Enhanced Security Mitigation via Automation

Steve Mulhearn
Consulting Director

orange™ Business Services

FORTINET®

The Evolving Threat Landscape

Giant Equifax data breach: 143 million people could be affected

Equifax says a giant cybersecurity breach compromised the personal information of as many as 143 million Americans — almost half the country

CNNtech | September 8, 2017: 9:23 AM ET

EXPLOIT

Why 'WannaCry' Malware Caused Chaos for National Health Service in U.K.

EXPLOIT

Bad Rabbit: Game of Thrones-referencing ransomware hits Europe

NotPetya-style malware infects Kiev's metro system, Odessa airport and Russian media, demanding bitcoin for decryption key

The Guardian | Wednesday 25 October 2017 06.06 EDT

2017

>$1 BILLION

Source: FBI, 2016

2017

35x Growth

Source: FortiGuard Labs, 2017

SELF PROPOGATE

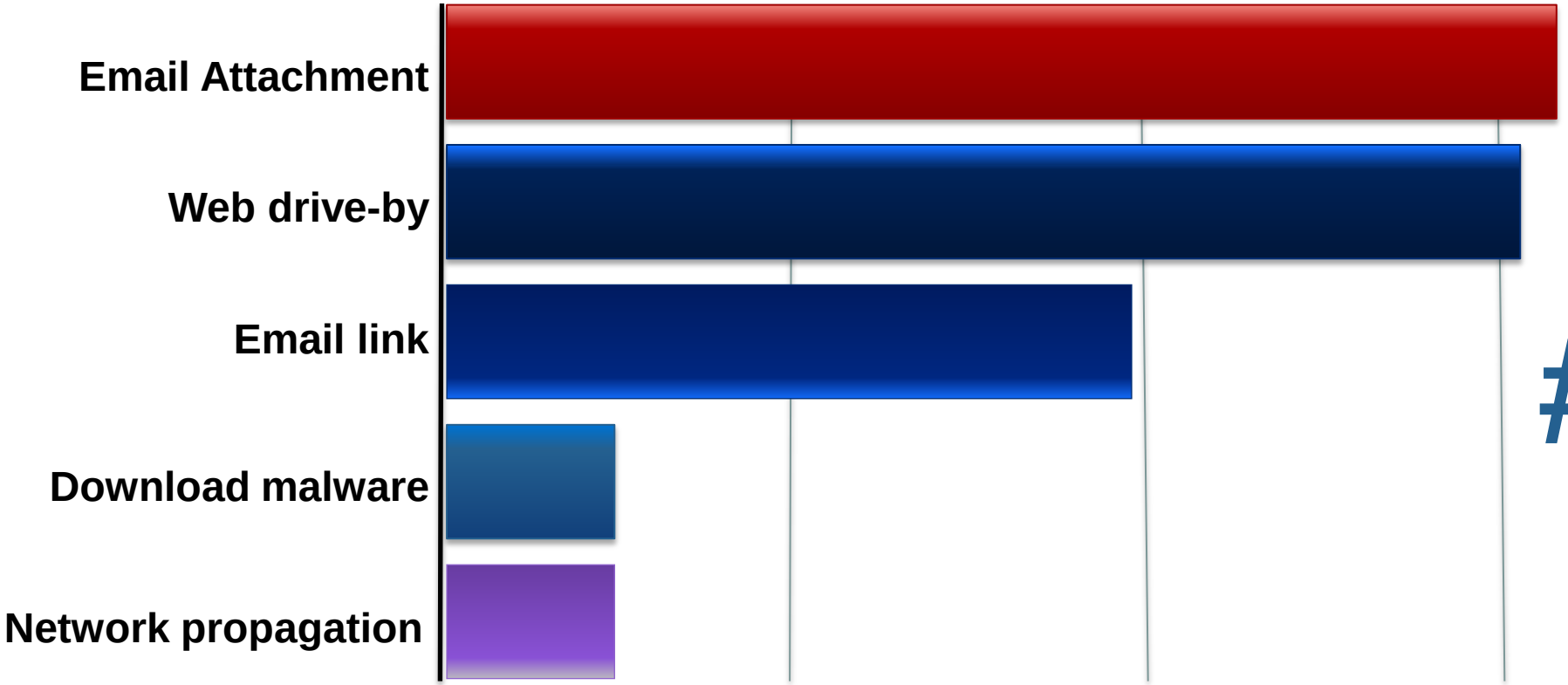
aaS Analysis Service

AI Adaptive Malware

FORTINET

Concern #1 The Enterprise Attack Surface is Broad

Top 5 Avenues for Crimeware



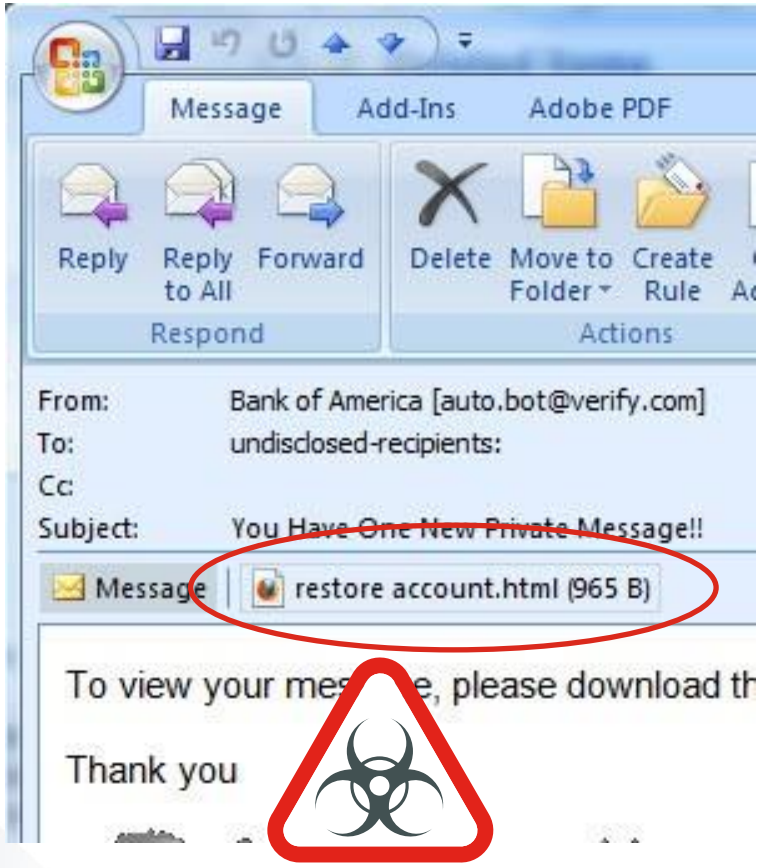
#1 Phishing Malvertisement

Source: Verizon. 2016 Data Breach Investigations Report. 2016.

What are the Most Common Threat Vectors?

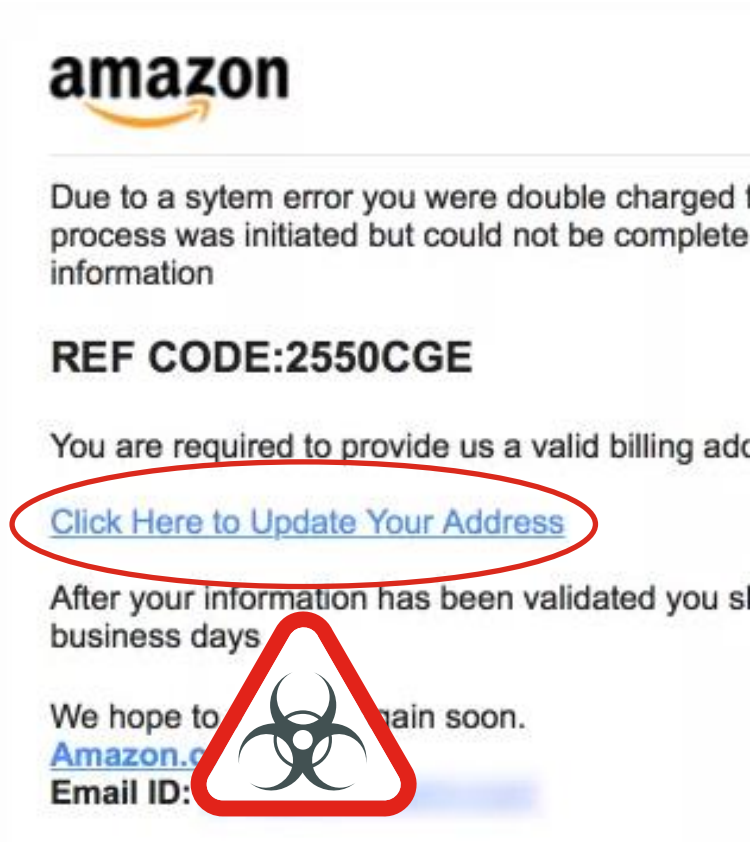
All Rely on Social Engineering

EMAIL ATTACHMENT



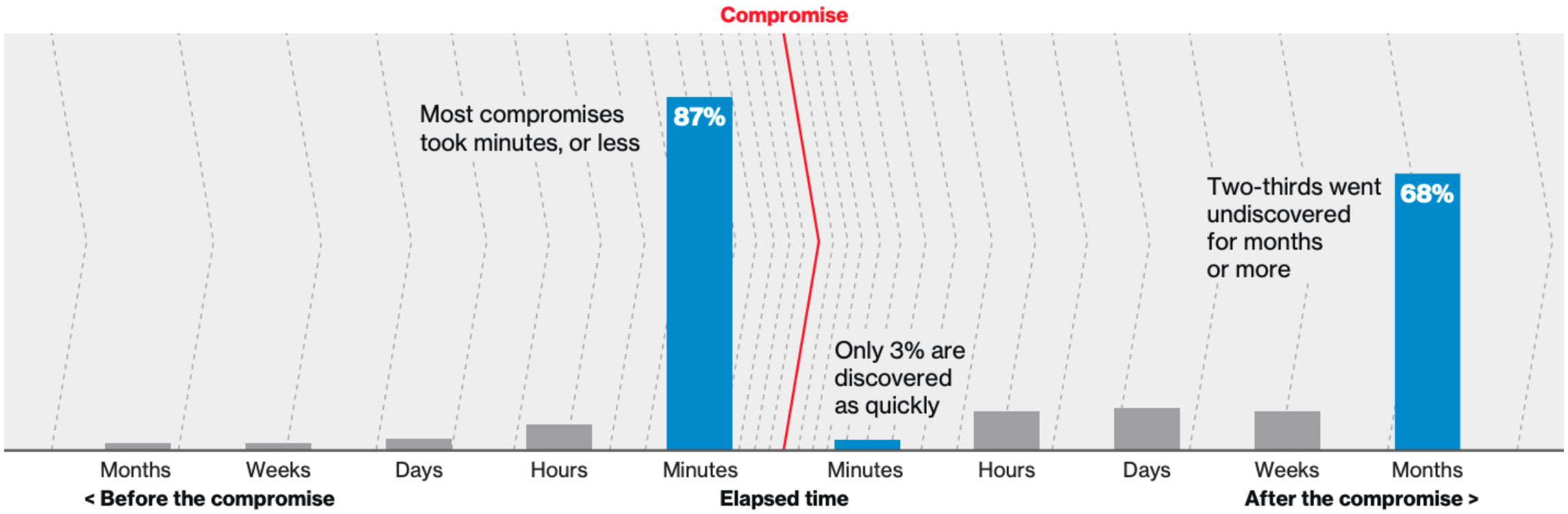
WEB-DRIVE-BY

EMAIL LINK



Time To Discover a Breach

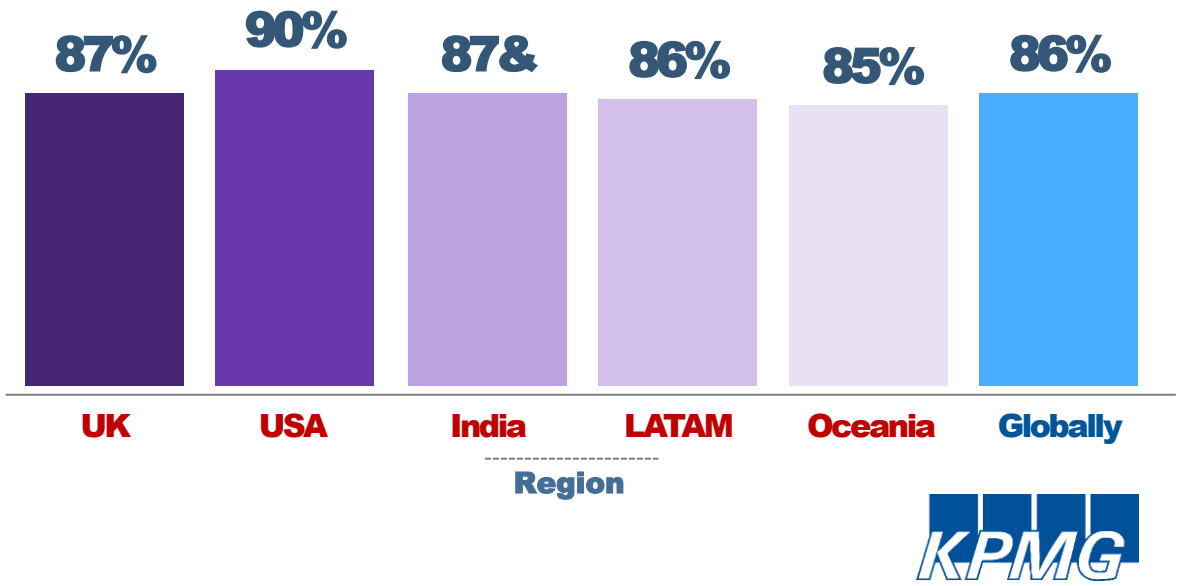
For the majority, TTD is too long and it is already too late!



Verizon 2018 Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

Cyber Skills Shortage

ISACA members who believe there is a shortage of skilled cybersecurity professionals (%)



KPMG

65% report skills shortage holding them back, *up from 59% last year*

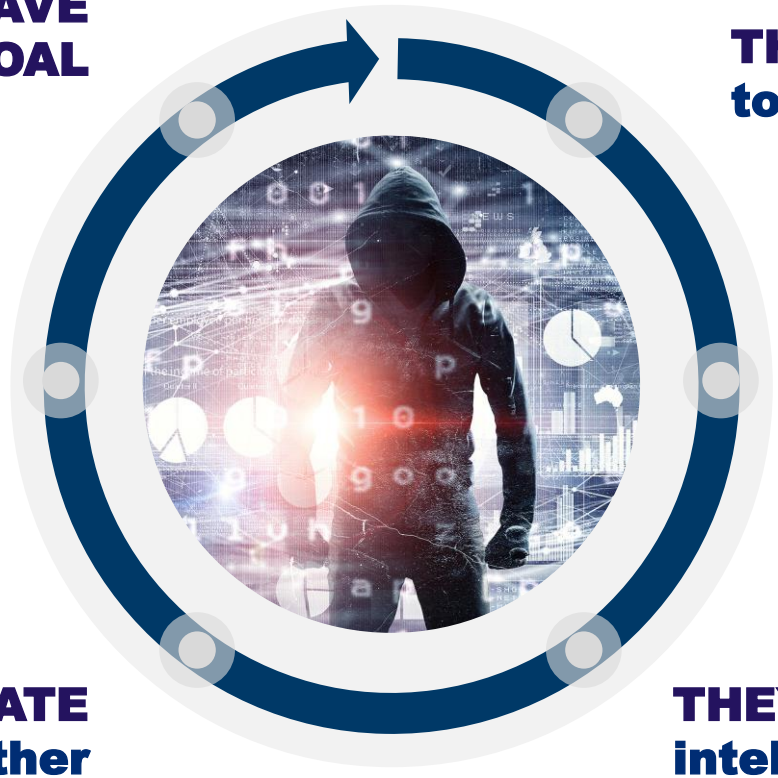
44% expect to increase team size next year, compounding the issue

HARVEY NASH
The Power of Talent

Why Are the Criminals So Successful?

THEY HAVE A COMMON GOAL

THEY TALK to each other



They are NOT LIMITED BY RULES

THEY TRADE with each other

THEY INTEGRATE their tools together

THEY SHARE intellectual property

FORTIGUARD LABS 2018

Since 2000, FortiGuard Labs has provided in-house, industry-leading security intelligence and research, powering Fortinet's platform and delivering a suite of advanced services

Industry Leading Patented Security Technology

Zero-day Research

- 500 0-days discovered (Q4'17)

Delivering Advanced Technologies

- FortiSandbox

NEW *Anti-Exploit Engine (FortiClient)*

Delivering Intelligence Services

- CPRL AV, IPS, App Control, IP Reputation, Web Filter, Anti-Spam, Web Security App, Vulnerability Management

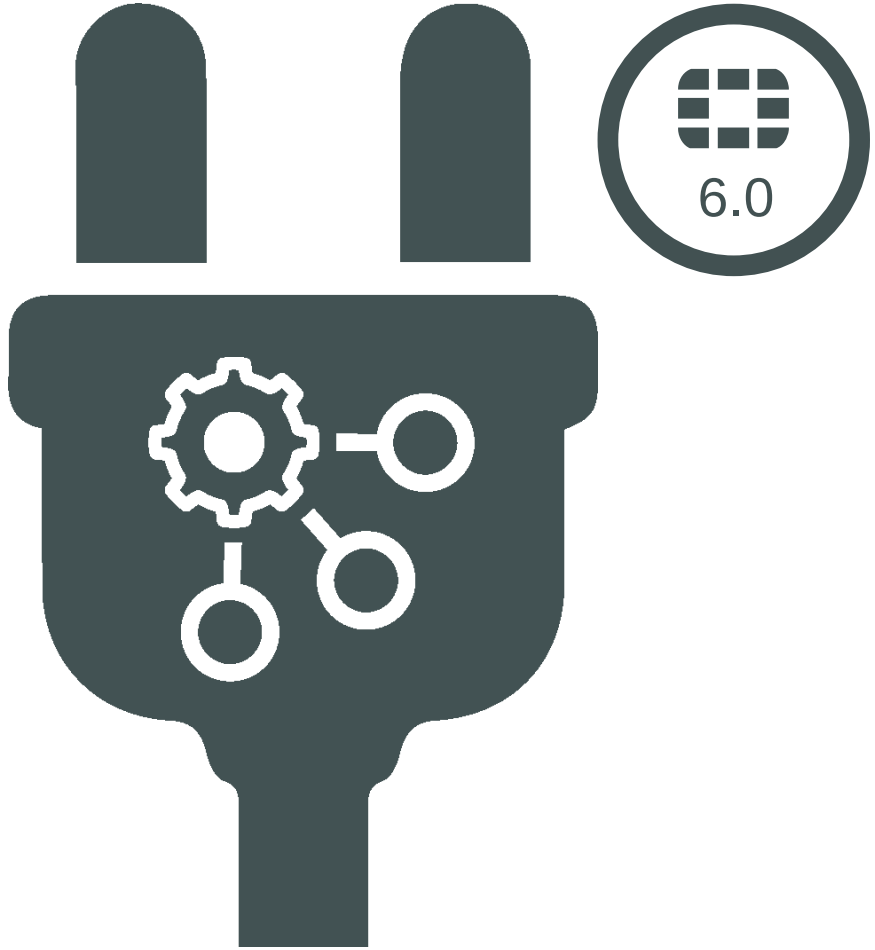
NEW *Virus Outbreak Service and Content Disarm & Reconstruction (FortiMail and FortiGate)*

Published Research

- Quarterly Threat Report
- Bi-weekly Threat Brief
- Blogs

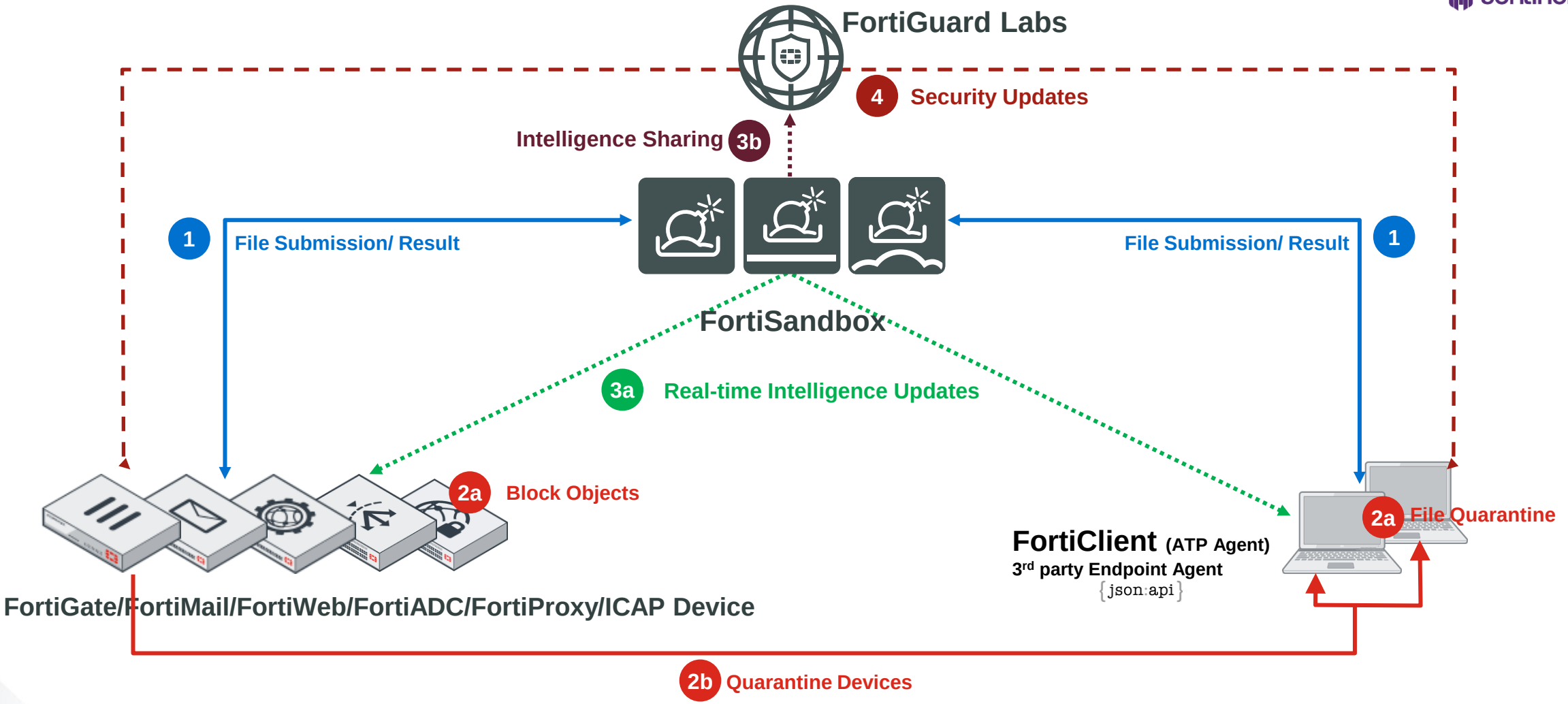
Automated Security Fabric

- Fortinet Automation
  - Detect 0-day from unkown objects (files or URLs)
  - Reduce Time to Detection
  - Mitigate the Threat
  - NOC-SOC Integration



That is Fully Automated

ATP Framework: Automated Intelligence Sharing and Response



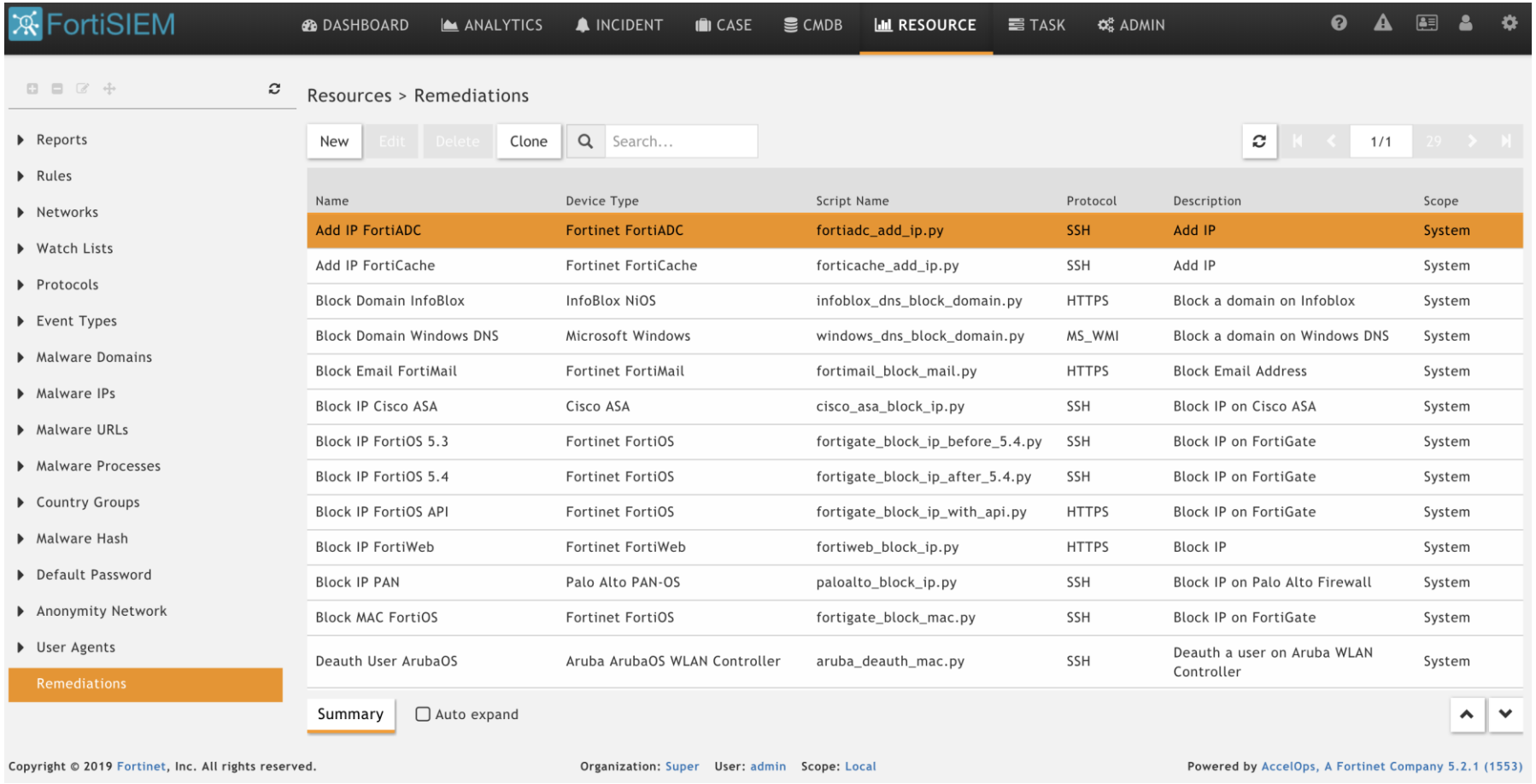
Virus Outbreak Service (VOS) with FortiSandbox

- What it is
  - Real-time emerging threat signature database
  - Up-to-date protection vs traditional AV updates
  - Applies to FortiGate and FortiMail
- Benefits
  - Reduces detection time of latest known malware
  - Including FortiSandbox pre-filter stage
- How does FortiSandbox compliment this service
  - Detects Zero-day/Unknown Malware
  - Newly acquired intelligence contributes to VOS service

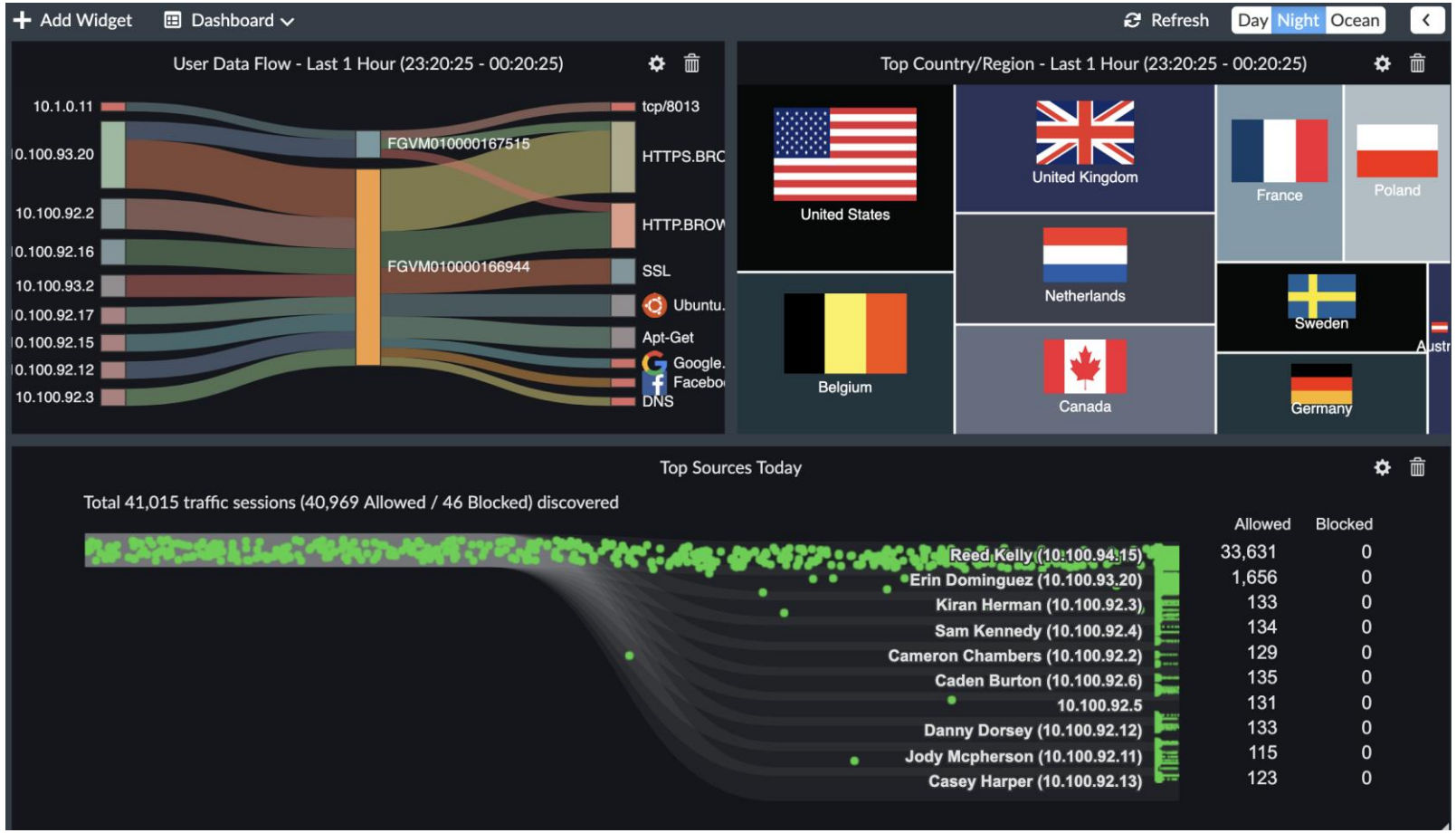
Content Disarm & Reconstruct (CDR) with FortiSandbox

- What it is
  - Strips active content (scripts, macros, etc) from Office and Adobe documents
- Benefits
  - Eliminates the possibility of infection via documents
  - Real-time document disarmament with no delay
- How does FortiSandbox complement this service
  - Analyze the original documents to identify breach attempts
  - Detects Zero-day/Unknown executable malware

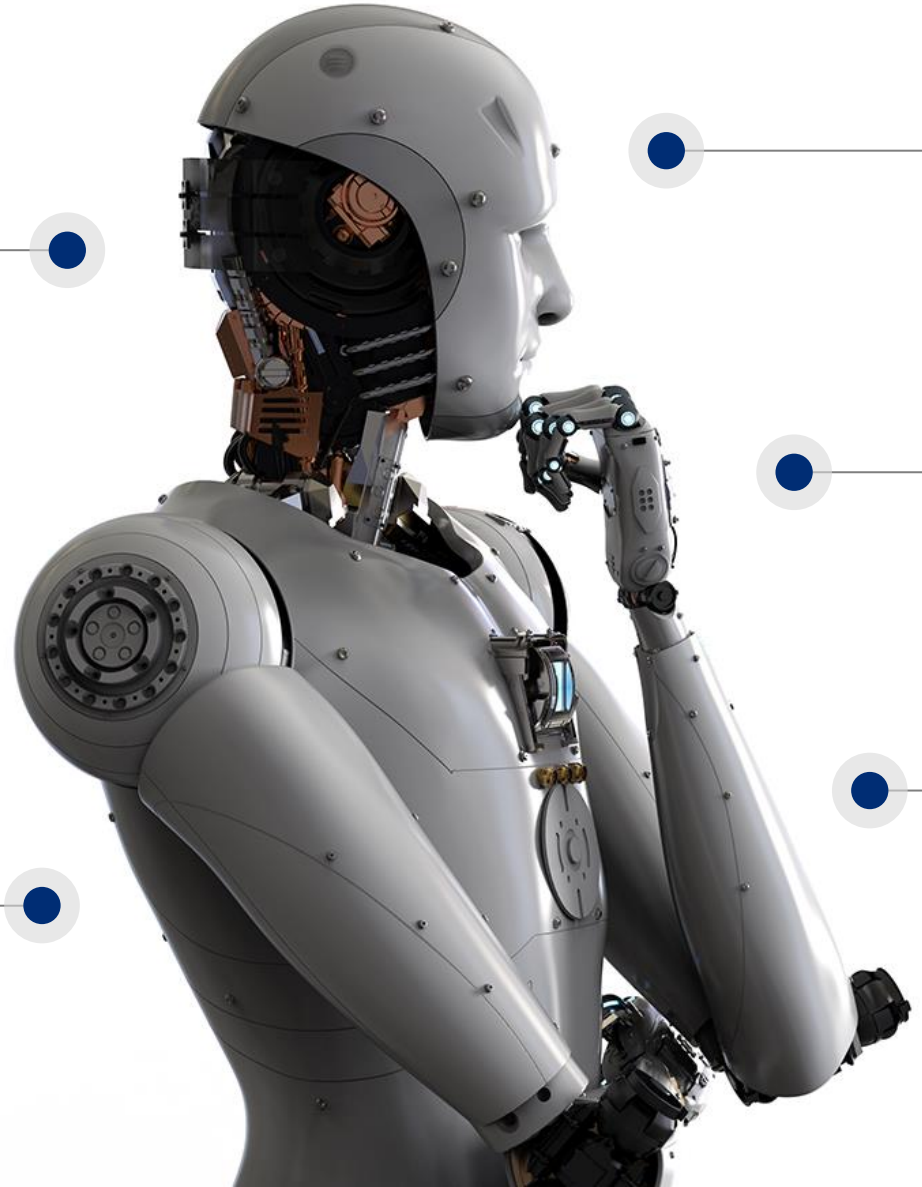
FortiSIEM Remediations Library



NOC-SOC VIEW



Where is it Going ?



BETTER COMMUNICATION

MORE INTELLIGENT SYSTEMS

IMPROVED INTELLIGENCE

IMPROVED VENDOR COMMUNICATION

SEAMLESS INTEGRATION WITH INDIVIDUAL SYSTEMS

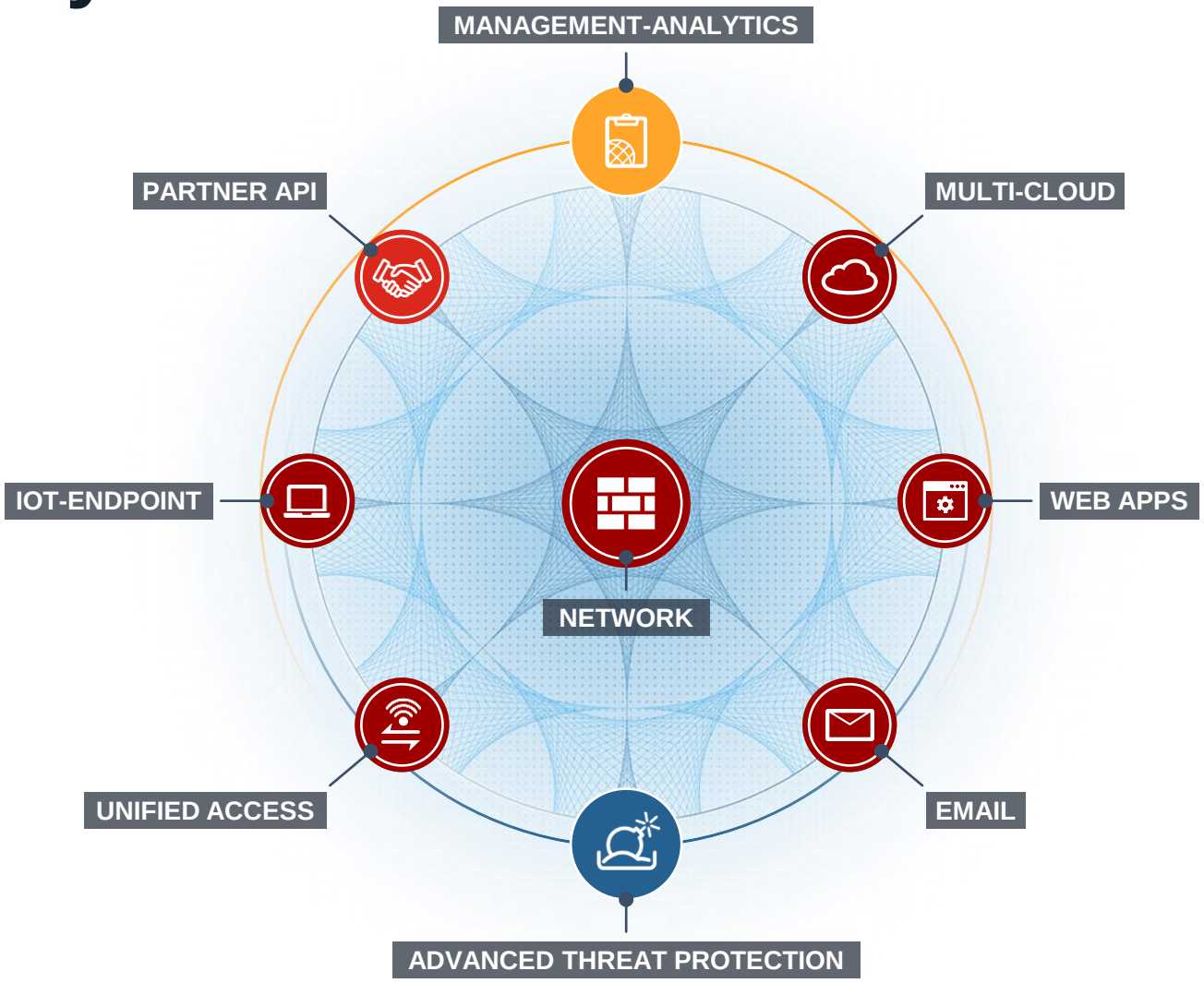
INTERWOVEN SOLUTIONS PROVIDING INTELLIGENT ACCURATE REPORTING

The Solution: Fortinet Security Fabric

BROAD

INTEGRATED

AUTOMATED



Thank you