

Cybowall Produktübersicht





KERNKOMPETENZEN

- Unternehmen mit in verschiedenen vertikalen Märkten führenden Produkten
- Bereitstellung und Verwaltung zahlreicher großformatiger Cloud-Plattformen für Unternehmen
- Managed Services, Unternehmenssoftware, SaaS
- Telekommunikations-Installation weltweit
- Innovatives, führendes Unternehmen im Bereich Anti-Botnet-Aktivität



PRODUKTREIHEN

- Cybowall:
 - Fortschrittliche Bedrohungserkennung
- PineApp Mail Secure:
 - Fortschrittliche Nachrichtenlösung
- CyboCloud:
 - Lösung für Cloud Messaging
- Outbound Spam Guard (OSG):
 - IP Blacklisting-Schutz für Telekommunikationsunternehmen



FAKTEN UND DATEN

- Hauptsitz sowie Forschung und Entwicklung in Israel
- In Privatbesitz
- Globales Unternehmen mit Partnern in Nordamerika, Europa, der Gemeinschaft Unabhängiger Staaten und Fernost
- Breite Installationsbasis in über 60 Ländern

HERAUSFORDERUNGEN FÜR CYBERSECURITY BEI KMU

RESSOURCEN UND FACHWISSEN

KMU stehen den gleichen Bedrohungen mit geringeren Ressourcen und weniger internem Fachwissen gegenüber

ERHOLUNG VON CYBER-ANGRIFFEN

33 % aller KMU benötigten 3 Tage, um sich von einem Angriff zu erholen. 60 % aller KMU machen innerhalb von 6 Monaten nach einem Angriff geschäftliche Verluste

KOSTEN VON DATENSCHUTZVERLETZUNGEN

Die Erholung von einer Datenschutzverletzung kann ein kleines bis mittelgroßes Unternehmen zwischen 36.000 und 50.000 US-Dollar kosten



GLOBALES ANGRIFFSZIEL

43 % aller globalen Angriffe zielen auf KMU mit weniger als 250 Mitarbeitern ab (9 % mehr als im Vorjahr)

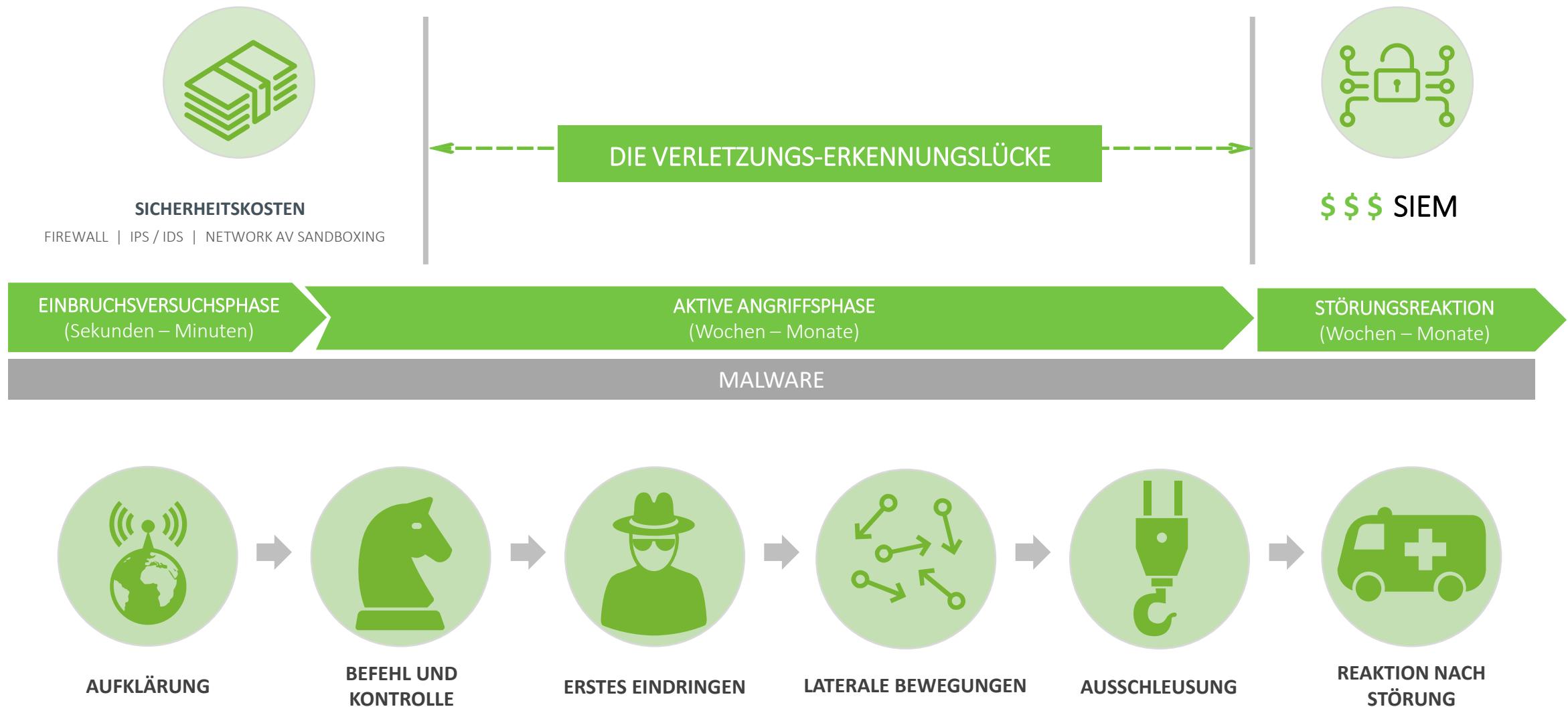
„SPEAR PHISHING“-ANGRIFFE

Steigerung um 55 % gegenüber dem Vorjahr bei „Spear Phishing“-Angriffen auf Unternehmen aller Art

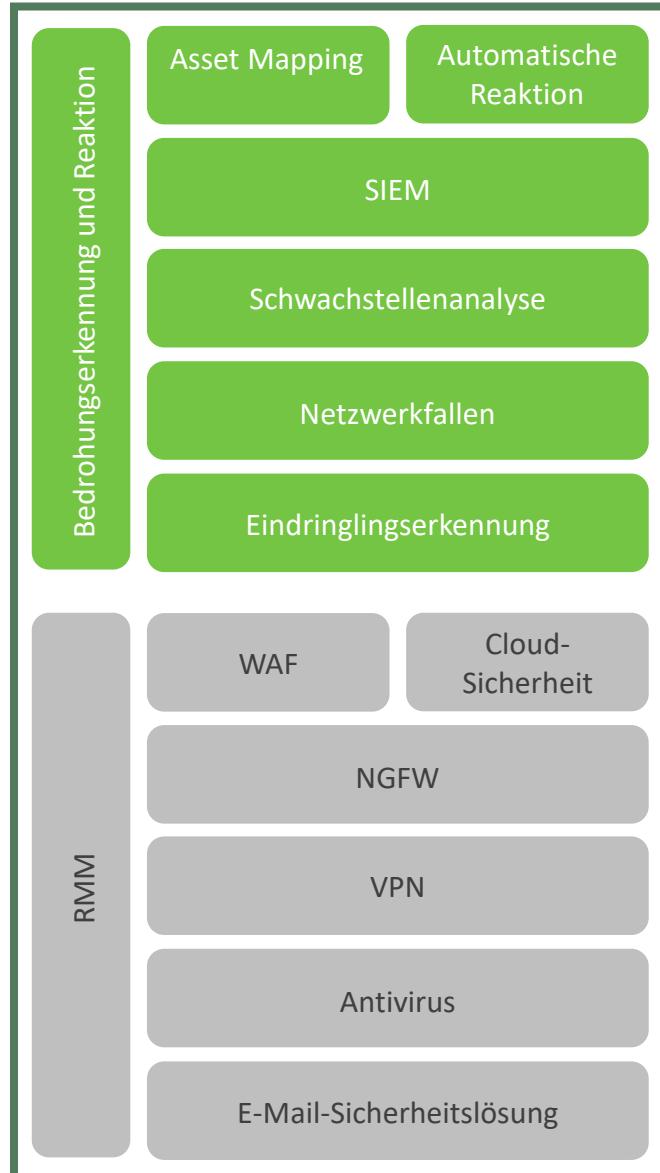
AKTIONSPLAN FÜR CYBER-ANGRIFFE

8 von 10 KMU haben nicht einmal einen grundlegenden Reaktionsplan gegen Cyber-Angriffe.

ERKENNUNGSLÜCKE FÜR DATENSICHERHEITS BEDROHUNGEN



CYBONET MARKTCHANCEN FÜR EINE EINZELNE KMU-LÖSUNG

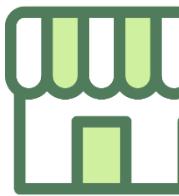


Typisches Unternehmens-Sicherheitspaket



- Kostenintensiv
- Erfordert Betreuung durch eigenen Analysten/ Datensicherheitsbeauftragten (CISO)/EDV-Sicherheitszentrum (SOC)

Typisches KMU-Sicherheitspaket

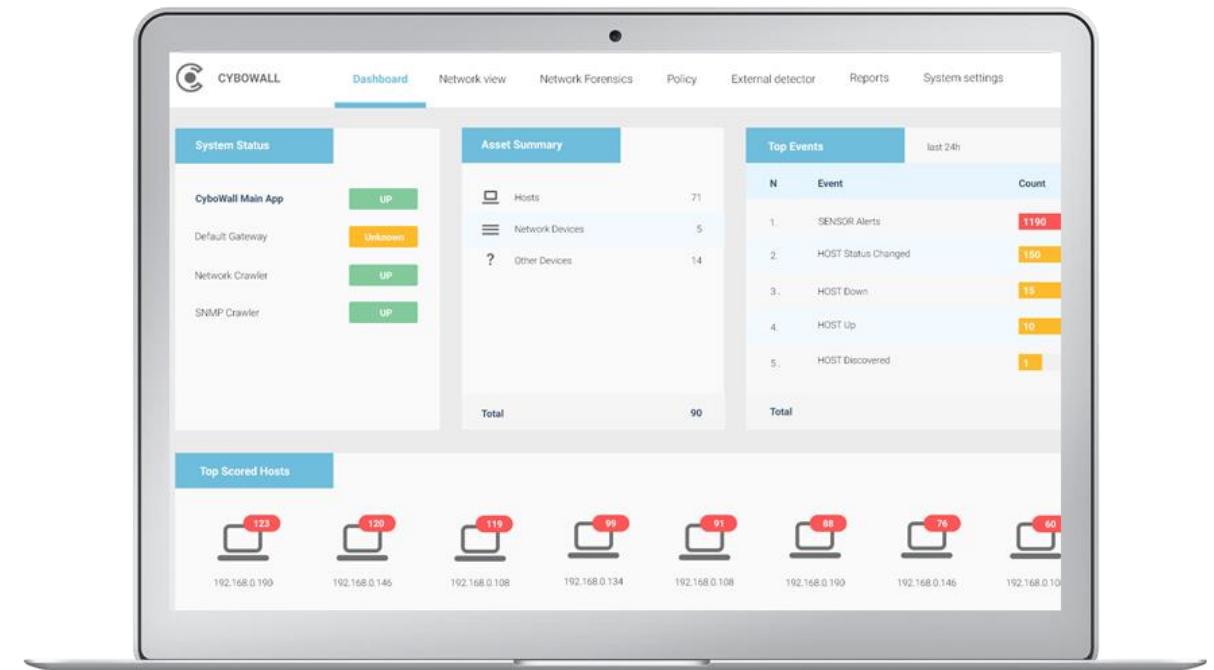


- Kostengünstig für KMU
- Verwaltung durch KMU-Ressourcen möglich

CYBONET VORSTELLUNG CYBOWALL

Erkennung von Eindringlingen, Netzwerk-Sichtbarkeit und Schwachstellen-Management für kleine und mittelgroße Unternehmen

- Schnelle Erkennung potentieller Schwachstellen und aktueller Datenschutzverletzungen
- Potentielle Schwachstellen erkennen und minimieren
- Strukturierung und Berichterstattung entsprechend von Richtlinien und Zertifikaten (DSGVO, PCI-DSS, ISO etc.)
- Aufzeichnung und Analyse aller Ereignisse und Störungen innerhalb des Netzwerkes zur weiteren Prüfung



CYBOWALL LÖSUNGSVORTEILE

Erkennung lateraler Bewegungen

zum Fixieren von Eindringlingen,
die bereits in das Sicherheitssystem
eingedrungen sind



Endpoint-Manipulation und
Malware aufhalten
durch Netzwerk- und Endpunkt-
Erkennung

Identifikation von Schwachstellen

zum Festlegen der
Prioritäten für Patches



Mapping von Network Assets
für bessere Sichtbarkeit mit einer
detailgenauen Endpunktübersicht

Erkennung von aktiven Sicherheitsverstößen

Decken Sie Netzwerkangriffe
schnellstmöglich auf und reduzieren
Sie damit schädigende Auswirkungen



Einhaltung von Regulierungsvorgaben
für DSGVO, ISO, PCI-DSS, HIPAA etc.

CYBOWALL ÜBERSICHT

1 Netzwerk-Sensor

- Netzwerk-Sichtbarkeit
- Port mirroring/TAP
- IDS auf Netzwerkebene
- Eingehender und ausgehender Traffic

2 Netzwerk-Fallen

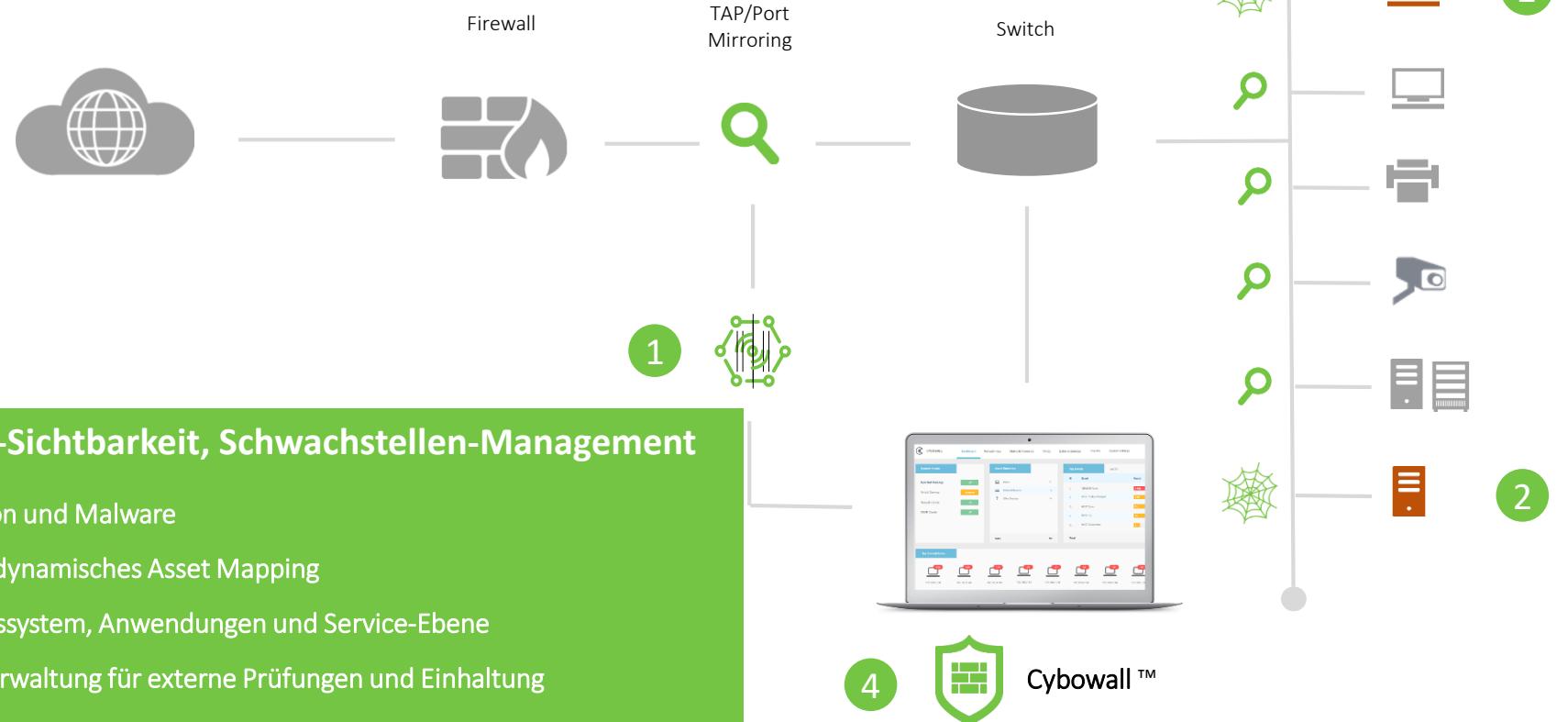
- Verteiltes Täuschungsnetz
- Laterale Bewegungen

3 Autonomer Endpunkt-Scan

- Asset Mapping und Port-Profile
- Nutzung von WMI für Registry - und Verfahrensprüfungen
- Abgleich forensischer Daten mit IOC

4 Verletzungserkennung, Netzwerk-Sichtbarkeit, Schwachstellen-Management

- Identifikation von Endpunkt-Manipulation und Malware
- Vollständige Netzwerk-Sichtbarkeit und dynamisches Asset Mapping
- Schwachstellenmanagement für Betriebssystem, Anwendungen und Service-Ebene
- Integrierte Berichterstattung und Log-Verwaltung für externe Prüfungen und Einhaltung von Vorgaben



CYBOWALL FUNKTIONEN

Asset Mapping

Kontinuierlich aktualisierte Liste aller Endpunkte, einschließlich Port-Profile und Aktivitäten

Eindringungserkennung

Vollständige Sichtbarkeit von eingehendem und ausgehendem Traffic ohne Störungen zu verursachen

SIEM

Log-Management, Ereignis-Management, Ereignis-Korrelationsabgleich und Berichterstattung, um Verstöße gegen Richtlinien zu melden und entsprechende Reaktionen zu aktivieren

Netzwerk-Fallen

Ermöglichen Einblicke in laterale Bewegungen zwischen Endpunkten und Erkennung von Bedrohungen innerhalb des Netzwerkes durch Funktion als „Fallstrick“ für aktive Angriffe

Schwachstellen-Prüfung

Überwachung von Geschäftsanlagen und Erkennung anfälliger Systeme innerhalb des Netzwerkes, einschließlich Risikolevel, zur Einsatz-Priorisierung von Patches

Malware-Jäger

Erkennung bösartiger Dateien und deren Lokalisierung im Netzwerk



CYBOWALL PREISGESTALTUNG UND LIZENSIERUNG



SYSTEMLIZENZ

Einmalige Systemlizenzgebühr für Erstinstallation



PREISGESTALTUNG PRO ENDPUNKT

Berechnet pro Endpunkt mit Standard-Preis für alle Endpunktarten, einschließlich Arbeitsplätze, Server etc.



SUPPORT

Der Endpunkt-Preis versteht sich inkl. Kundenservice während der Geschäftszeiten



ERNEUERUNG

Erneuerungsgebühr basierend auf der Anzahl der Endpunkte mit Support

CYBOWALL PREISE (EUR)

	Stufe 1 – Anzahl Endpunkte	Stufe 2 – Anzahl Endpunkte	Stufe 3 – Anzahl Endpunkte	Stufe 4 – Anzahl Endpunkte	Stufe 5 – Anzahl Endpunkte	Stufe 6 – Anzahl Endpunkte
	100	101 - 250	251 - 500	501 - 750	751 - 1000	1001+
Systemlizenz	€ 4,217	€ 4,217	€ 4,217	€ 4,217	€ 4,217	€ 4,217
Pro Endpunkt, pro Jahr + Support	€ 59	€ 50	€ 38	€ 34	€ 30	€ 17
Pro Endpunkt – 1 J Erneuerung + Support	€ 59	€ 50	€ 38	€ 34	€ 30	€ 17
Pro Endpunkt – 2 J Erneuerung + Support	€ 100	€ 85	€ 65	€ 58	€ 51	€ 29
Pro Endpunkt – 3 J Erneuerung + Support	€ 133	€ 113	€ 86	€ 77	€ 68	€ 38

CYBOWALL INTUITIVE ÜBERWACHUNG

CYBOWALL

Dashboard Network View Network Forensics Policy Reports System settings

User: Admin Host: [Change](#)

System status	
Cybowl main app	UP
Advanced IDS	Unknown
Asset builder	Unknown
SNMP connector	Unknown
CPU usage	5%
Memory usage	70%
Bandwidth (Mbps)	15
Disk size	1 Tb
Disk status	Normal

Asset summary	
General purpose	60
Broadband router	2
Switch	2
Total	64

Top events last 24h		
N	Event	Count
1.	WMI	16
2.	DNS malware	2
Total		18

Top scored hosts last 24h	
Your network is secure. Scored hosts not found.	

Top hosts last 24h									
N	Host	Name	Events	N	Host	Name	Events		
1.		192.168.17.4	EXCHANGE2010	7	4.		192.168.17.3	ADDO	2
2.		192.168.17.15	DESKTOP-WIN10	4	5.		192.168.17.218	RNDWIN7PC	1
3.		192.168.17.106	VOTIROSRV	4					

Threat GeoMap last 24h	
Outbound threats	
System configuration was modified. When you are ready to apply changes click here.	
Apply changes	

CYBOWALL INTUITIVE ÜBERWACHUNG

 CYBOWALL

Dashboard Network View Network Forensics Policy Reports System settings User: Admin Host: ▾

Threat GeoMap last 24h Outbound threats 

JS map by amCharts



Event timeline last 24h 

JS chart by amCharts



Time	Events
18:00 Sep 26	2
21:00 Sep 26	1
01:00 Sep 27	4
03:00 Sep 27	1
06:00 Sep 27	1
09:00 Sep 27	1
12:00 Sep 27	1
15:00 Sep 27	1

System configuration when you are ready to a changes click here

CYBOWALL IDENTIFIKATION VON SCHWACHSTELLEN

CYBOWALL				Dashboard	Network View	Network Forensics	Policy	Reports	System settings	User: Admin	Host: 			
19.	 General purpose	192.168.17.36			<div style="background-color: #e0f2e0; padding: 5px; border-radius: 5px; width: fit-content; margin: auto;"><p>Details of 192.168.17.106</p><p>Linux</p><p>Linux</p><p>Host details Open ports Hardware Software Vulnerability</p><p>Common Vulnerabilities and Exposures</p><table border="1" style="width: 100%; border-collapse: collapse;"><thead><tr><th>Application</th><th>Details</th><th>Top score</th></tr></thead><tbody><tr><td>Cisco WebEx Meetings</td><td>CVE-2017-3823</td><td>9.3</td></tr></tbody></table><p>Description: An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. A vulnerability in these Cisco WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows. The vulnerability is a design defect in an application programming interface (API) response parser within the extension. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.</p><p>Links:</p><p>http://www.securityfocus.com/bid/95737 https://0patch.blogspot.com/2017/01/micropatching-remote-code-execution-in.html https://bugs.chromium.org/p/project-zero/issues/detail?id=1096 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170124-webex</p><p>CWE: CWE-119</p><p>Cvssv3:</p><p>Attack vector: NETWORK Attack complexity: LOW Privileges required: NONE User interaction: REQUIRED Confidentiality: HIGH Integrity: HIGH Availability: HIGH</p><p>Cvssv2:</p><p>Attack vector: NETWORK Attack complexity: MEDIUM Confidentiality: COMPLETE Integrity: COMPLETE Availability: COMPLETE</p></div>	Application	Details	Top score	Cisco WebEx Meetings	CVE-2017-3823	9.3	Cybernet (192.168.17.0/24)		Details 
Application	Details	Top score												
Cisco WebEx Meetings	CVE-2017-3823	9.3												
20.	 General purpose	192.168.17.37				Cybernet (192.168.17.0/24)		Details 						
21.	 General purpose	192.168.17.38				Cybernet (192.168.17.0/24)		Details 						
22.	 General purpose	192.168.17.39				Cybernet (192.168.17.0/24)		Details 						
23.		192.168.17.42				Cybernet (192.168.17.0/24)		Details 						
24.	 General purpose	192.168.17.46				Cybernet (192.168.17.0/24)		Details 						
25.		192.168.17.47				Cybernet (192.168.17.0/24)		Details 						
26.		192.168.17.48				Cybernet (192.168.17.0/24)		Details 						
27.		192.168.17.49				Cybernet (192.168.17.0/24)		Details 						
28.		192.168.17.50				Cybernet (192.168.17.0/24)		Details 						
29.	 General purpose	192.168.17.51				Cybernet (192.168.17.0/24)		Details 						
30.	 General purpose	192.168.17.66				Cybernet (192.168.17.0/24)		Details 						
31.	 General purpose	192.168.17.69				Cybernet (192.168.17.0/24)		Details 						
32.	 General purpose	192.168.17.93				Cybernet (192.168.17.0/24)		Details 						
33.	 General purpose	192.168.17.99				Cybernet (192.168.17.0/24)		Details 						
34.	 Broadband router	192.168.17.101				Cybernet (192.168.17.0/24)		Details 						
35.	 General purpose	192.168.17.104				Cybernet (192.168.17.0/24)		Details 						
36.	 General purpose	192.168.17.105				Cybernet (192.168.17.0/24)		Details 						
37.	 General purpose	192.168.17.106				Cybernet (192.168.17.0/24)		Details 						
38.	 General purpose	192.168.17.107				Cybernet (192.168.17.0/24)		Details 						
39.	 General purpose	192.168.17.109				Cybernet (192.168.17.0/24)		Details 						
40.	 General purpose	192.168.17.114				Cybernet (192.168.17.0/24)		Details 						
41.	 General purpose	192.168.17.130				Cybernet (192.168.17.0/24)		Details 						
42.	 General purpose	192.168.17.131				Cybernet (192.168.17.0/24)		Details 						
43.	 General purpose	192.168.17.133				Cybernet (192.168.17.0/24)		Details 						
44.	 General purpose	192.168.17.140				Cybernet (192.168.17.0/24)		Details 						
45.	 General purpose	192.168.17.170				Cybernet (192.168.17.0/24)		Details 						
46.	 General purpose	192.168.17.171				Cybernet (192.168.17.0/24)		Details 						
47.	 General purpose	192.168.17.181				Cybernet (192.168.17.0/24)		Details 						
48.	 General purpose	192.168.17.183				Cybernet (192.168.17.0/24)		Details 						
49.	 General purpose	192.168.17.200				Cybernet (192.168.17.0/24)		Details 						
50.	 General purpose	192.168.17.201				Cybernet (192.168.17.0/24)		Details 						

CYBOWALL EINSTIEGSFRAGEN

- **Geschätzte Endpunkt-Gesamtzahl?**
Dies beinhaltet Drucker, Server, Arbeitsplätze etc. Schätzungen sind mehr als ausreichend
- **Gesamtanzahl aller Netzwerke?**
Bitte alle VLANs etc. einrechnen
- **Marke und Modell des Core Switch?**
Bitte so detailliert wie möglich angeben
- **Zugriff auf und/oder Möglichkeit von Port Mirroring?**
- **Prozentsatz der Arbeitsplätze und Server, die ein Microsoft-Betriebssystem nutzen?**
Schätzungen sind mehr als ausreichend
- **Haben Sie Zugriff auf den WMI-Zugang und/oder die Fähigkeit, diesen zu verwalten?**



CYBONET
R&D Center
Matam, Building 23,
P.O.B. 15102
Haifa 3190501 Israel

+972 (4) 821-2321
 info@cybonet.com
 www.cybonet.com