Malware Isolation Webinare
4. / 9. April 2019

Symantec

Symantec Web Isolation

Reto Weber
Channel System Engineer

April 2019

90% der Cyber Attacken kommen über Web und Email

Symantec

Web Threats

700+
Neue **browser & plug-in vulnerabilities** pro Jahr

78%
Können genutzt werden um **malware zu versenden**

Every 4 seconds
Ein **unbekannte malware** wird heruntergeladen

Email & Phishing Threats

182%
Wachstum bei **active phishing URLs**

55%
der Large Enterprise sind **Ziel von Spear Phishing Attacken**

12%
der **User klicken auf nicht vertrauens-würdige Links oder Anhänge**

Source: Verizon DBIR, Symantec ISTR, Gartner

AVANTEC
Competence. Security. Trust.

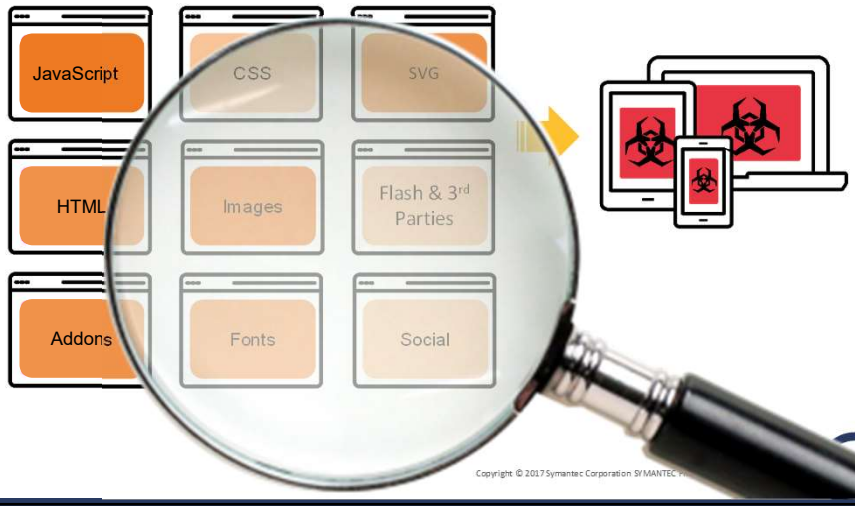
Malware Isolation Webinare
4. / 9. April 2019

Der Webbrowser ist das Angriffsziel No 1

Symantec.

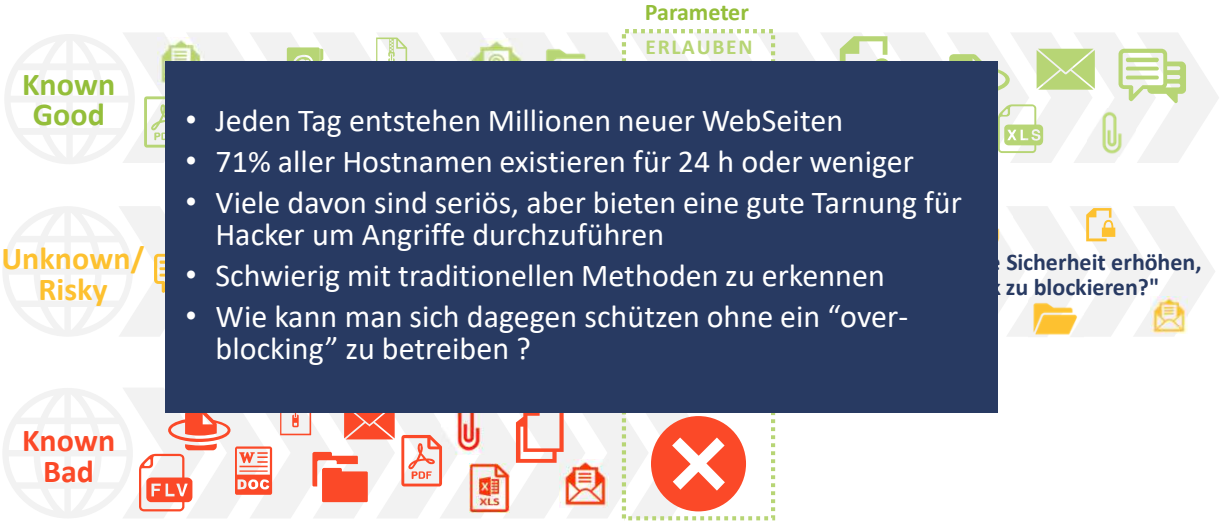
Ausnutzen von Web-Browser Funktionalitäten

Moderne Angriffs-Methoden nutzen Schwachstellen bei Browsern aus und bringen Schadcode auf den Endpunkt durch Web-Page rendering Resourcen.



Die Situation heute – Web Zugriffe

Symantec.



- Jeden Tag entstehen Millionen neuer WebSeiten
- 71% aller Hostnamen existieren für 24 h oder weniger
- Viele davon sind seriös, aber bieten eine gute Tarnung für Hacker um Angriffe durchzuführen
- Schwierig mit traditionellen Methoden zu erkennen
- Wie kann man sich dagegen schützen ohne ein “over-blocking” zu betreiben ?

AVANTEC
Competence. Security. Trust.

Malware Isolation Webinare
4. / 9. April 2019

Drei Use Cases

Symantec.

1. Vermeiden von ***Over-blocking*** **-** Zugriff auf unkategorisierte oder verdächtige Web Seiten zulassen

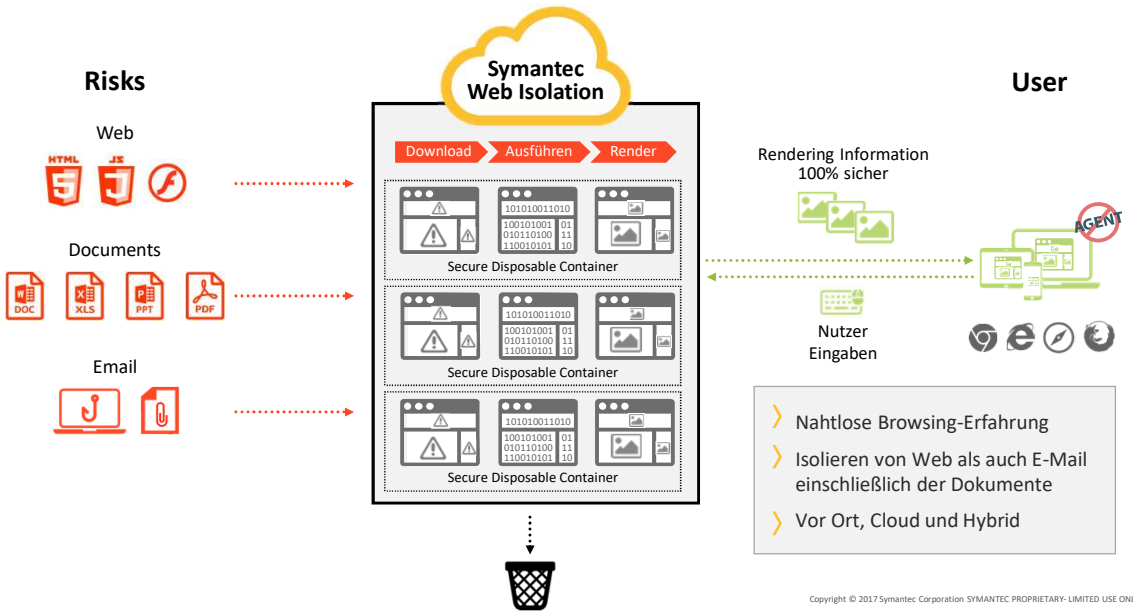
2. Zusätzlicher Schutz für bestimmte ***Nutzergruppen***

3. Abwehren von ***phishing Attacken*** durch Isolation von embedded URLs

WEB — Mail

Web Isolation Architecture

Symantec.



- Nahtlose Browsing-Erfahrung
- Isolieren von Web als auch E-Mail einschließlich der Dokumente
- Vor Ort, Cloud und Hybrid

AVANTEC
Competence. Security. Trust.

Malware Isolation Webinare
4. / 9. April 2019

Symantec Web Isolation Lösung

schließt eine gefährliche Sicherheits-Lücke (Browser)

Symantec.

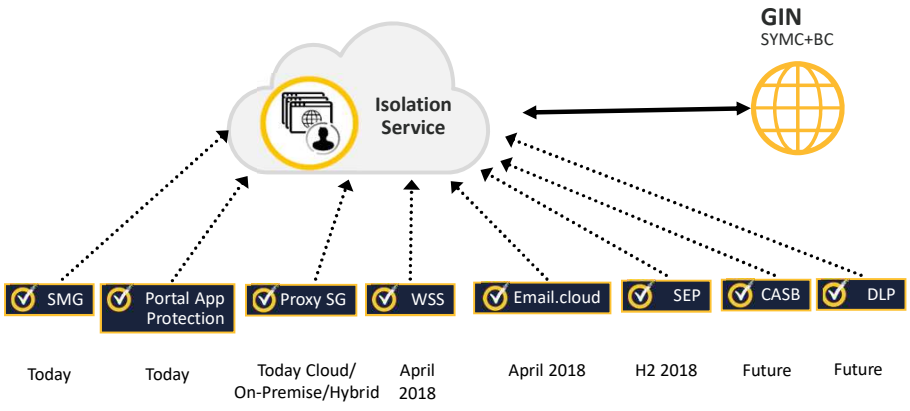
Innovative Lösung: Zero Trust Ansatz fur Zugriff auf Web Seiten

Adressiert Thematik Overblocking und in Email embedded Links

Komplementär zu bestehenden Lösungen: Verbesserung ohne großen Aufwand

Isolation Integration Portfolio

Symantec.



Also:

Stand-alone offering

3rd Party
NGFW
Proxies
Email

AVANTEC
Competence. Security. Trust.

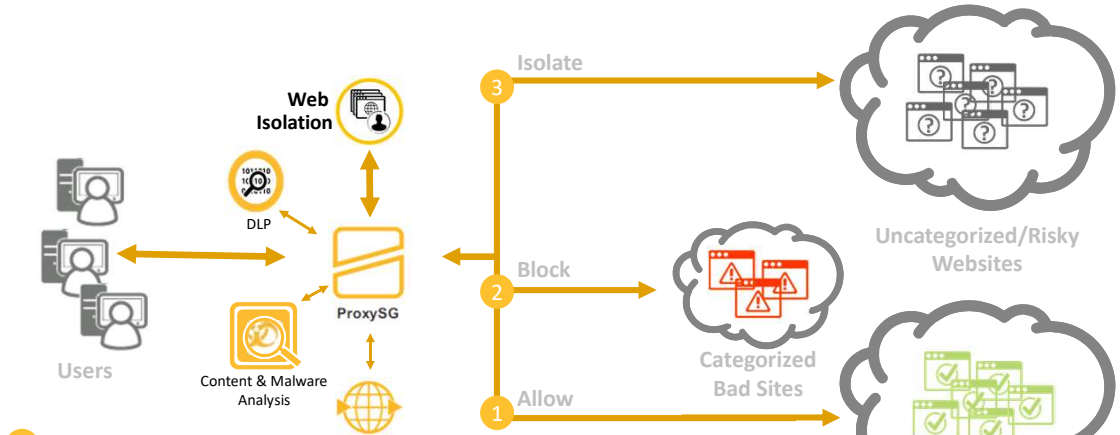
Malware Isolation Webinare
4. / 9. April 2019

Symantec.

ProxySG/WSS Integration

SWG integrated isolation capabilities

Symantec.



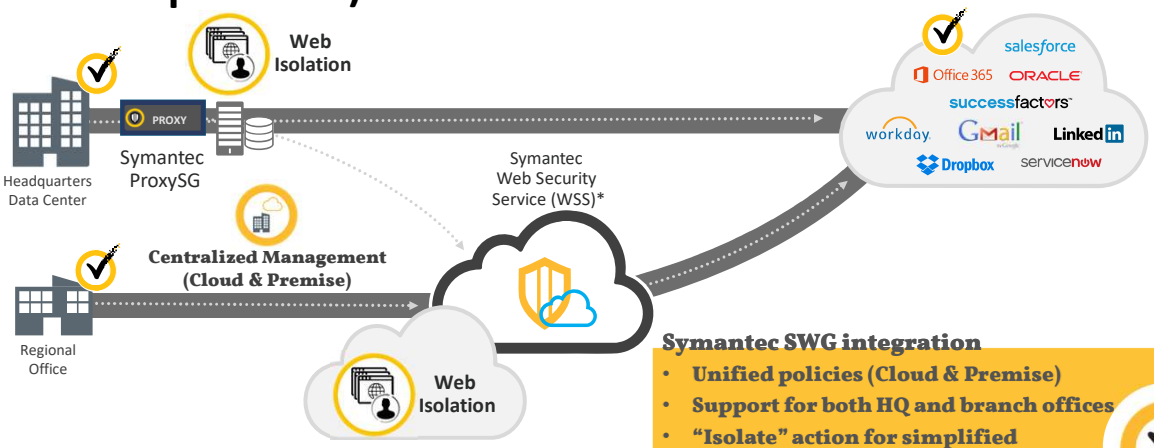
1. Allow trusted sites
2. Block known bad sites
3. Isolate uncategorized/risky sites where access is needed

AVANTEC
Competence. Security. Trust.

Malware Isolation Webinare
4. / 9. April 2019

Hybrid Integration with Symantec SWGs (cloud and on-premises)

Symantec



Symantec SWG integration

- **Unified policies (Cloud & Premise)**
- **Support for both HQ and branch offices**
- **"Isolate" action for simplified configuration**
- **Centralized management**
- **Unified logging and reporting**
- **Frictionless deployment**

11

Stop Over-blocking

Symantec

Web isolation with proxy using categories (with risk levels: BCIS-advanced)

Web access policy:

- Allow certain categories and low risk sites
- Block certain categories and riskiest sites
- Middle ground categories and potentially risky sites get isolated
  - Expanded access with no malware risk

Risk Level	Allowed Categories	Customer Category	Categories where some access may be required			Uncategorized	Security Concerns	
	Health, Financial Services, etc.	Category of Interest	File Storage/ Sharing	Dynamic DNS Host	Hacking	Uncategorized	Suspicious	Malicious Outbound	...
10	DENY							
9	DENY							
8	DENY							
7	ALLOW	ISOLATE						
6	ALLOW	ISOLATE						
5	ALLOW	ISOLATE						
4	ALLOW	ISOLATE						
3	ALLOW							
2	ALLOW							
1	ALLOW							

12

AVANTEC
Competence. Security. Trust.

Malware Isolation Webinare
4. / 9. April 2019

Symantec.

Demo

Symantec.

Danke für Ihre Aufmerksamkeit

Reto Weber
reto_weber@Symantec.com

AVANTEC
Competence. Security. Trust.