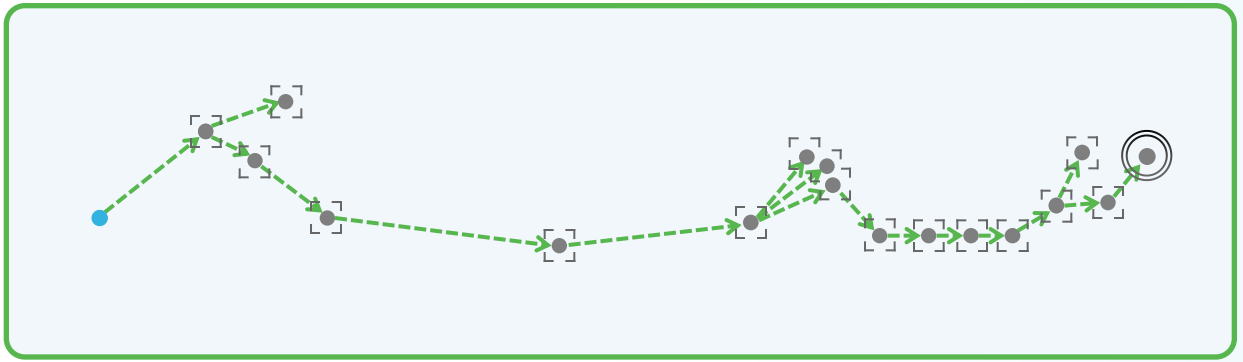
**„Golden Gun“ von Francisco Scaramanga aus James Bond: „The Man with the Golden Gun“**

# Cisco Advanced Malware Protection arbeitet mit **Retrospective Security**

| Point-in-Time-Schutz | Retrospective Security |
| --- | --- |
|  |  |
| Dateireputation, Sandbox-Analysen und Verhaltenserkennung | Kontinuierliche Analysen |

Nur bei Cisco® AMP verfügbar

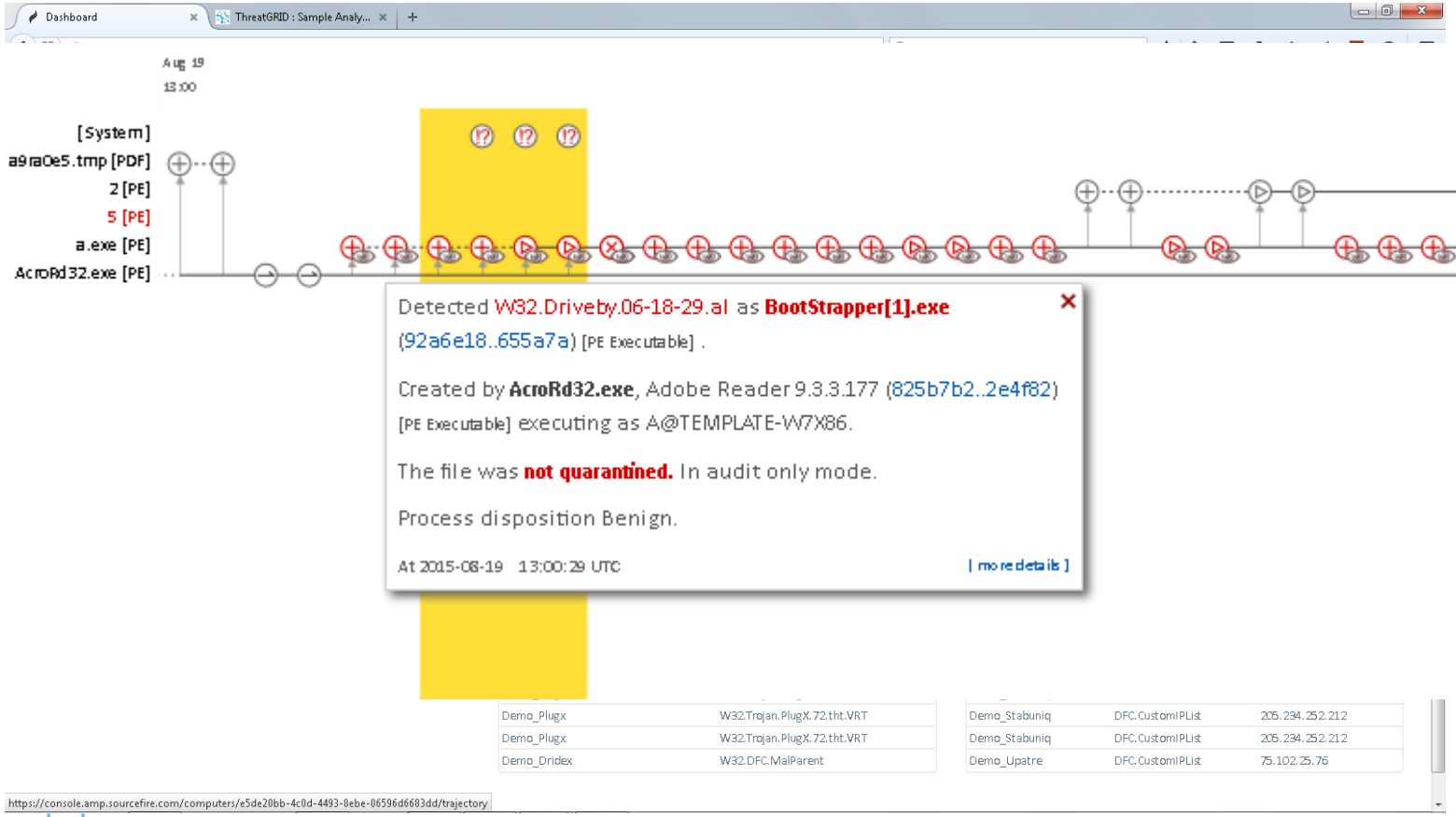
# Plan B: Retrospective Security



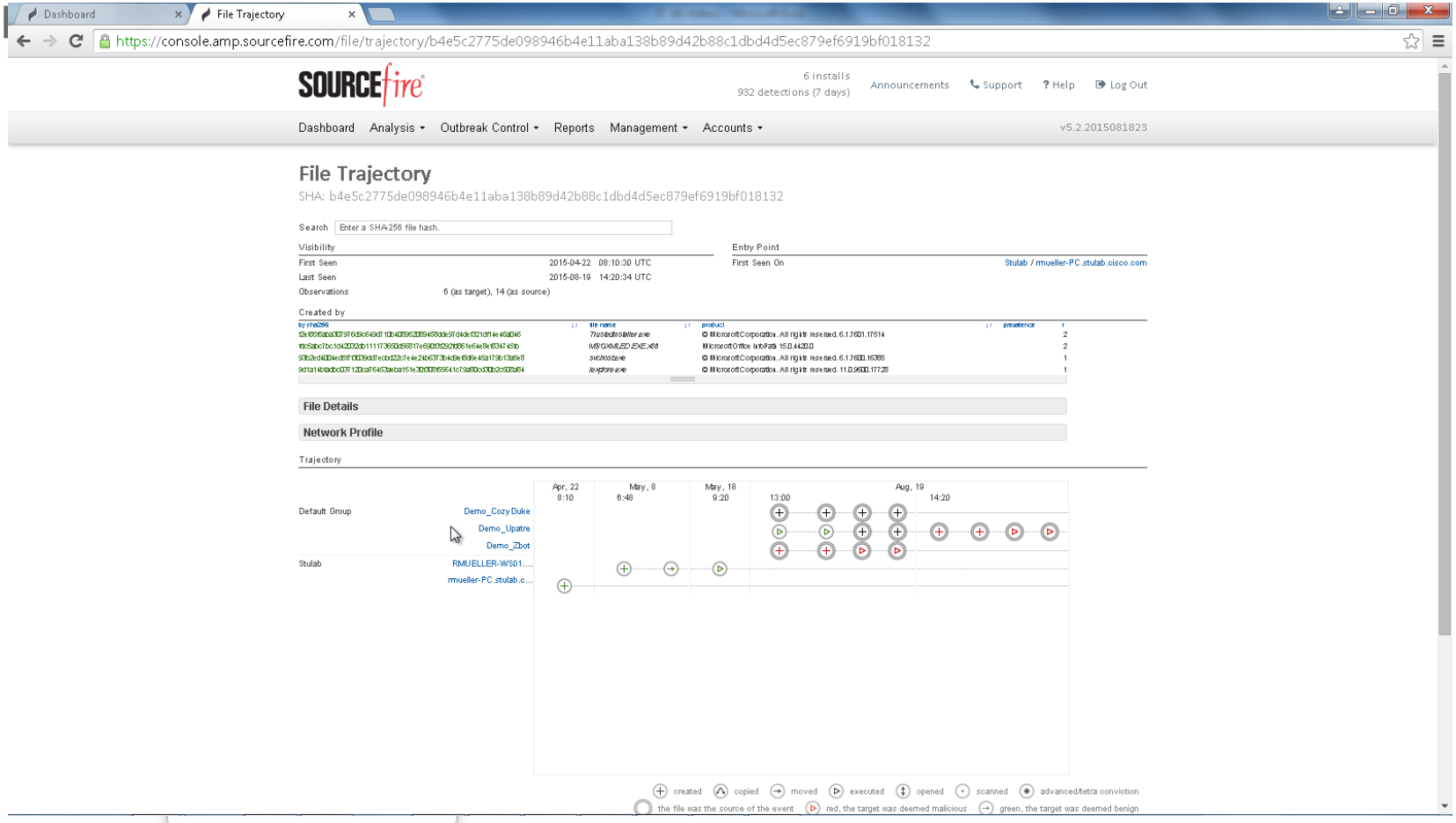
| | |
|---|---|
| 1 | Analyse wird bei erstem Kontakt einer Datei durchgeführt |
| 2 | Datei wird fortlaufend analysiert, Änderungen an der Einstufung werden ggf. ermittelt |
| 3 | Umfassende Transparenz von Pfad, Aktionen oder Kommunikationswegen einer bestimmten Software wird hergestellt |

# Was genau ist passiert?

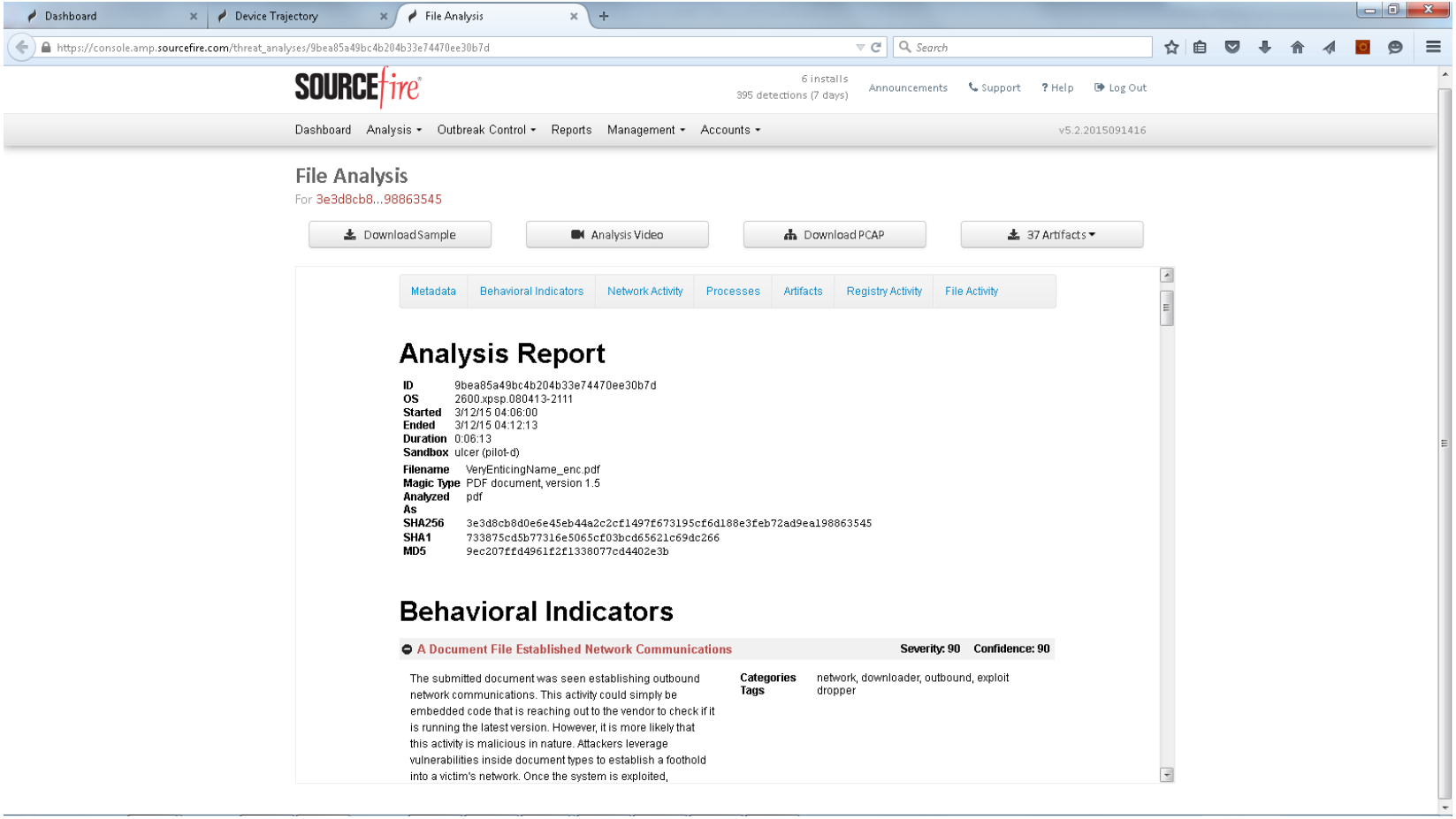
## Cisco AMP zeigt eine detaillierte Historie des Angriffs



# Wie weit ist die Infektion bereits fortgeschritten?

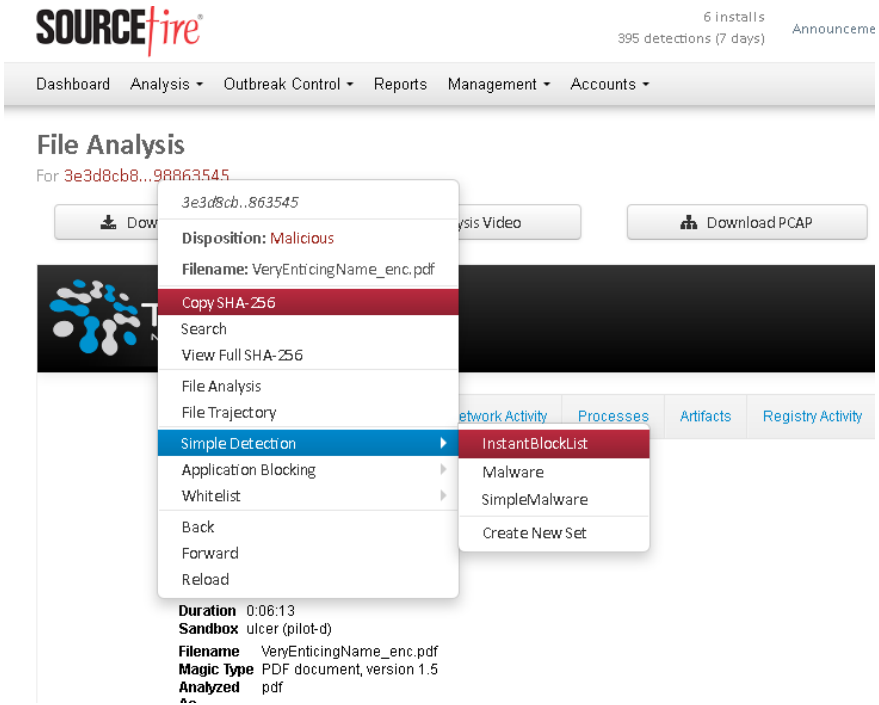


# Was genau macht die Malware?

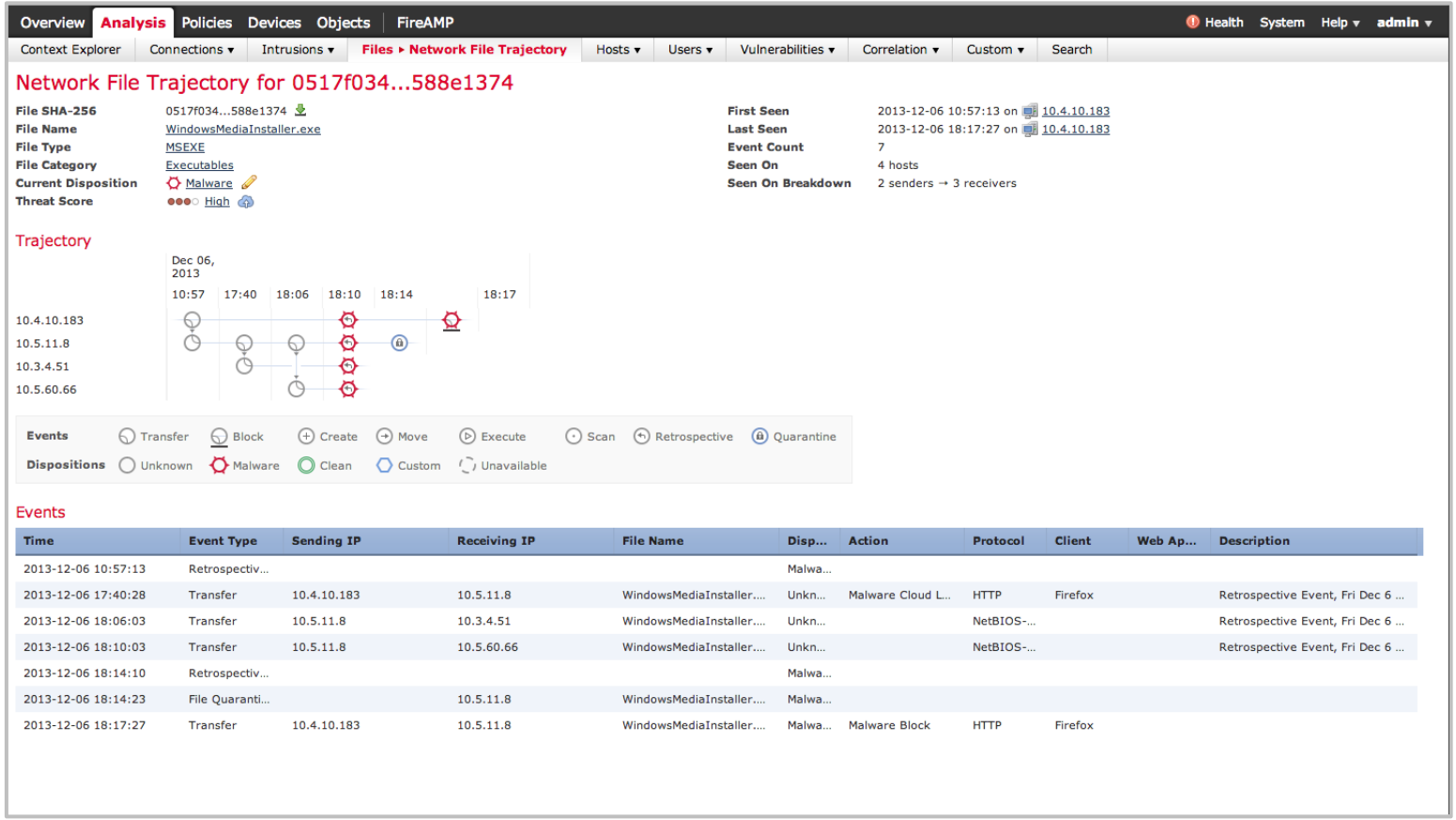


# Wie können wir den Angriff stoppen?

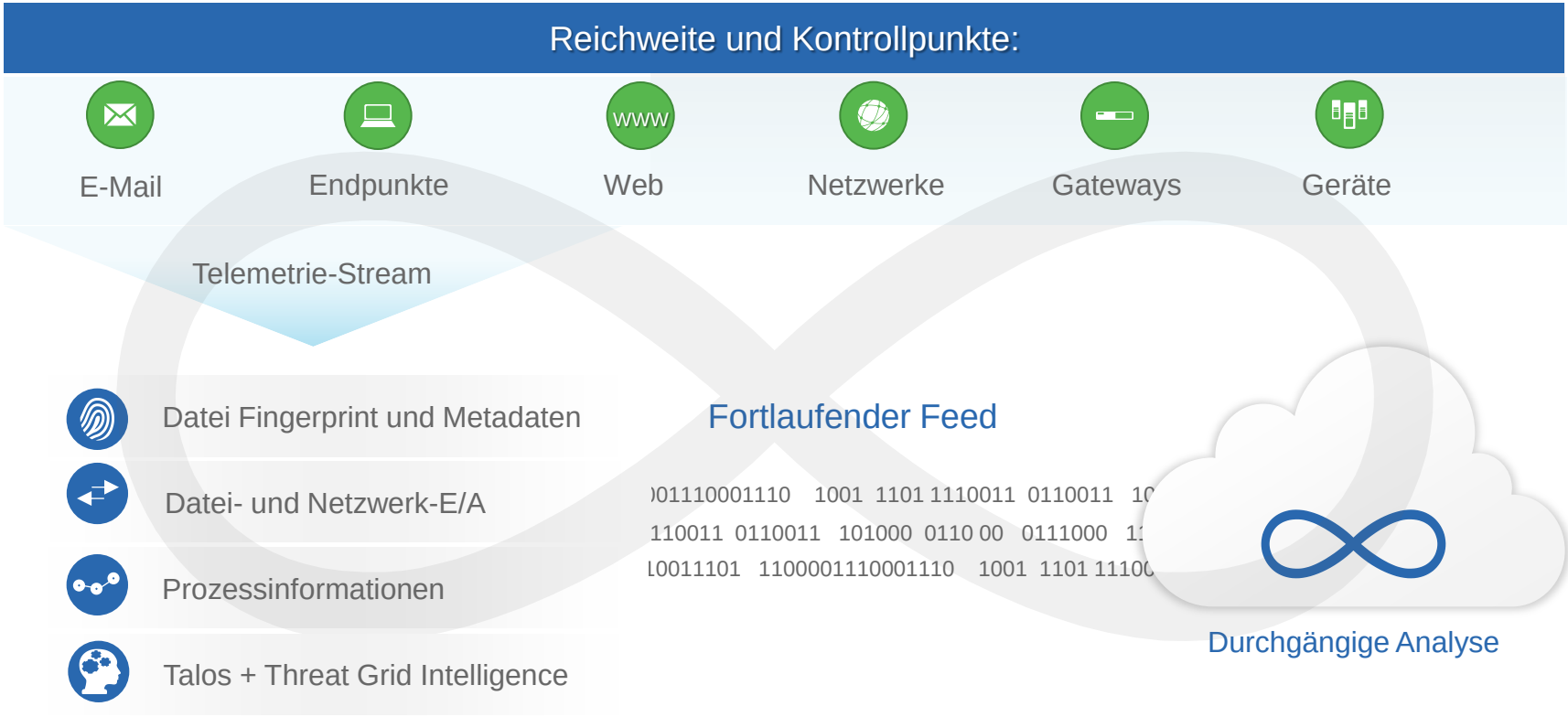
Per Mausklick wird ein File an allen Endgeräten und auch im Netzwerk als “Schädling” gekennzeichnet und unter Quartäne gesetzt



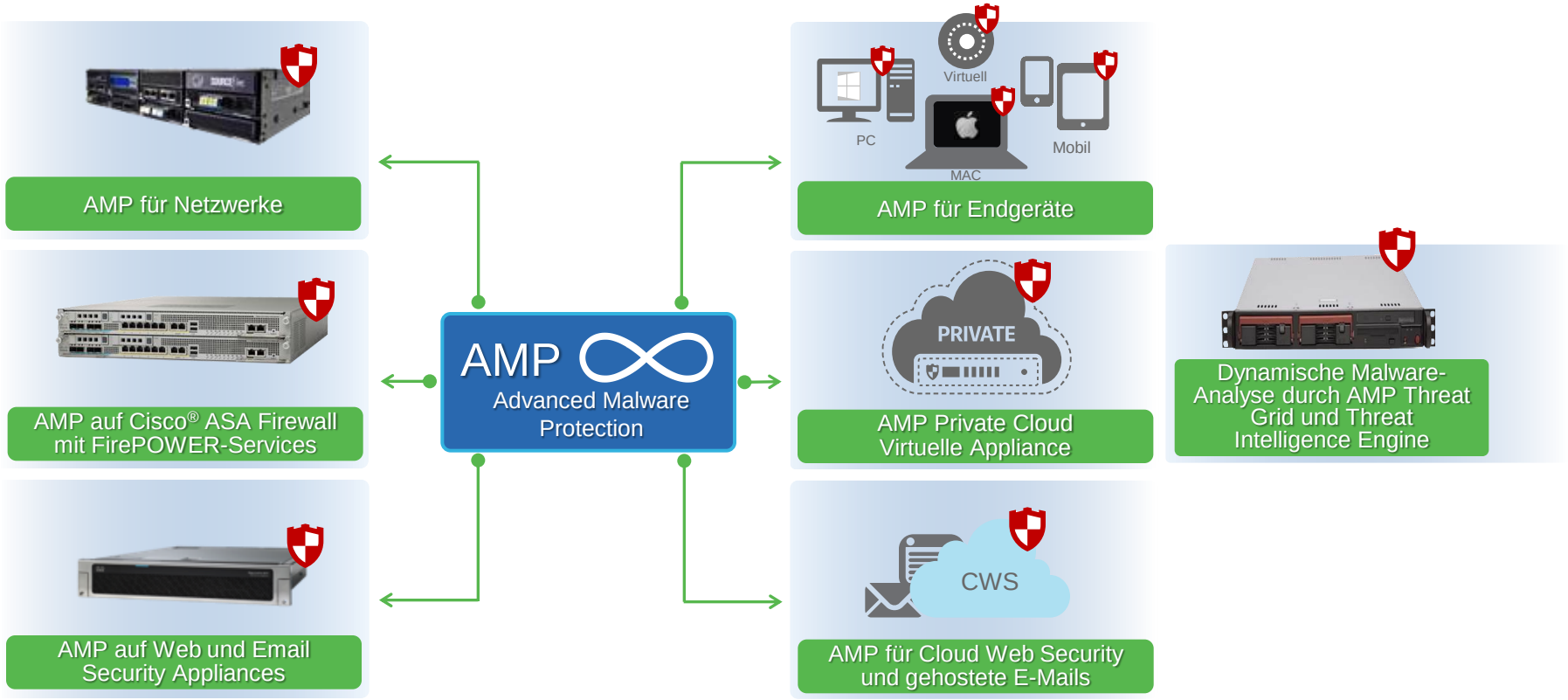
# Korrelation zwischen Netzwerk und Endgeräten ermöglicht Netzweite Kontrolle



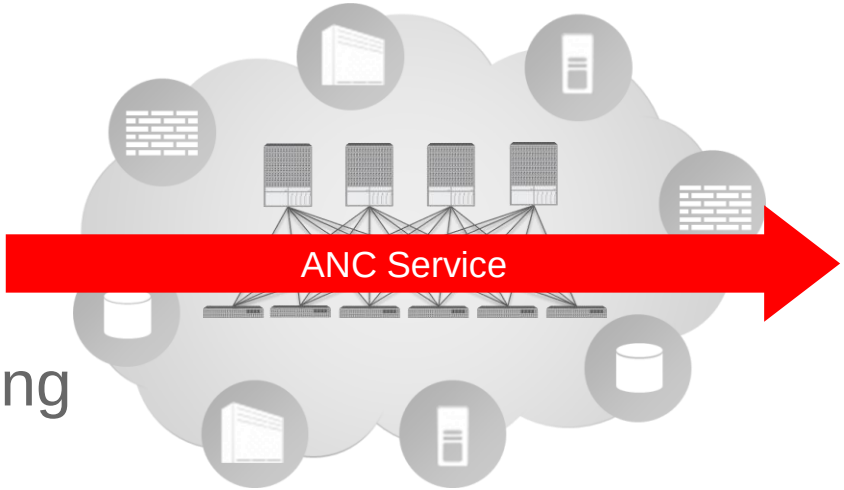
# Warum ist durchgängige Absicherung erforderlich?



# Cisco AMP Everywhere-Strategie bietet Schutz für das erweiterte Netzwerk



# Cisco Rapid Threat Containment
## Integration von Malware-Erkennung und Netzwerk Policy Kontrolle



## Angriffserkennung

- IDS Sig
- Malware
- Traffic
- Anwendungen
- ..

## Quarantine Action

- VLAN Zuweisung
- dACLs
- SGT (Secure Group Tagging)

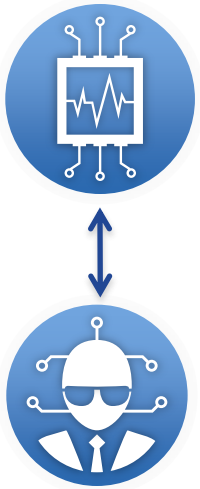
# Das Cisco Netzwerk nutzen, um gezielte Angriffe zu erkennen

Verkehrs-Anomalien erkennen

Policy Verletzungen erkennen

Tiefe Einsicht in den Netz-Verkehr

Network As A Sensor (NaaS)



Network As An Enforcer (NaaE)

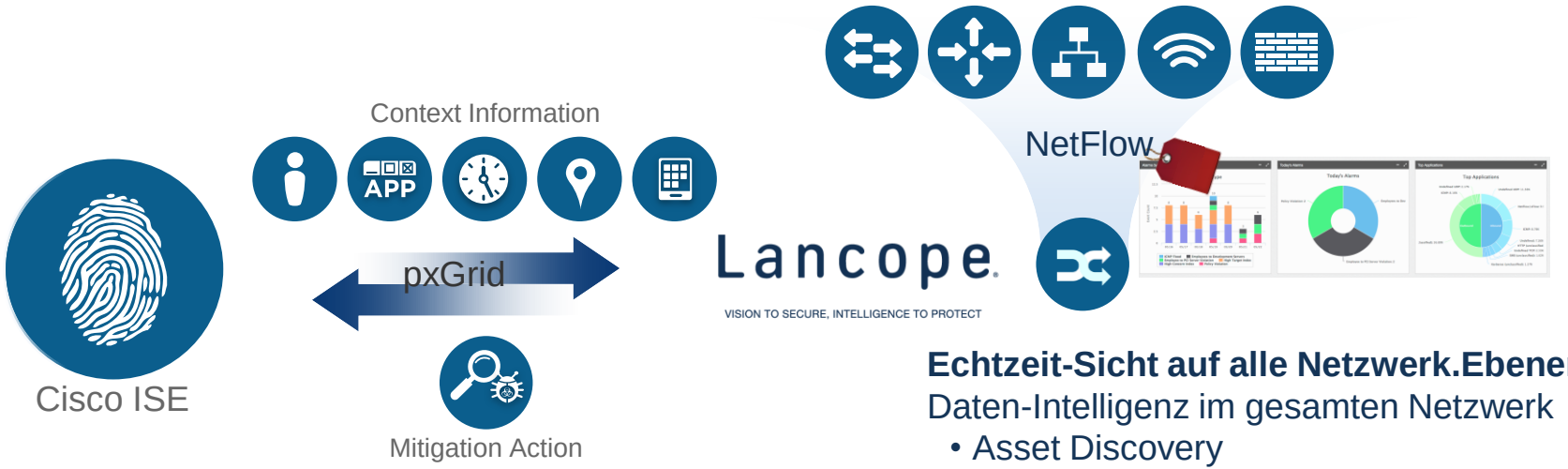
Dynamische Netzwerk-Segmentierung zur Eingrenzung von Angriffen

Isolieren von Bedrohungen

Zugangskontrolle zu gesicherten Ressourcen

Dynamische Policies & Nutzergruppen

# Network as a Sensor: Lancope StealthWatch




**Echtzeit-Sicht auf alle Netzwerk.Ebenen**

Daten-Intelligenz im gesamten Netzwerk

- Asset Discovery
- Netzwerk Profile
- Security Policy Monitoring
- Erkennen von Anomalien
- Schnelle Reaktion im Gefahrenfall

pxGrid = API

# Lancope StealthWatch
## Netzwerktransparenz durch NetFlow-Analyse

### Monitor

- Verstehen, was normal im Netzwerk ist
- Echtzeit-Abbild allen Netzerk-Verkehrs

### Detect

- Netzwerk-Anomalien erkennen
- Verhalten erkennen, das auf APTs, Insider Threats, DDoS, und Malware hinweist

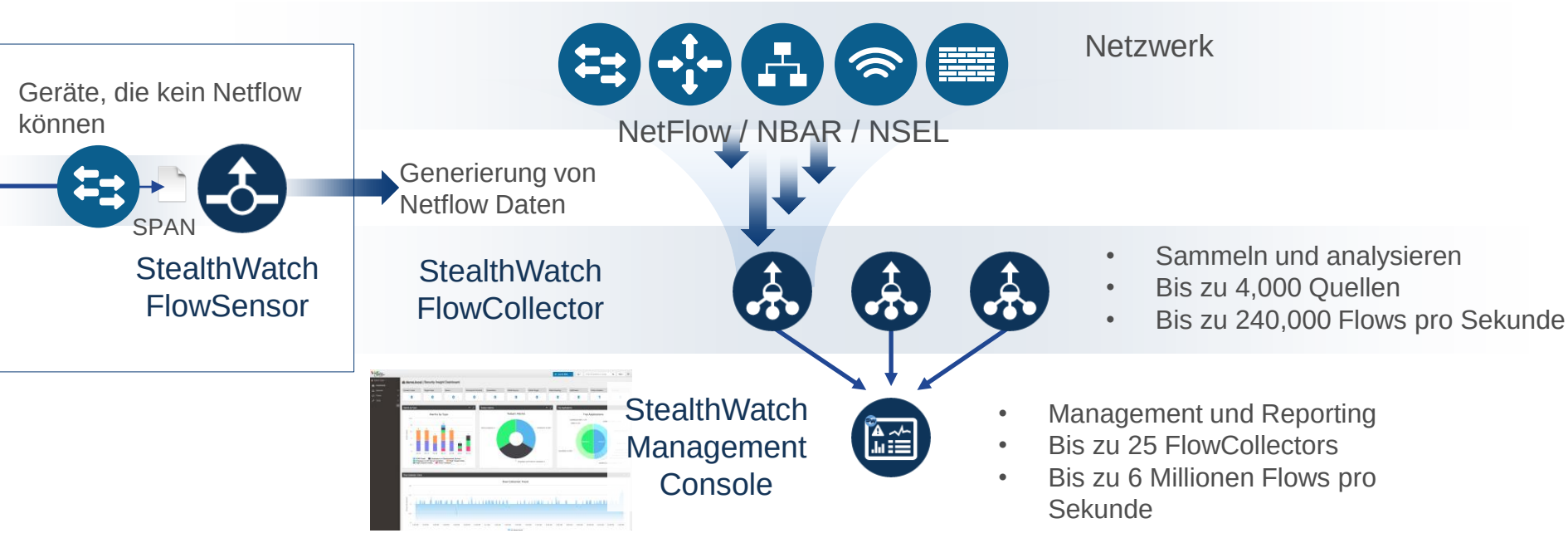
### Analyze

- Sammeln & Analysieren kompletter Netzwerk-Verläufe
- Schnellere Ursachen-Erkennung durch forensische Untersuchungen

### Respond

- Schnellere Fehlerbeseitigung und Eingrenzug von Bedrohungen
- Schnelle Reaktion auf Bedrohungen durch Isolierung von Bedrohungen via ISE

# Überblick Lancope StealthWatch



# Alarme auf Basis verhaltensbasierter Analyse

| Policy | Start Active Time | Alarm | Source | Source Host Groups | Source User ... | Source Devic... | Target | Details |
|---|---|---|---|---|---|---|---|---|
| Desktops & Trusted Wireless | Jan 3, 2013 5:45:00 PM (20 hours 33 minutes 30s ago) | Suspect Data Loss | 10.10.101.89 | Atlanta, Desktops | ud0158 | Windows7-Workstation | Multiple Hosts | Observed 5.33G bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:30:00 PM (20 hours 48 minutes 30s ago) | Suspect Data Loss | 10.50.100.64 | Desktops, New York, New York | ud0142 | Apple-iPad | Multiple Hosts | Observed 515.84M bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:25:00 PM (20 hours 53 minutes 30s ago) | Suspect Data Loss | 10.10.101.89 | Atlanta, Desktops | ud0158 | Windows7-Workstation | Multiple Hosts | Observed 4.82G bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:10:00 PM (21 hours 8 minutes 30s ago) | Suspect Data Loss | 10.50.100.64 | Desktops, New York, New York | ud0142 | Apple-iPad | Multiple Hosts | Observed 502.72M bytes. Policy maximum allows up to 500M bytes. |
| Desktops & Trusted Wireless | Jan 3, 2013 5:10:00 PM (21 hours 8 minutes | Suspect Data Loss | 10.10.101.68 | Atlanta, Desktops | uc0123r | Windows7-Workstation | Multiple Hosts | Observed 578.81M bytes. Policy maximum allows up to 500M |

| Policy | Start Active Time | Alarm | Source | Source Host Groups | Source User Name | Device Type | Target |
|---|---|---|---|---|---|---|---|
| Desktops & Trusted Wireless | Jan 3, 2013 | Suspect Data Loss | 10.10.101.89 | Atlanta, Desktops | John Smith | Apple-iPad | Multiple Hosts |



Thank you.