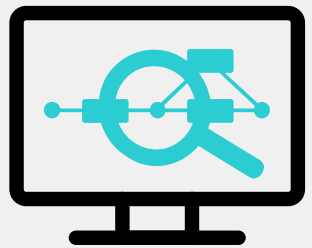
Je ochrana vašich koncových zariadení dostatočná?

Jaro Stolicny

Systems Engineer, Fortinet



Problems that keep CISOs Awake at Night

Lack of Visibility

63%

of companies cannot monitor off-network endpoints, over half can't determine endpoint compliance status

Breach Anxiety

Accelerating Threat landscape
Ransomware
Business disruption

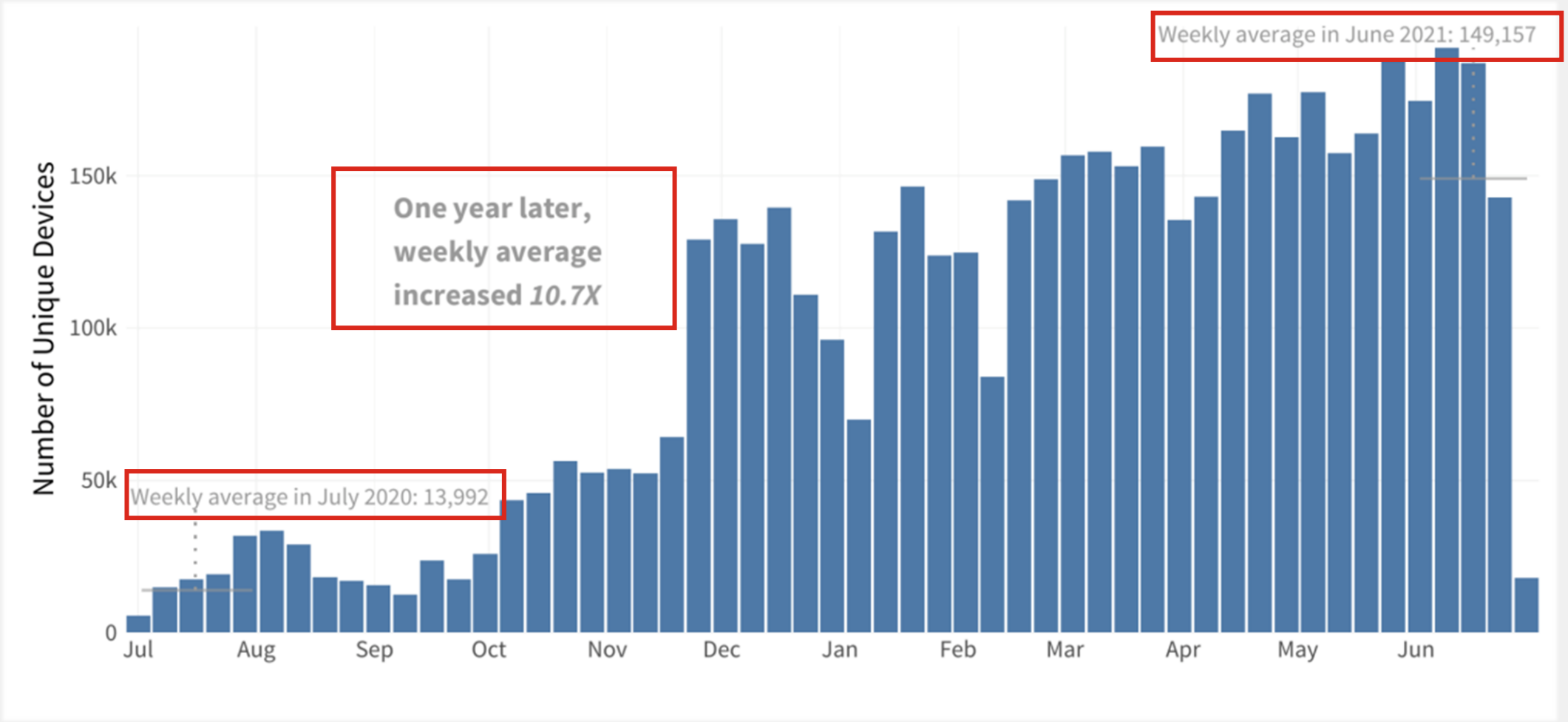
Alert Fatigue
Analyst Burnout

Fortinet pledges to train 1 million people to help close the cybersecurity skills gap

Notes/Sources:
Gartner: Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017

© Fortinet Inc. All Rights Reserved.

Ransomware in numbers



source: FortiGuard Labs – Global Threat Landscape Report (Aug. 2021)

© Fortinet Inc. All Rights Reserved.

FortiGuard Labs Statistics

15 Million
Botnet C&C attempts
THWARTED
PER MINUTE

47 Million
SPAM
Blocked Per Day

462,000
Malicious Website
ACCESSES
Blocked Per Minute

906
ZERO DAY
THREATS DISCOVERED

5.3 Million
NETWORK INTRUSION ATTEMPTS
resisted per minute

136,000
PHISHING
Blocked Per Minute

1.2 PB
Of Threat Samples

609,000
HOURS
of Threat Research
GLOBALLY PER WEEK

904,000
MALWARE PROGRAMS
Neutralized Per Minute

Q4 2020

© Fortinet Inc. All Rights Reserved.

206 days

Average time to discover data breaches

73 days

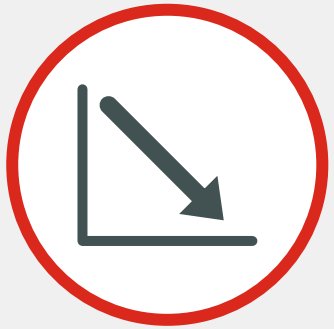
Average time to contain breaches once discovered

Source: Ponemon Institute (on behalf of IBM), 2019
SANS institute

© Fortinet Inc. All Rights Reserved.

Prevention is a Necessity

Know Your Environment



Reduce Attack Surface

Security Hygiene

Malware Prevention

© Fortinet Inc. All Rights Reserved.

FortiEDR Machine Learning based Protection

FortiEDR – Real-time & Automated

Visibility + Action

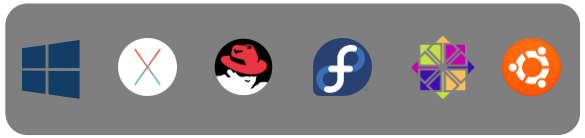
Pre-Infection		Post-Infection/ Post Execution			
Discover & Predict	**Prevent**	**Detect**	**Defuse**	**Respond & Investigate**	**Remediate & Roll back**
Proactive risk mitigation	Pre-execution protection	File-less and advanced threats	Stop Breach and Ransomware	Full attack visibility	Automated Dis-infection
• Discover rogue devices & IoT • Vulnerabilities • Virtual patching	• Kernel-level • Machine learning AV • Application communication control	• Behavioral based • Detect memory based attacks • Threat classification	• Block Malicious actions • Prevent data loss • Zero Dwell time	• Playbook automation • Forensic data • Threat hunting • Big data analytics	• Clean up / Roll back • Eliminate re-image/rebuild • Minimize business disruption

Automation | Cloud . Hybrid . Air-gap deployment | OS coverage

© Fortinet Inc. All Rights Reserved.

What's in FortiEDR

Breadth of Platform Coverage



Fabric Telemetry & Analytics (XDR)

Remove Kernel Dependency

ORACLE LINUX aws

macOS Big Sur

Security Efficacy

Communication Control

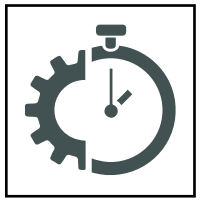
Asset Control

Pre- and Post-infection Protection

CPRL & FortiGuard Integration

Malicious Domain Filtering

SOC Efficiency



Code Tracing Based Forensics

Fabric Powered IR Recipes

Behavior Based Threat Hunting

MITRE Tags

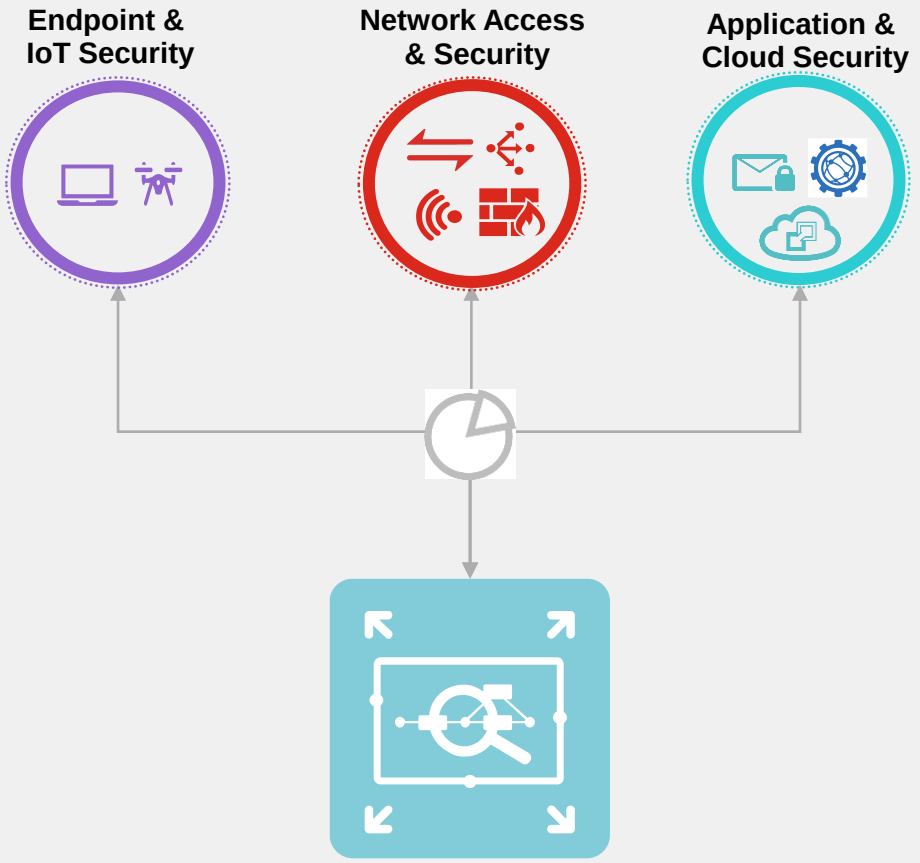
3rd Party IR Integration

© Fortinet Inc. All Rights Reserved.

Introducing FortiXDR

Fully-automated incident detection, investigation and response

- Broad attack surface coverage / telemetry
  - Endpoint, IoT and access for remote work
  - Network, applications and cloud for hybrid
- Cloud-native detection, investigation and response
  - Fortinet curated
  - Easy to add, continually updated
  - Extensible over time
- Improved operational efficiency
  - ¾ reduction in alerts
  - Incident classification in seconds
  - Ability to predefine response actions



© Fortinet Inc. All Rights Reserved.

Managed Detection and Response (MDR)

FortiResponder SOC Services

FortiResponder MDR and Incident Response SOC Services

Delivered by experienced Fortinet analysts
Leverage Fortinet best practice TTPs
24x7 Service, Global availability

FortiResponder services monitor ~600,000 devices across high profile customers

FortiResponder Managed Detection & Response

24x7 Remote Monitoring and Response Service

24x7 continuous threat monitoring
Alert triage and incident handling
Delivered via the FortiEDR platform

FortiResponder Incident Response

Post-breach Remote Forensics & Incident Response Service

Incident analysis, response, containment and remediation
Decrease mean time to resolution (MTTR)
Reduce organizational impact

© Fortinet Inc. All Rights Reserved.

Benefits

FortiResponder Managed Detection and Response

Accelerate SOC Maturity

24/7 - Scale the Existing SOC

Reduce Analyst Burnout

© Fortinet Inc. All Rights Reserved.


FORTINET