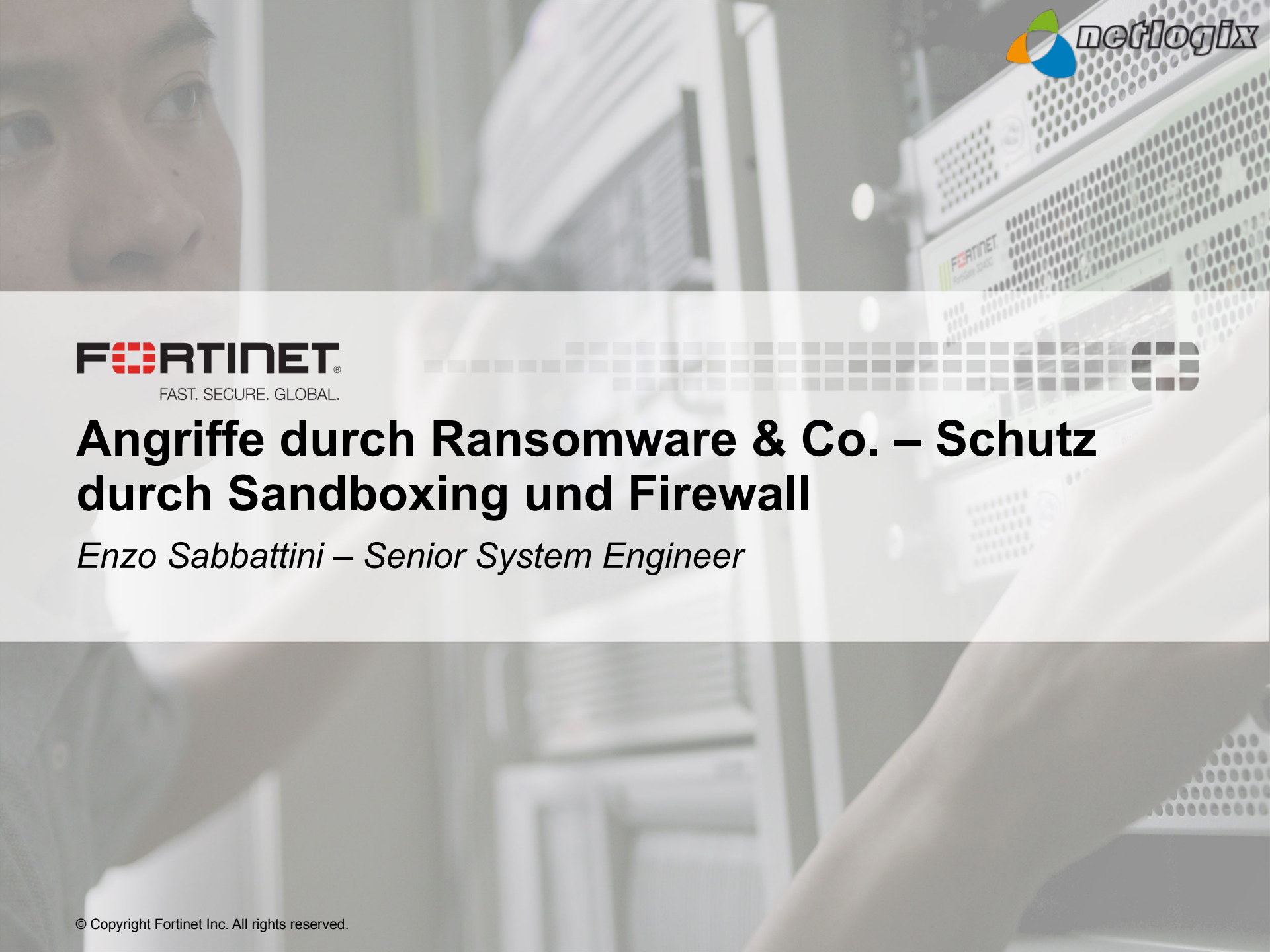
Risiko
Sicherheit

RISIKO
ODER
SICHERHEIT?!?



FAST. SECURE. GLOBAL.

Angriffe durch Ransomware & Co. – Schutz durch Sandboxing und Firewall

Enzo Sabbattini – Senior System Engineer

© Copyright Fortinet Inc. All rights reserved.

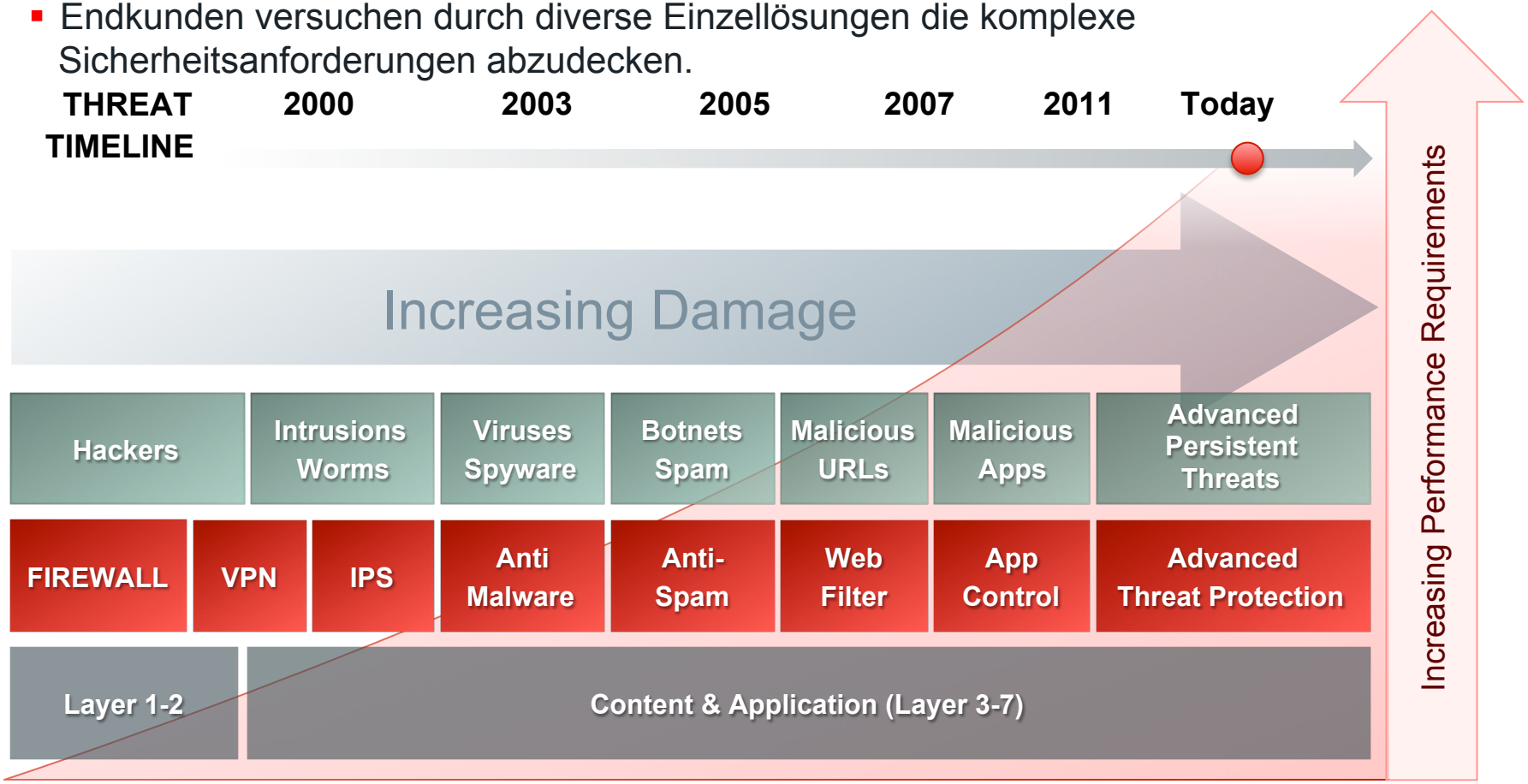
Intention von Hacker – früher

Intention von Hacker – heute

Neue Ziele von Hacker

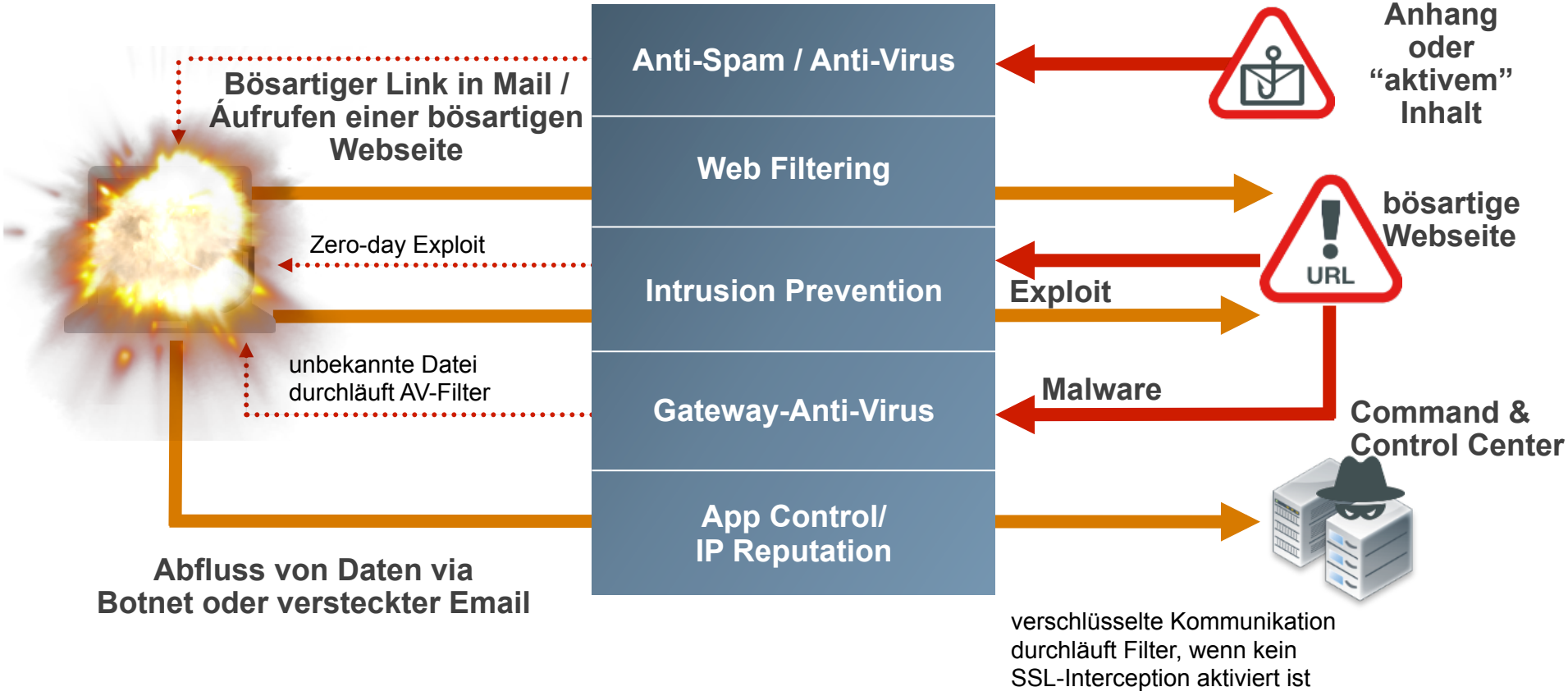
Herausforderung

- Heutige Bedrohungen sind komplexer und verursachen mehr Schaden als je zuvor. Um dies zu stoppen werden eine Reihe von Sicherheitstechnologien benötigt.
- Die meisten Anbieter von Sicherheitslösungen decken nur einen geringen Teil ab.
- Endkunden versuchen durch diverse Einzellösungen die komplexe Sicherheitsanforderungen abzudecken.

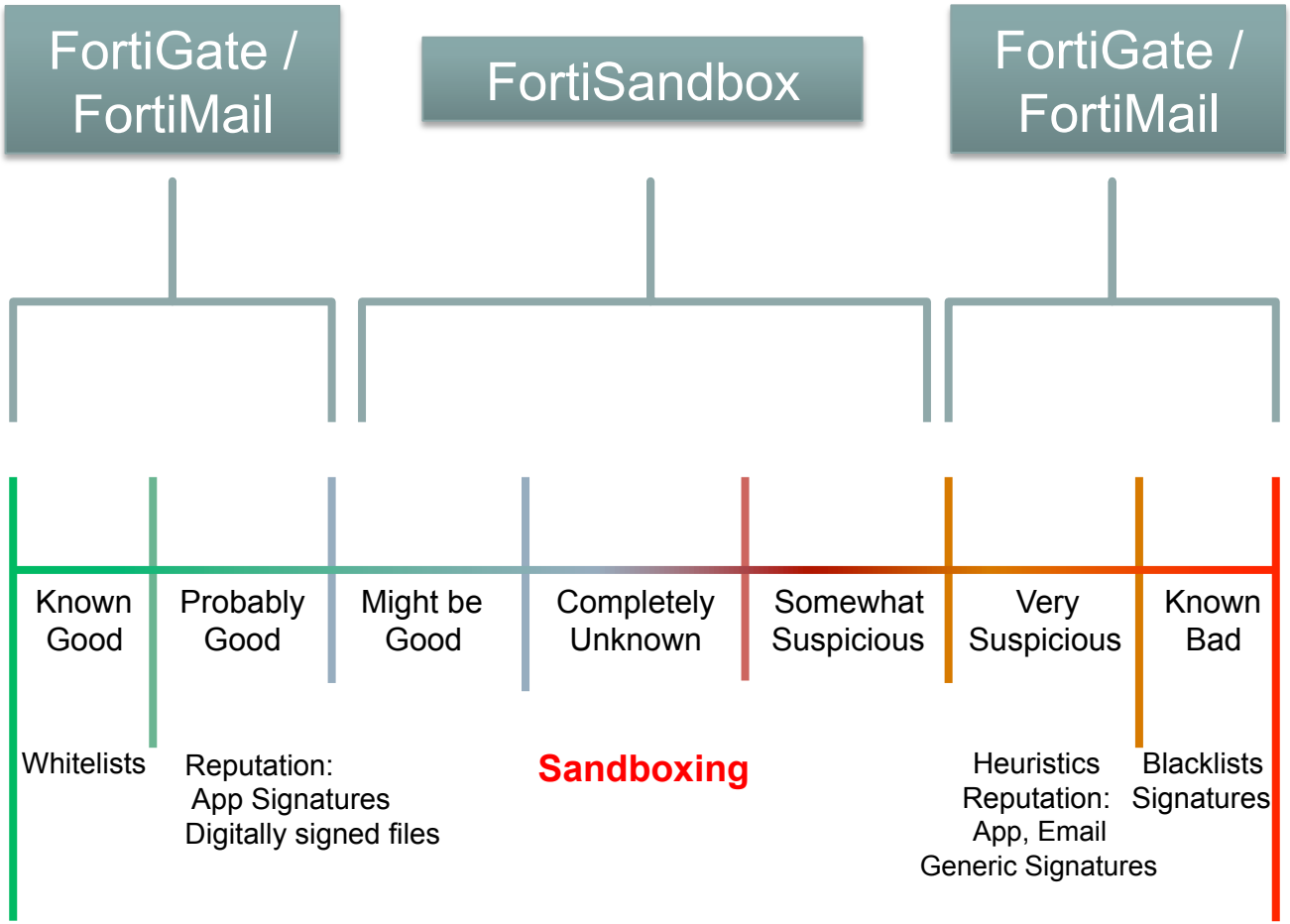


Typischer Ablauf eines zielgerichteten Angriffs

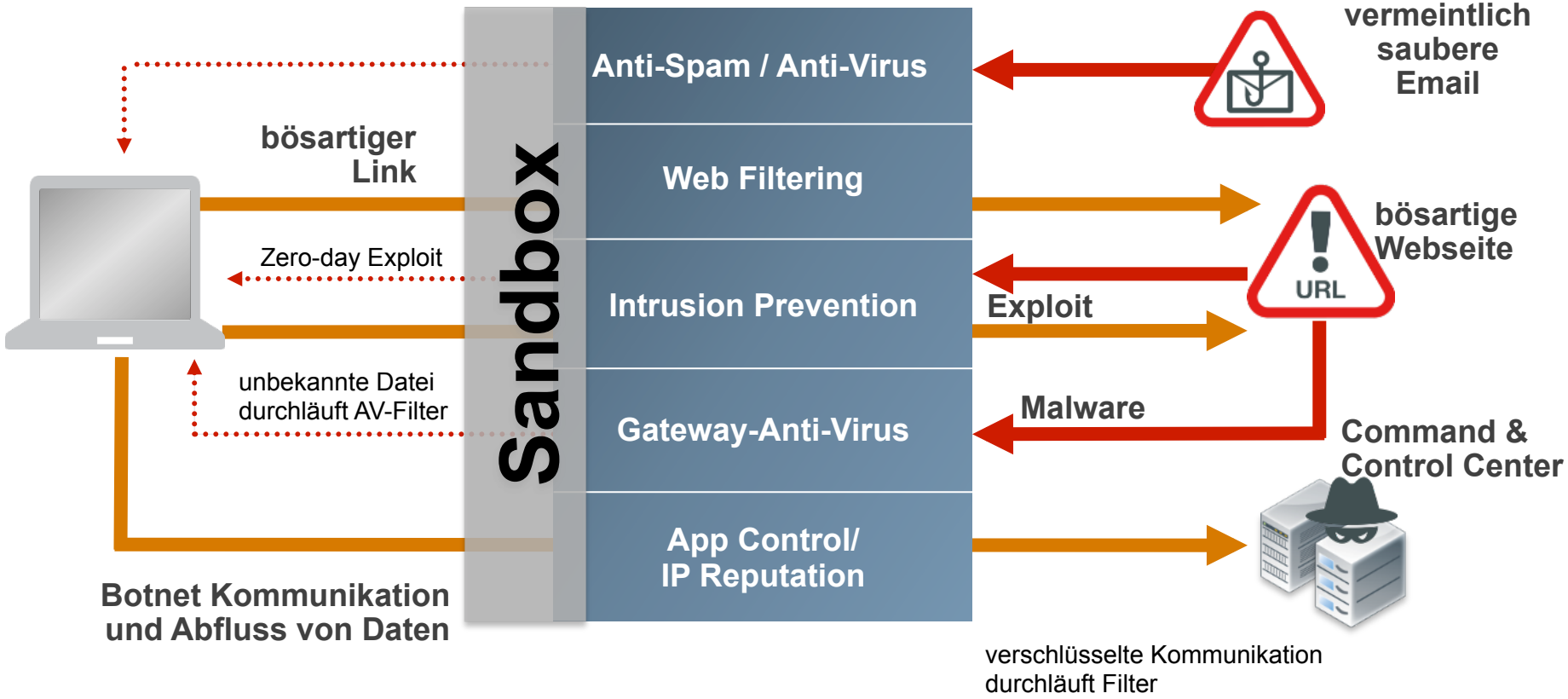
Sowohl Gateway-AV als auch Client-AV schlagen nicht an, da es sich um einen Zero-Day handelt



Malware? Goodware? I-don't-know-ware?



Die FortiSandbox als ganzheitlicher Ansatz



FortiGate ATP Integration

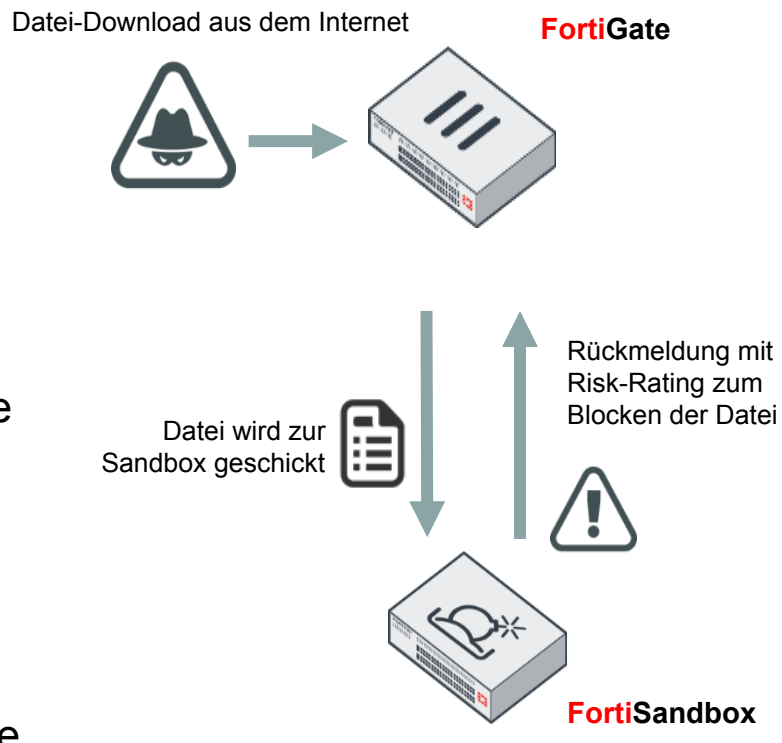
- Extrahiert die Datei aus dem evtl. SSL-verschlüsselten Datenstrom
- Nutzt das AV Profil – Flow (full) und Proxy Mode

- FortiGate überträgt nur supportete Dateitypen
- Filterung erfolgt über die FGT AV engine

- Dateitypen können manuell auf eine Whitelist gesetzt werden, um Bandbreite und Performance auf der Sandbox zu schonen

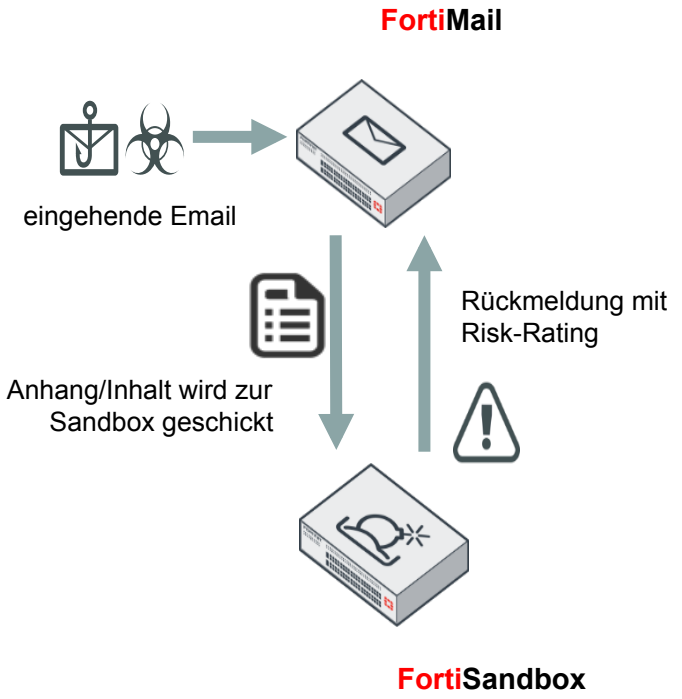
- Die FortiGate wird über die Analyse-Ergebnisse informiert

- Nutzung der Analyseergebnisse über dynamische Thread-DB Updates
  → Daten werden nicht doppelt analysiert und somit auch schneller erkannt



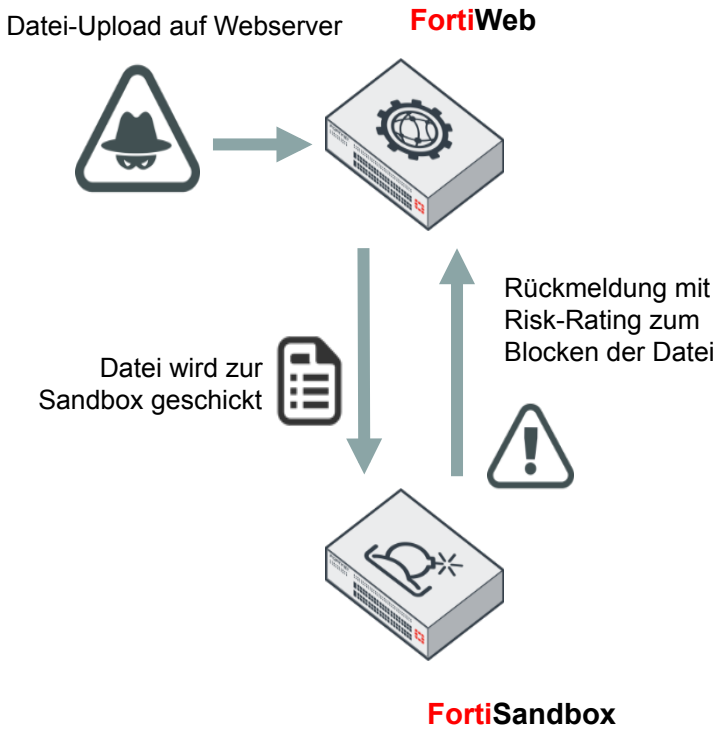
FortiMail ATP-Integration

- Übertragen von Anhängen bzw. Inhalten zur tieferen Analyse an die FortiSandbox
- Filterung kann basierend auf Dateitypen erfolgen
- Mails werden während der Analyse in der Queue gehalten
- Automatisches Weiterleiten bzw. Blocken der Mail basierend auf dem Analyseergebnis
- Nutzung der Analyseergebnisse über dynamische Thread-DB Updates
  → Daten werden nicht doppelt analysiert und somit auch schneller erkannt



FortiWeb ATP-Integration

- Uploads zu Web Applikationen (Bewerbungs-Portal, Bürger-Portal, etc.) werden zur er-weiterten Analyse an die FortiSandbox gesendet.
- Die FortiWeb wird über die Analyse-Ergebnisse informiert.
- Verdächtige Dateien werden dementsprechend geblockt und gleiche Dateien werden zukünftig ohne weitere Analyse gleich behandelt.

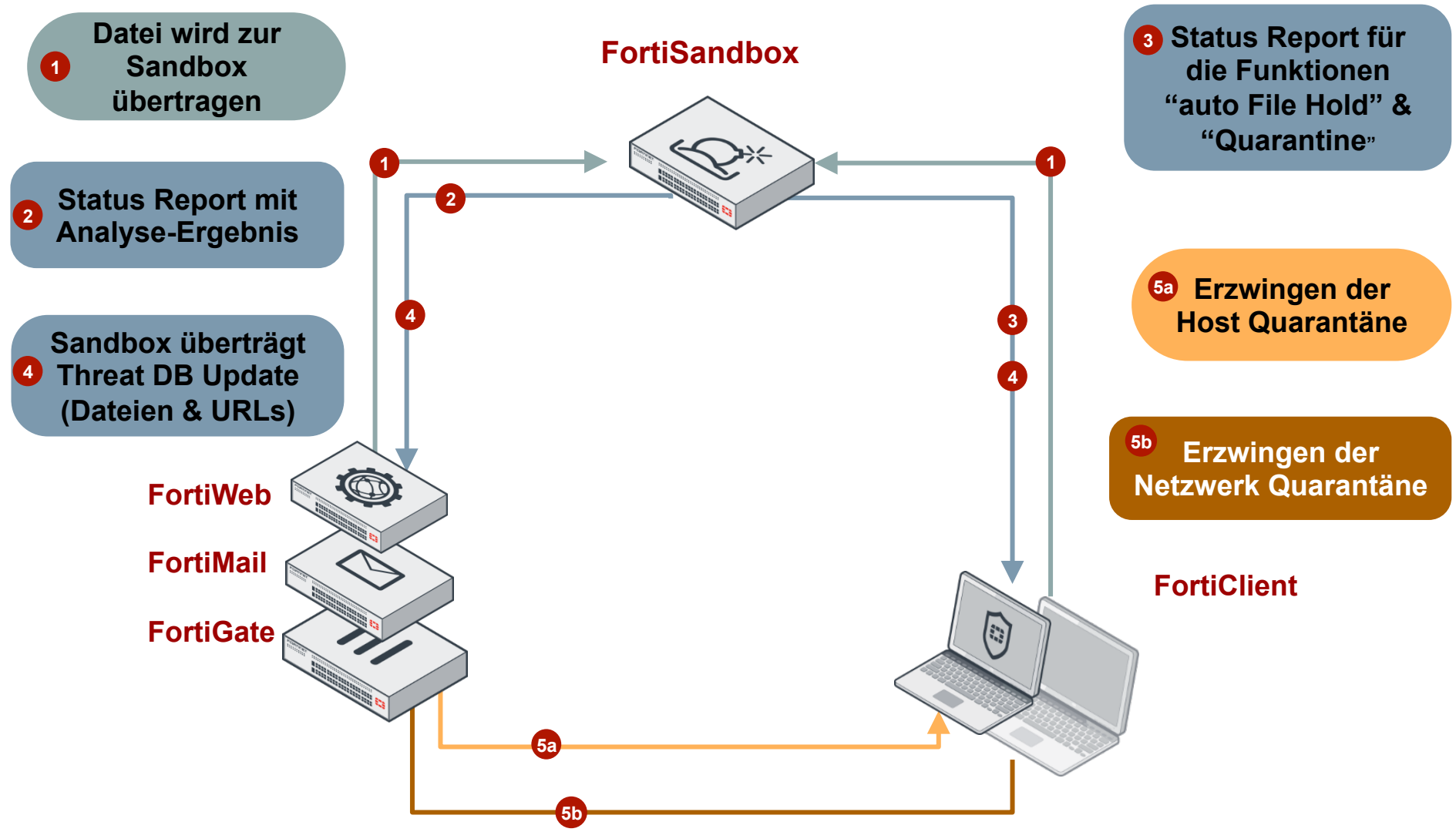


Die ganzheitliche Fortinet ATP Lösung

1 Datei wird zur Sandbox übertragen

2 Status Report mit Analyse-Ergebnis

4 Sandbox überträgt Threat DB Update (Dateien & URLs)



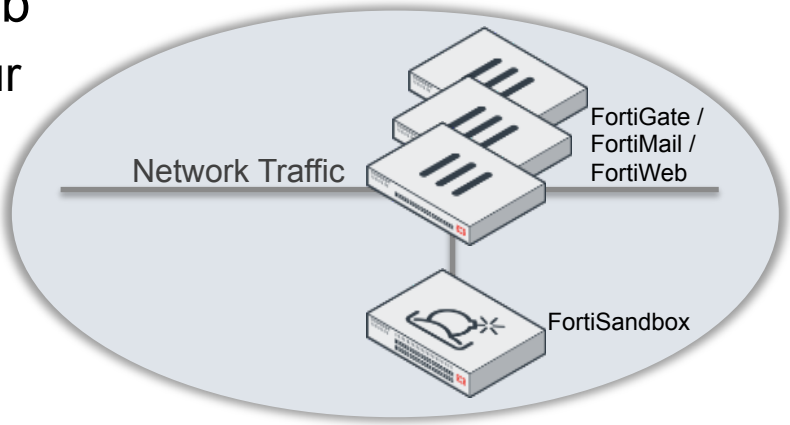
3 Status Report für die Funktionen “auto File Hold” & “Quarantine”

5a Erzwingen der Host Quarantäne

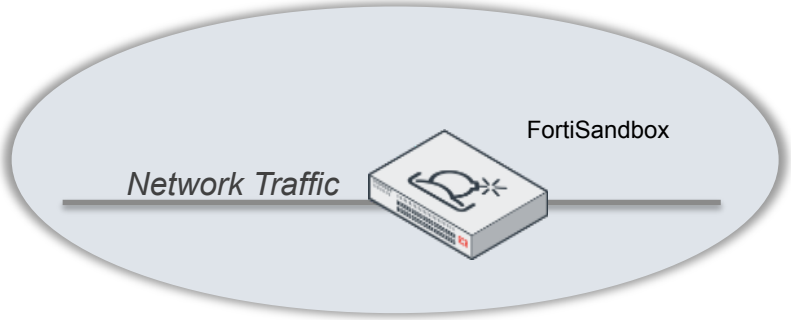
5b Erzwingen der Netzwerk Quarantäne

Flexible Einsatzmöglichkeiten

- Integration mit Fortigate/FortiMail/FortiWeb
  - » Dateien werden “angehalten” und gezielt zur FortiSanbox gesendet



- Sniffer-Modus / SPAN-Modus
  - » Dateien werden aus dem durch das Gerät geleiteten Verkehrsstrom extrahiert



- On-demand
  - » Dateien werden manuell, per FortiClient oder per API zur FortiSandbox hochgeladen

FortiSandbox Optionen

- flexible Lösung – Cloud – VM-based - Appliances / Cluster

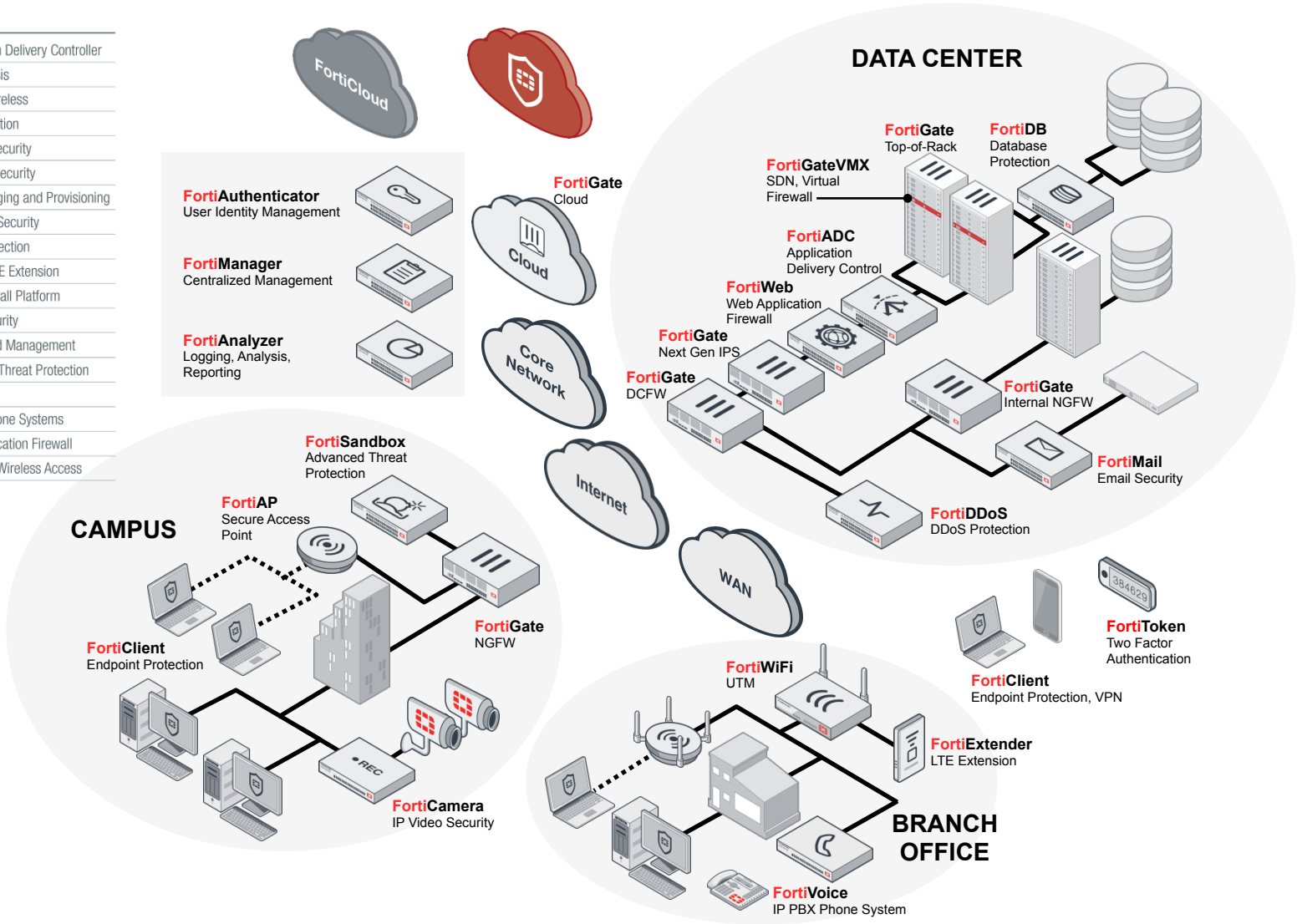
	FortiSandbox Cloud	FortiSandbox VM	FortiSandbox 1000D	FortiSandbox 3000D
VMs	NA	4+	8	28

einfache Lizenzierung –
unabhängig von der Art der Nutzung und Anzahl der User/Mailboxen

The Fortinet Secured Network

Product List

FortiADC	Application Delivery Controller
FortiAnalyzer	Log Analysis
FortiAP	Secure Wireless
FortiAuthenticator	Authentication
FortiCamera	IP Video Security
FortiClient	Endpoint Security
FortiCloud	Cloud Logging and Provisioning
FortiDB	Database Security
FortiDDoS	DDoS Protection
FortiExtender	Cellular LTE Extension
FortiGate	Core Firewall Platform
FortiMail	Email Security
FortiManager	Centralized Management
FortiSandbox	Advanced Threat Protection
FortiToken	2FA Token
FortiVoice	IP PBX Phone Systems
FortiWeb	Web Application Firewall
FortiWiFi	UTM with Wireless Access



FORTINET