



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



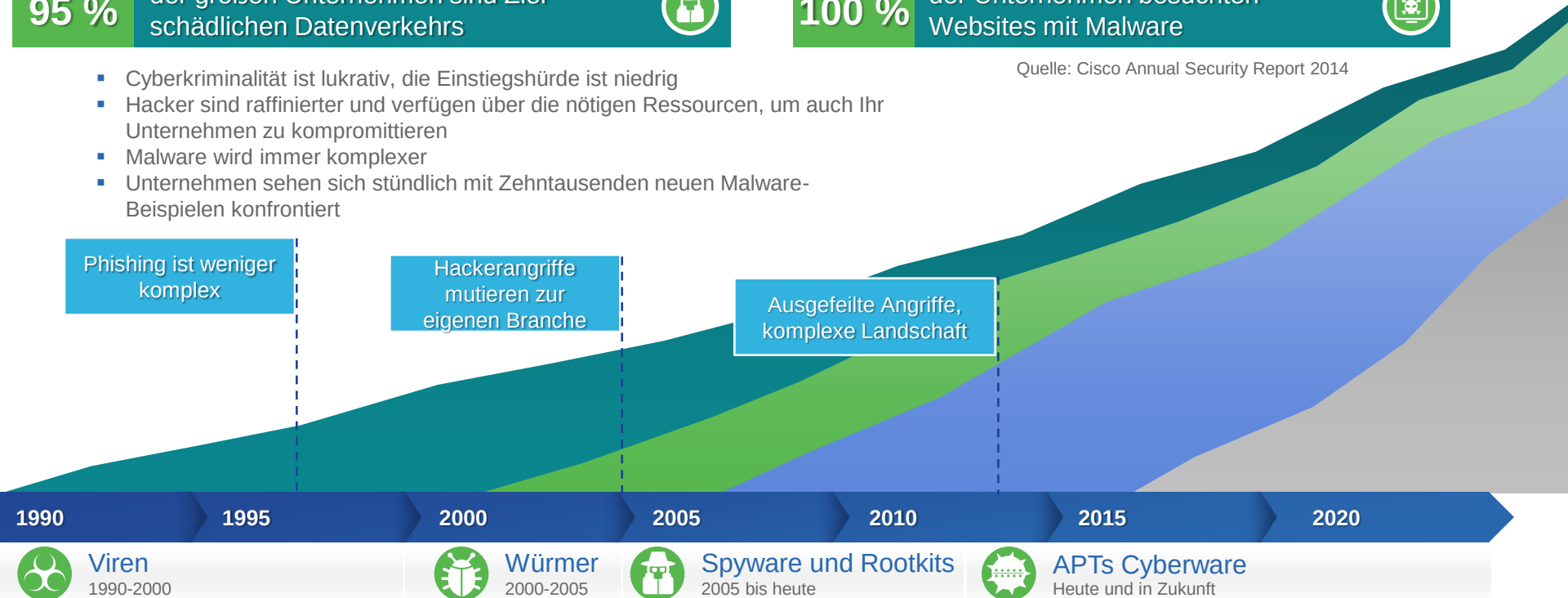
100 %

der Unternehmen besuchten
Websites mit Malware



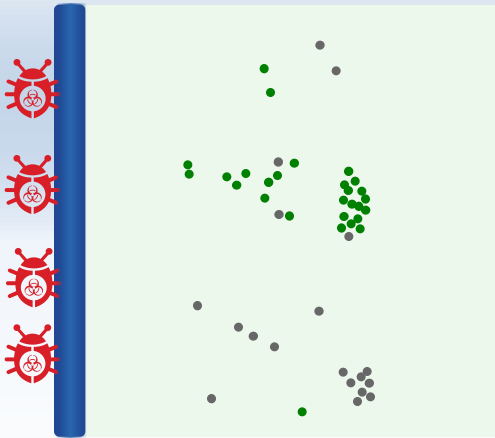
- Cyberkriminalität ist lukrativ, die Einstiegshürde ist niedrig
- Hacker sind raffinierter und verfügen über die nötigen Ressourcen, um auch Ihr Unternehmen zu kompromittieren
- Malware wird immer komplexer
- Unternehmen sehen sich stündlich mit Zehntausenden neuen Malware-Beispielen konfrontiert

Quelle: Cisco Annual Security Report 2014

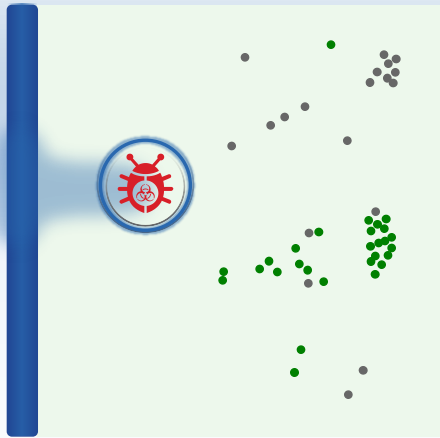


Umfassende Sicherheit bedeutet heute mehr als nur Policy Control

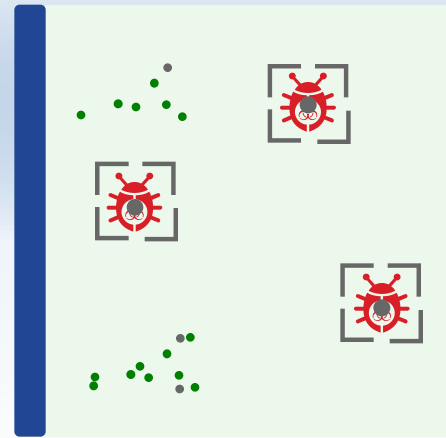
Schutz vor
Sicherheitsverletzungen



Schnelle Erkennung, Reaktion,
Beseitigung



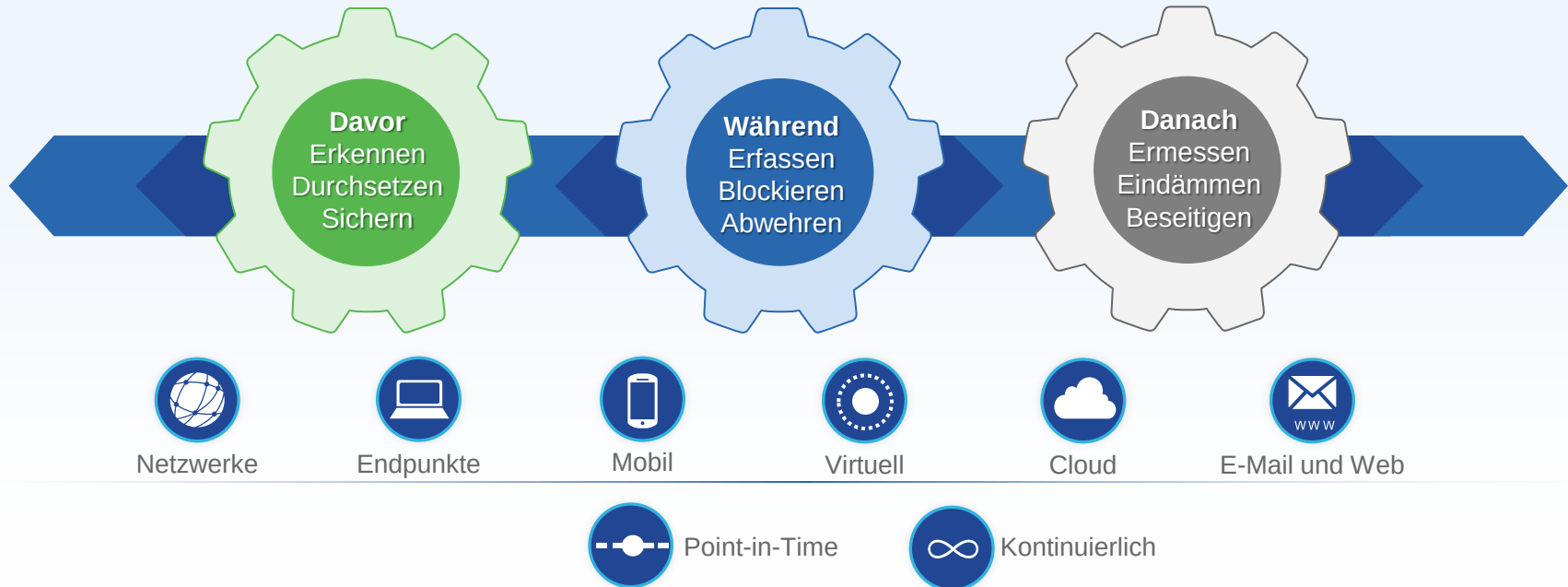
Threat Intelligence



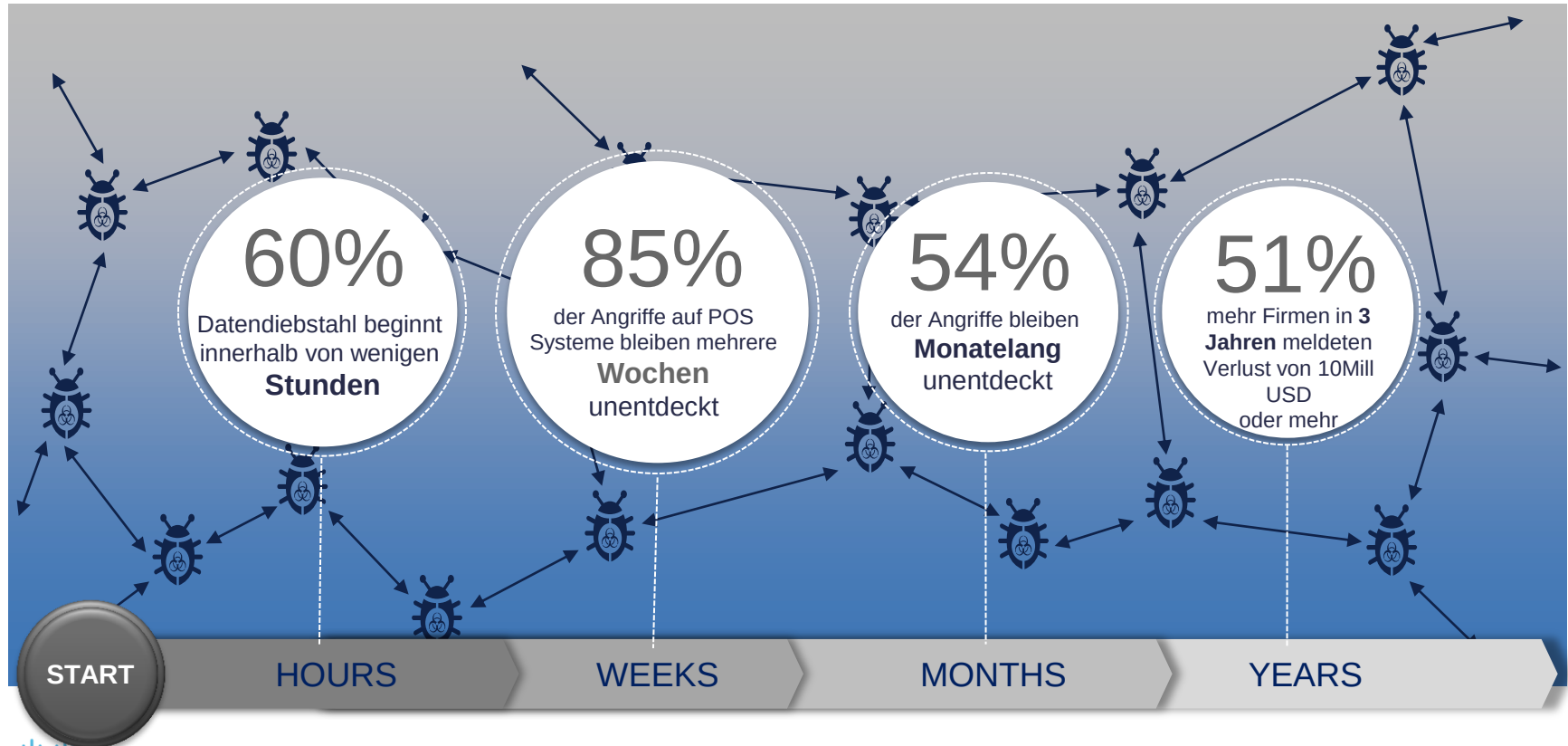
Quelle: <http://www.pcworld.com/article/2109210/report-average-of-82-000-new-malware-threats-per-day-in-2013.html>

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

Angriffscontinuum



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 Sicherheitsmechanismen durchschlüpft...
- ... weil sie gänzlich **neu** ist und als solche zunächst nicht zu erkennen ist...



Der Mehrwert von Retrospective Security

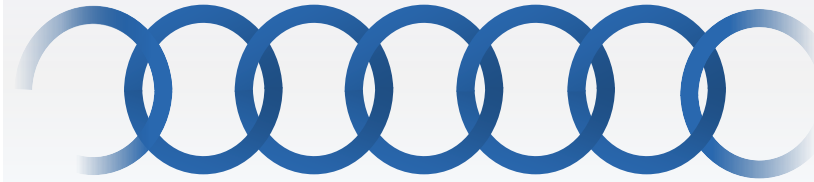
- Wenn Malware trotz aller Sicherheitsmechanismen trotzdem durchschlüpft...
- ... weil sie gänzlich **neu** ist und als solche zunächst nicht zu erkennen ist...
- ... und am nächsten Tag weiss ich, das ist Malware
- Dann möchte ich wissen
 - Woher es kam, wie kam es durch?
 - Was macht es genau?
 - Und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



Dateireputation, Sandbox-Analysen und
Verhaltenserkennung

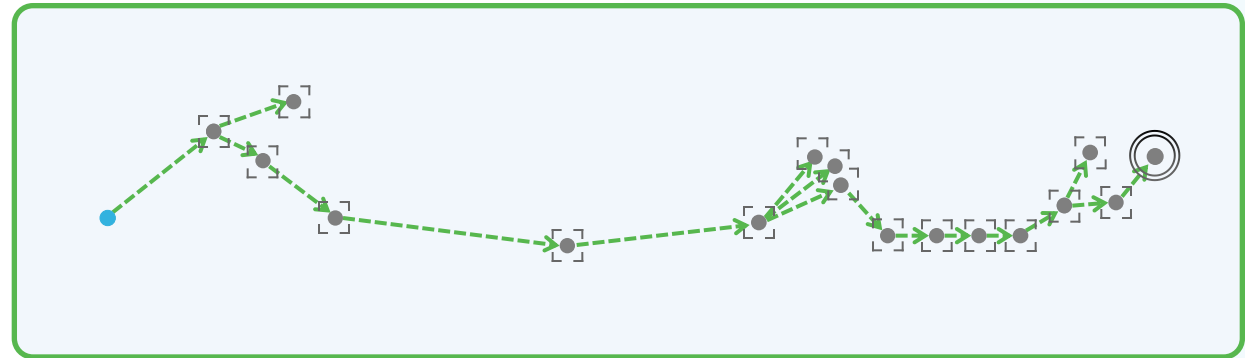
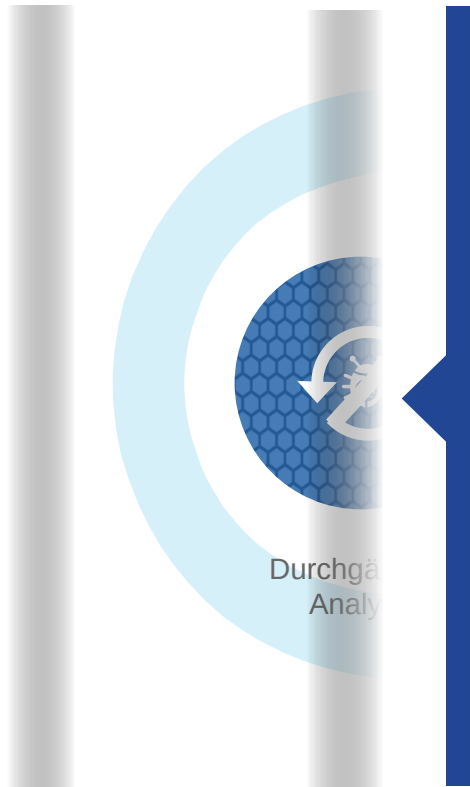
Retrospective Security



Kontinuierliche Analysen

Nur bei Cisco® AMP verfügbar

Plan B: Retrospective Security



1

Analyse wird bei
erstem Kontakt
einer Datei
durchgeführt

2

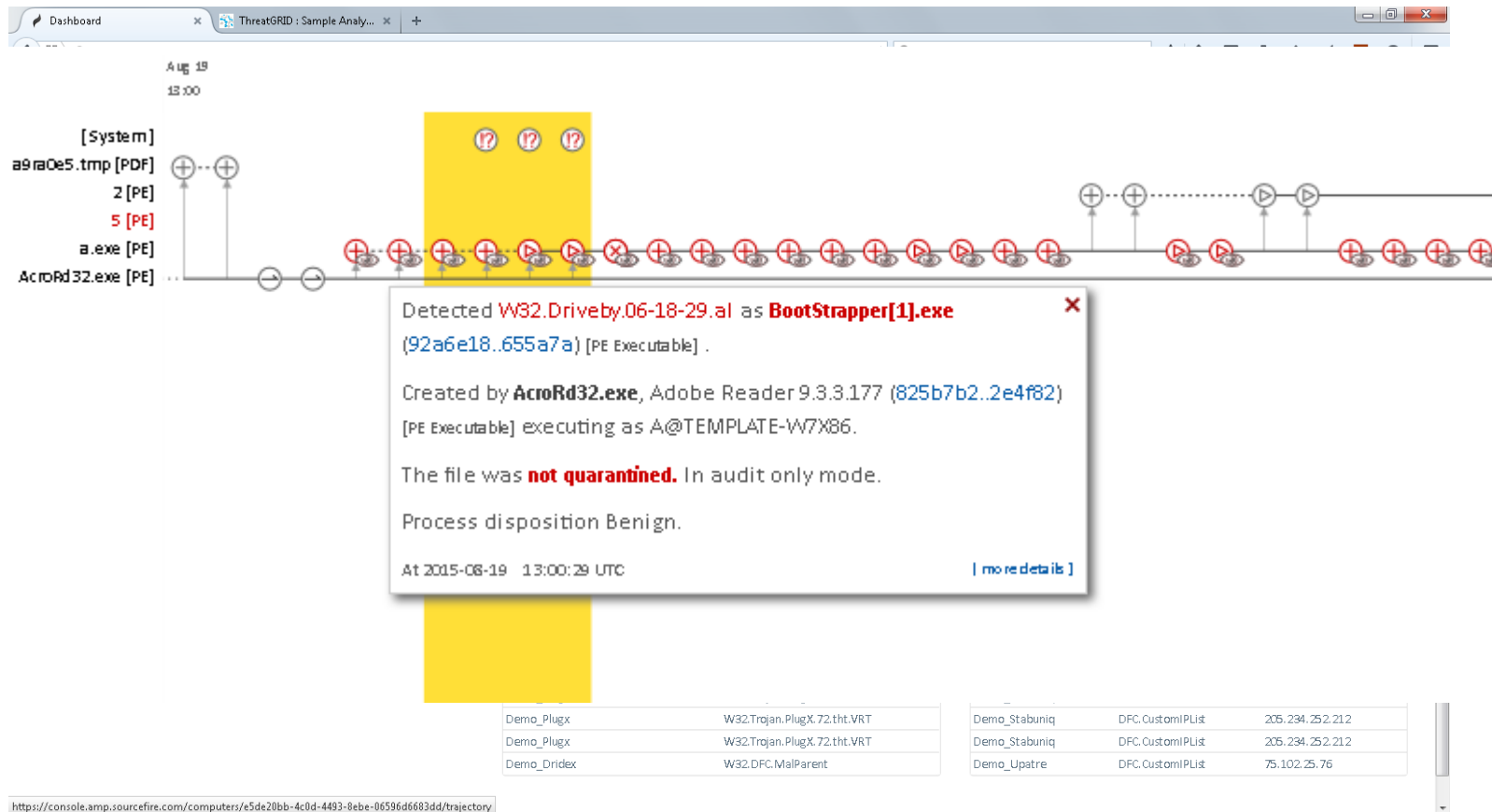
Datei wird fortlaufend
analysiert,
Änderungen an der
Einstufung werden
ggf. ermittelt

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?

Dashboard x File Trajectory x

https://console.amp.sourcefire.com/file/trajectory/b4e5c2775de098946b4e11aba138b89d42b88c1dbd4d5ec879ef6919bf018132

SOURCEfire 6 installs 932 detections (7 days) Announcements Support ? Help Log Out

Dashboard Analysis Outbreak Control Reports Management Accounts v5.2.2015081823

File Trajectory

SHA: b4e5c2775de098946b4e11aba138b89d42b88c1dbd4d5ec879ef6919bf018132

Search

Visibility

First Seen 2015-04-22 08:10:30 UTC Entry Point First Seen On Stulab / mueller-PC.stulab.cisco.com

Last Seen 2015-08-19 14:20:34 UTC

Observations 6 (as target), 14 (as source)

Created by

by file name	product	prevalence
ch1956a3d39765c54d8712d4039c3394593a974d4c321d14465d46	Microsoft Corporation, All rights reserved. 6.1.7601.17514	7
1925bcb7b15d33d3b111735595911469d032926951e6494304745b	Microsoft Office Word 15.0.4420.0	2
5f3b2d4d4e4d9f003d3f7cd220744246c73b426f90645a113b13b6f8	Microsoft Corporation, All rights reserved. 6.1.7601.16305	1
9d1a142ebd03712d3a76453abaf51e1c008b65641c73a8d0c002c52864	Microsoft Corporation, All rights reserved. 11.0.9600.11729	1

File Details

Network Profile

Trajectory

Default Group Demo_CozyDuke Demo_Uptane Demo_Zbot

Stulab RMUELLER-WS01... mueller-PC.stulab.c...

Legend: + created, A copied, → moved, ▶ executed, ↑ opened, ○ scanned, ★ advanced/tetra conviction

the file was the source of the event (red), the target was deemed malicious (red), the target was deemed benign (green)

Was genau macht die Malware?

The screenshot displays the Sourcefire console interface. At the top, there's a navigation bar with tabs for Dashboard, Device Trajectory, and File Analysis. The File Analysis tab is active, showing a search bar and a status bar with 6 installs and 395 detections. Below this, a breadcrumb trail leads to File Analysis, and a version number v5.2.2015091416 is shown. The main content area is titled 'File Analysis' and shows a specific file analysis for ID 3e3d8cb8...98863545. It includes buttons for Download Sample, Analysis Video, Download PCAP, and 37 Artifacts. A tabbed interface shows various analysis categories, with 'Analysis Report' selected. The report details the file's metadata, including its name (VeryEnticingName_enc.pdf), type (PDF document), and hashes (SHA256, SHA1, MD5). Below the report, the 'Behavioral Indicators' section highlights a critical finding: 'A Document File Established Network Communications' with a severity of 90 and confidence of 90. The description explains that the document established outbound network communications, likely to check for updates, which is a common tactic for malware. The categories listed are network, downloader, outbound, exploit, and dropper.

Dashboard | Device Trajectory | File Analysis

https://console.amp.sourcefire.com/threat_analyses/9bea85a49bc4b204b33e74470ee30b7d

6 installs
395 detections (7 days)

Announcements | Support | Help | Log Out

Dashboard | Analysis | Outbreak Control | Reports | Management | Accounts

v5.2.2015091416

File Analysis

For 3e3d8cb8...98863545

Download Sample | Analysis Video | Download PCAP | 37 Artifacts

Metadata | Behavioral Indicators | Network Activity | Processes | Artifacts | Registry Activity | File Activity

Analysis Report

ID	9bea85a49bc4b204b33e74470ee30b7d
OS	2600.xsp.080413-2111
Started	3/12/15 04:06:00
Ended	3/12/15 04:12:13
Duration	0:06:13
Sandbox	ulcer (pilot-d)
Filename	VeryEnticingName_enc.pdf
Magic Type	PDF document, version 1.5
Analyzed As	pdf
SHA256	3e3d8cb8d0e6e45eb44a2c2cf1497f673195cf6d188e3feb72ad9ea198863545
SHA1	733875cd5b77316e5065cf03bcd65621c69dc266
MD5	9ec207f4961f2f1338077c4402e3b

Behavioral Indicators

A Document File Established Network Communications Severity: 90 Confidence: 90

The submitted document was seen establishing outbound network communications. This activity could simply be embedded code that is reaching out to the vendor to check if it is running the latest version. However, it is more likely that this activity is malicious in nature. Attackers leverage vulnerabilities inside document types to establish a foothold into a victim's network. Once the system is exploited,

Categories Tags network, downloader, outbound, exploit dropper

Wie können wir den Angriff stoppen?

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

The screenshot shows the Sourcefire web interface. At the top, the Sourcefire logo is on the left, and '6 installs', '395 detections (7 days)', and 'Announceme' are on the right. Below this is a navigation bar with 'Dashboard', 'Analysis', 'Outbreak Control', 'Reports', 'Management', and 'Accounts'. The main section is titled 'File Analysis' and shows a file ID '3e3d8cb8...98863545'. A dropdown menu is open, listing actions: 'Download', 'Download Analysis Video', 'Download PCAP', 'Copy SHA-256', 'Search', 'View Full SHA-256', 'File Analysis', 'File Trajectory', 'Simple Detection' (highlighted), 'Application Blocking', 'Whitelist', 'Back', 'Forward', and 'Reload'. The 'Simple Detection' sub-menu is also open, showing 'InstantBlockList' (highlighted), 'Malware', 'SimpleMalware', and 'Create New Set'. Below the menu, file details are visible: 'Duration: 0:06:13', 'Sandbox: ulcer (pilot-d)', 'Filename: VeryEnticingName_enc.pdf', 'Magic Type: PDF document, version 1.5', and 'Analyzed: pdf'.

Korrelation zwischen Netzwerk und Endgeräten ermöglicht Netzweite Kontrolle

OverviewAnalysisPoliciesDevicesObjectsFireAMP

Context ExplorerConnectionsIntrusionsFiles > Network File TrajectoryHostsUsersVulnerabilitiesCorrelationCustomSearch

Network File Trajectory for 0517f034...588e1374

File SHA-2560517f034...588e1374
File Name[WindowsMediaInstaller.exe](#)
File Type[MSEXE](#)
File Category[Executables](#)
Current Disposition **Threat Score** High

First Seen2013-12-06 10:57:13 on [10.4.10.183](#)
Last Seen2013-12-06 18:17:27 on [10.4.10.183](#)
Event Count7
Seen On4 hosts
Seen On Breakdown2 senders → 3 receivers

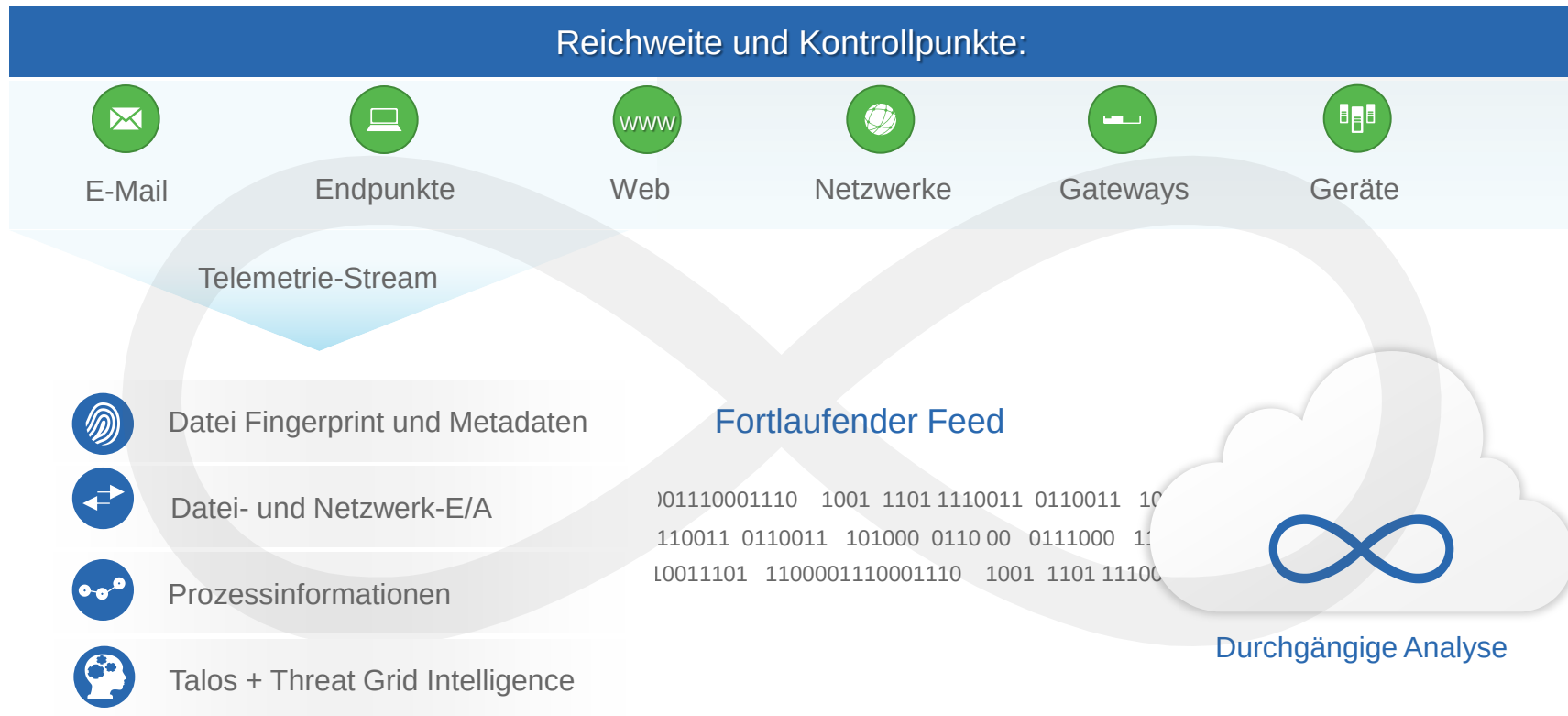
Trajectory

Events Transfer Block Create Move Execute Scan Retrospective Quarantine
Dispositions Unknown Malware Clean Custom Unavailable

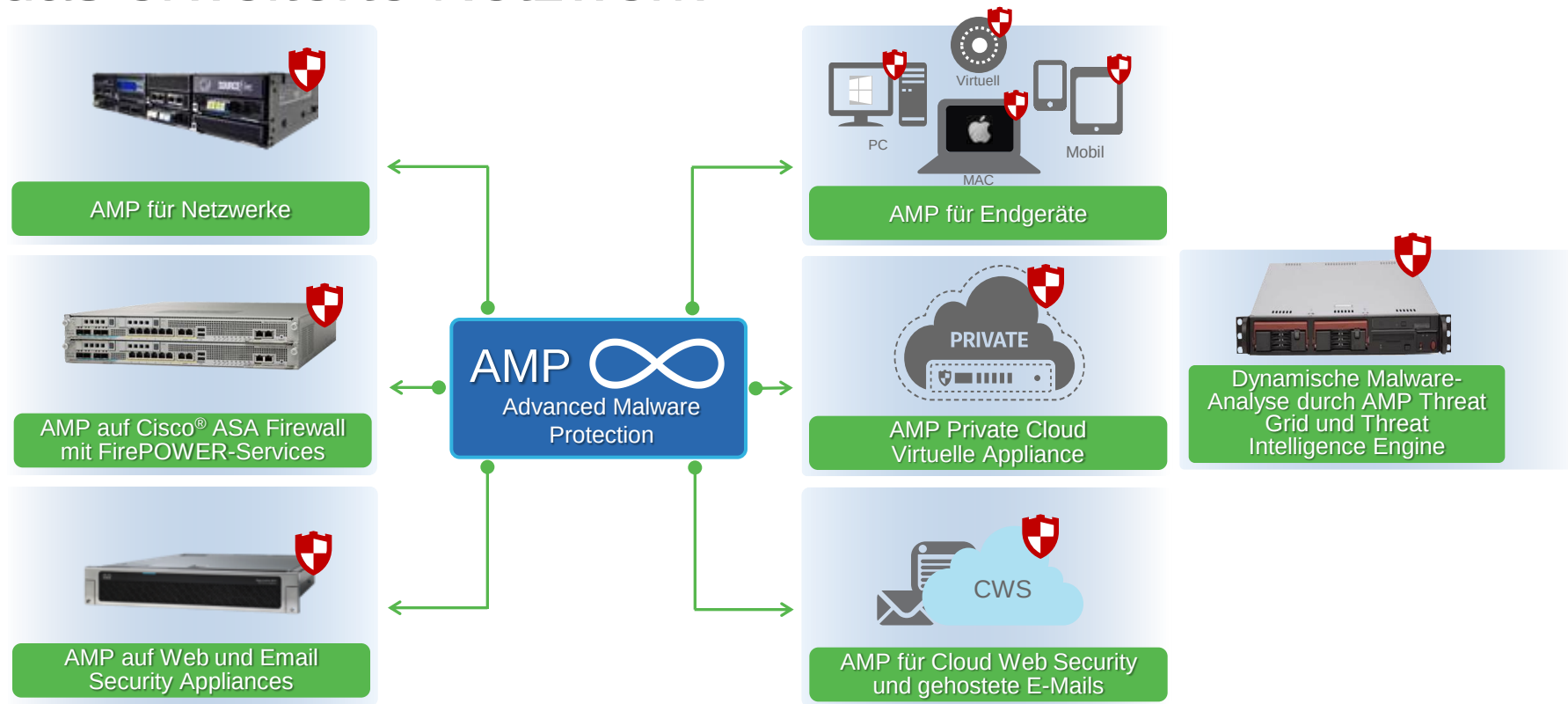
Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Warum ist durchgängige Absicherung erforderlich?

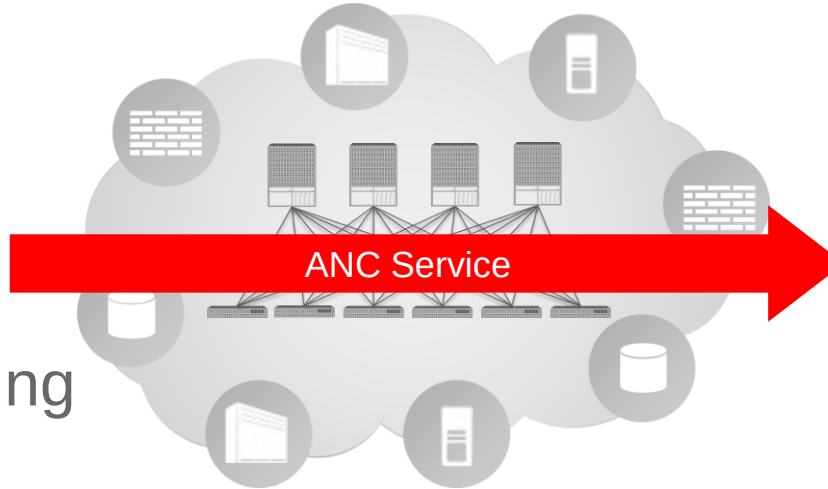


Cisco AMP Everywhere-Strategie bietet Schutz für das erweiterte Netzwerk



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)

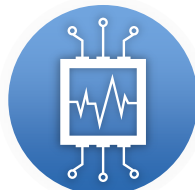
Das Cisco Netzwerk nutzen, um gezielte Angriffe zu erkennen

Verkehrs-Anomalien erkennen

Policy Verletzungen erkennen

Tiefe Einsicht in den Netz-
Verkehr

Network As A Sensor (NaaS)



Network As An Enforcer (NaaE)

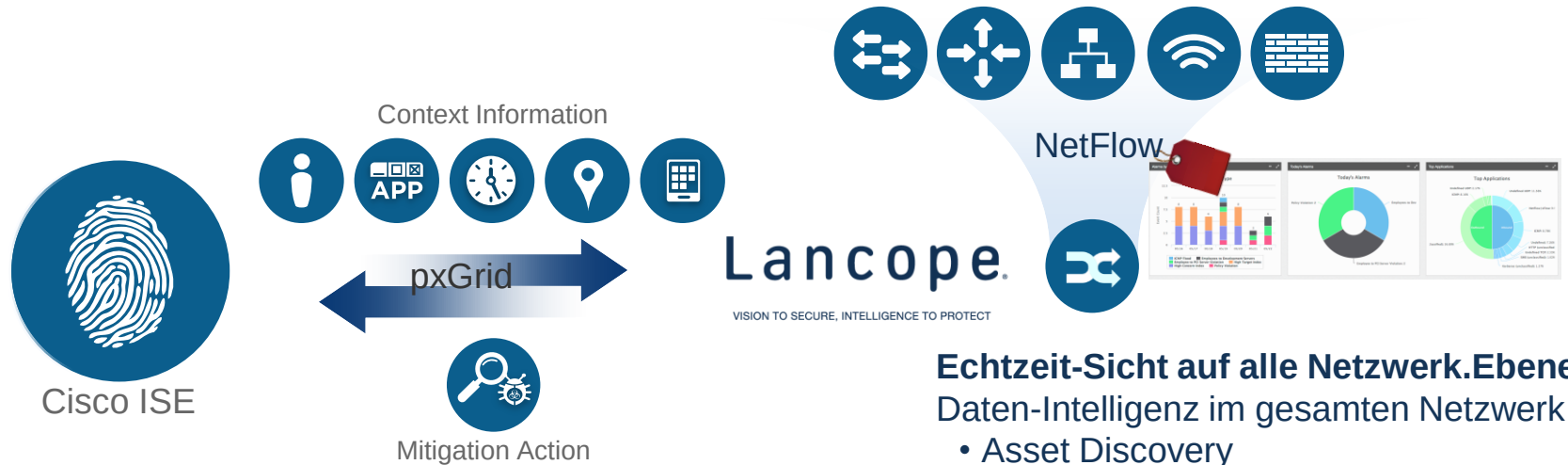
Dynamische Netzwerk-
Segmentierung zur
Eingrenzung von Angriffen

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

Lancope StealthWatch

Netzwerktransparenz durch NetFlow-Analyse

Monitor



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

Detect



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

Analyze



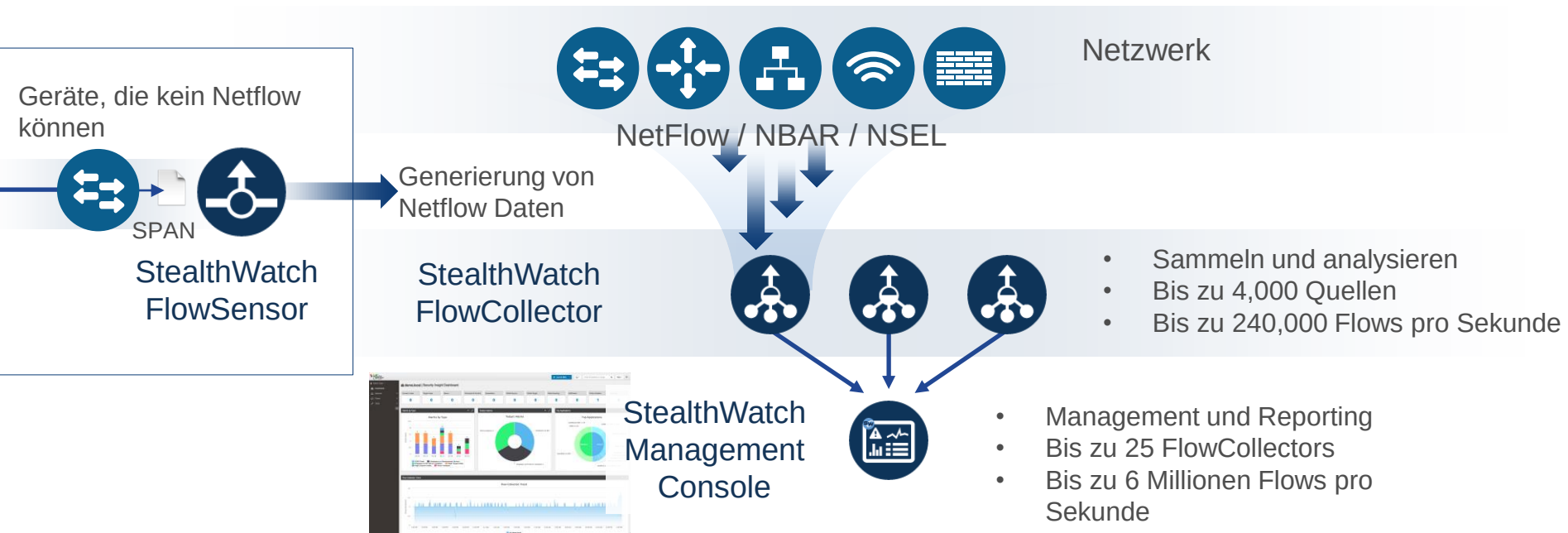
- Sammeln & Analysieren kompletter Netzwerk-Verläufe
- Schnellere Ursachen-Erkennung durch forensische Untersuchungen

Respond



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

Überblick Lancope StealthWatch



Alarmer auf Basis verhaltensbasierter Analyse

	Policy	Start Active Time	Alarm	Source	Source Host Groups	Source User ...	Source Device ...	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-Wor kstation	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-Wor kstation	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 30s ago)	Suspect Data Loss	10.10.101.68	Atlanta, Desktops	uc0123r	Windows7-Wor kstation	Multiple Hosts	Observed 578.81M bytes. Policy maximum allows up to 500M bytes.

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.

