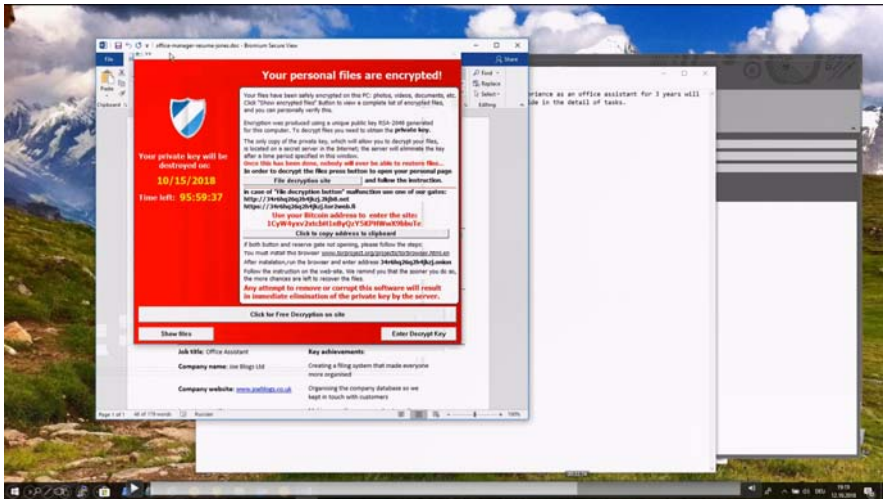
Malware Isolation Webinare
4. / 9. April 2019

AVANTEC
Competence. Security. Trust.

Weil Sicherheit alles ändert.

Dirk Gluch
Principal Security Engineer
gluch@avantec.ch

AVANTEC
Competence. Security. Trust.



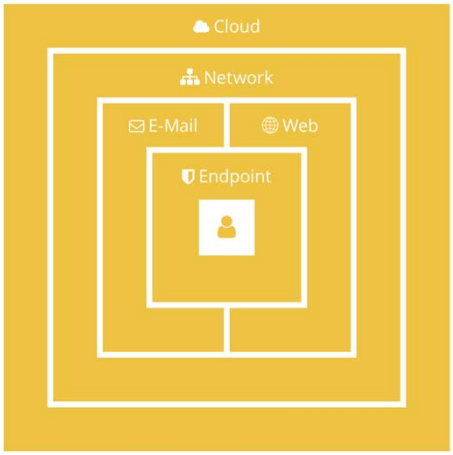
Malware Isolation Webinar

AVANTEC
Competence. Security. Trust.

Malware Isolation Webinare
4. / 9. April 2019

Gefährliches maximal minimieren –
wie wir Sie dabei unterstützen können.

Unsere Kompetenzen.



Unsere Kompetenzen

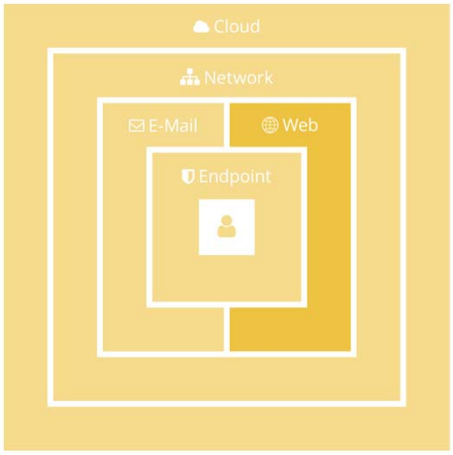
- Cloud Security
- Network Security
- E-Mail Security
- WEB Security
- Endpoint Security
- User
- Sandboxing

AVANTEC
Competence. Security. Trust.

Malware Isolation Webinare
4. / 9. April 2019

Web Security.

AVANTEC
Competence. Security. Trust.

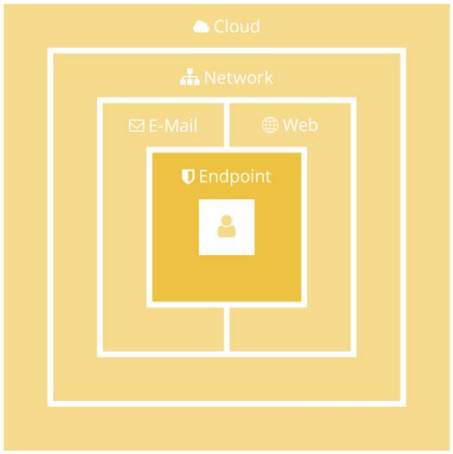


Web Security

- URL Filter and Web Application Control
- Visibility & Control (against Shadow IT)
- Anti-Malware
- Advanced Threat Protection
- SSL Interception
- Bandwidth Control
- Caching & Stream Splitting

Endpoint Security.

AVANTEC
Competence. Security. Trust.



Endpoint Security

- **Prevention**
  - Anti-Malware
  - Next Generation Endpoint Security
  - Isolation
- Detection
- Response
- Privilege Management
- Whitelisting/Application Control

AVANTEC
Competence. Security. Trust.

Malware Isolation Webinare
4. / 9. April 2019

Unsere Partner.

AVANTEC
Competence. Security. Trust.

algosec | Avecto | BLUE COAT | Bromium | Check Point SOFTWARE TECHNOLOGIES LTD. | cisco IronPort

FireEye | FORTINET | gemalto SafeNet | Pulse Secure | WISeKey QuoVadis | SEPPMAIL SWISS E-MAIL SECURITY

Symantec | TREND MICRO | VECTRA | zscaler

Betreuung von A – Z.

AVANTEC
Competence. Security. Trust.

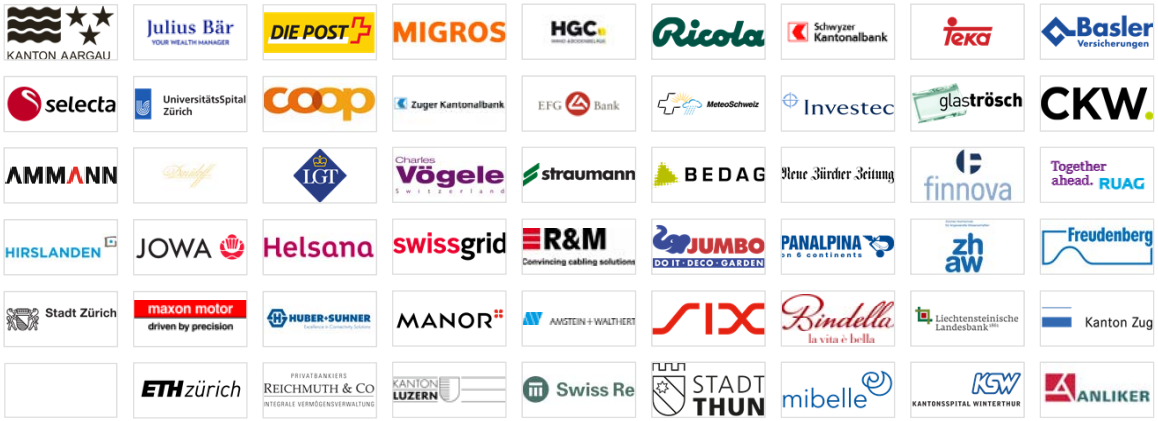
- Beratung
- Konzept
- Teststellung
- Projekt-Umsetzung & Schulung
- Wartung & Support
- Betreuung & Optimierung

AVANTEC
Competence. Security. Trust.

Malware Isolation Webinare
4. / 9. April 2019

Referenzen.

AVANTEC
Competence. Security. Trust.



Unsere DNA – Ihr Vorteil

AVANTEC
Competence. Security. Trust.

Über 20 Jahre Erfahrung
Seit 1995 der führende Integrator in der Schweiz

Höchste Kontinuität
Geringe Fluktuation, langjährige Betreuung durch die gleichen Mit-Arbeitenden

Bestes Know-how
Das beste Engineering am Markt, mehrfach ausgezeichneter Support

Best-of-Breed
Die führenden Lösungen aus einer Hand

Mehrwert durch Innovation
Ausgewählte neue Lösungsansätze ergänzen unser bewährtes Portfolio

Nachhaltige Partnerschaft
Langfristiges Denken, Ethisches Geschäftsverhalten, über 200 zufriedene Kunden

AVANTEC
Competence. Security. Trust.

Malware Isolation Webinare
4. / 9. April 2019

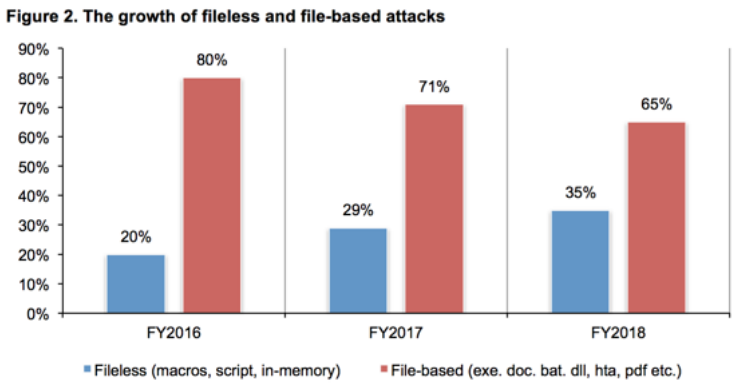
AVANTEC
Competence. Security. Trust.

Damit Gefährliches draussen bleibt –
wer sich dafür auf uns verlässt.

Malware 2018

AVANTEC
Competence. Security. Trust.

- Anzahl wächst weiterhin ~20% plus
- Mehr Fileless, weniger filebase
- More Ransomware und Cryptominer
- Weiterhin Verteilung via Spam, mail attachments und links
- Trojaner über 80%
- Signifikanter Anstieg für android und MacOS



AVANTEC
Competence. Security. Trust.

Malware Isolation Webinare
4. / 9. April 2019

Isolation is a Trend

AVANTEC
Competence. Security. Trust.

- Sandboxes
  - Am Mailgateway
  - Netzwerk
  - Malware Eco-System
- Isolation am Client
- Isoaltion im Netzwerk
  - Webaccess

Bromium und Symantec im Vergleich

AVANTEC
Competence. Security. Trust.

	Bromium	Symantec
Kern-Technologie	Isolation von Prozessen/Files mit potenziellem Schadcode in Micro-VM	"Flattening" von aktivem Content und reine visuelle Aufbereitung des Web-Streams
Web-Protection	Ja	Ja
E-Mail-Protection (z.B. Mail-Anhänge im Outlook)	Ja	Nein, jedoch Schutz vor verlinkten URLs in E-Mails
File-Protection	Ja	Nur Remote-Files
Usability	Normale Workflow- und Editierfähigkeiten, keine Einschränkungen von Webinhalten, Handling von Dateien etc.	Editieren von Files (teilweise View-Only bzw. nur PDFs), die meisten aktiven Contents auf Webseiten werden unterstützt
Deployment/Management	Agent auf Endpoints und zentrale Management-Konsole	Einfaches Deployment und Management, da zentral am Gateway, kein Agent auf Endpoint nötig
Kompatibilität	Windows	Jeder aktuelle Browser (unabhängig von OS)
Performance	Arbeitslast auf Endpoints verteilt, im normalen Office-Gebrauch keine Performance-Einbussen spürbar	Arbeitslast zentral auf Proxy, keine Performance-Einbussen auf dem Proxy, sofern dieser richtig dimensioniert ist

AVANTEC
Competence. Security. Trust.