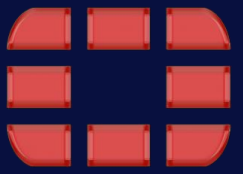
FREEBUF
企业安全俱乐部



威胁情报是高级威胁防御的灵魂

Fortinet 王哲闻

电话：186-1690-1110

Key Words

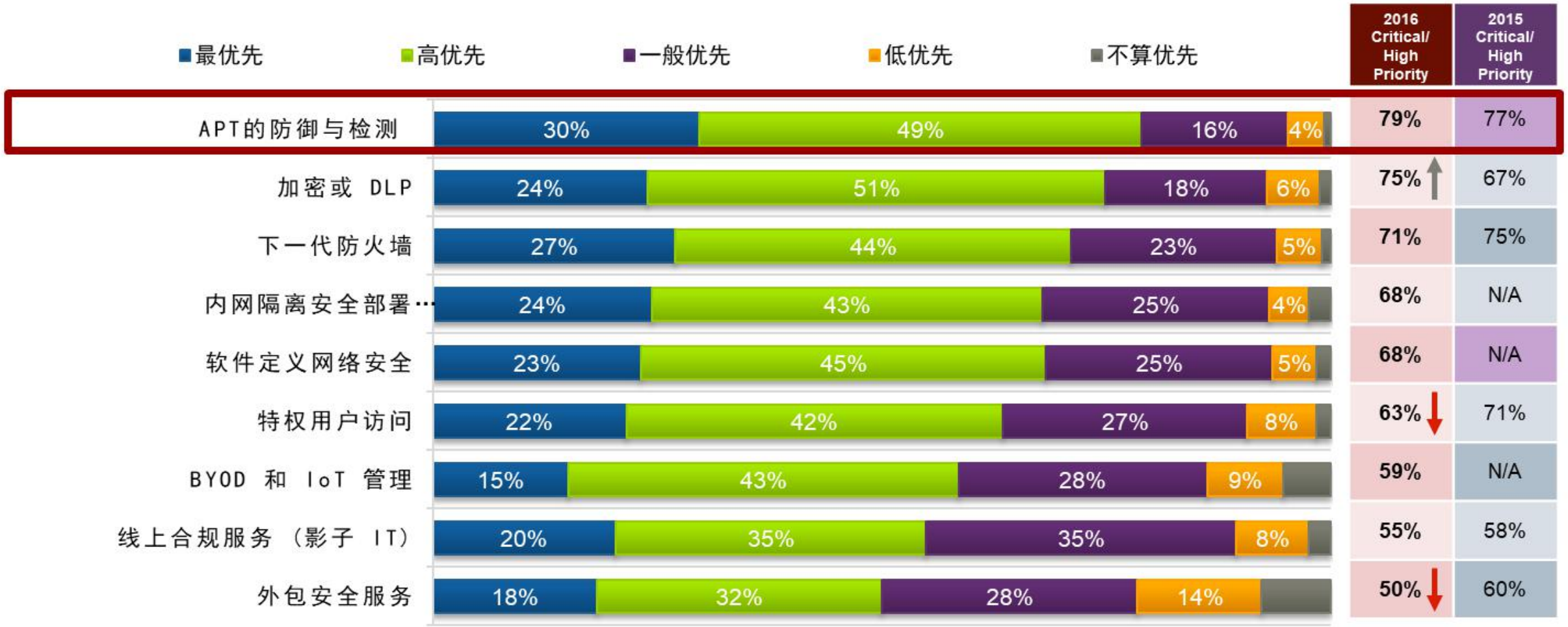
高级持续威胁

APT

威胁情报

TI

高级可持续性威胁（APT）是IT管理者最关注的问题



Source:
IDG Research, January 2016

高级可持续性威胁（APT）是怎么回事

为何一直检测不到？样本的唯一性

99.5%
的恶意文件是有针对性的唯一（变种的）

58
秒内就会感染内部网络

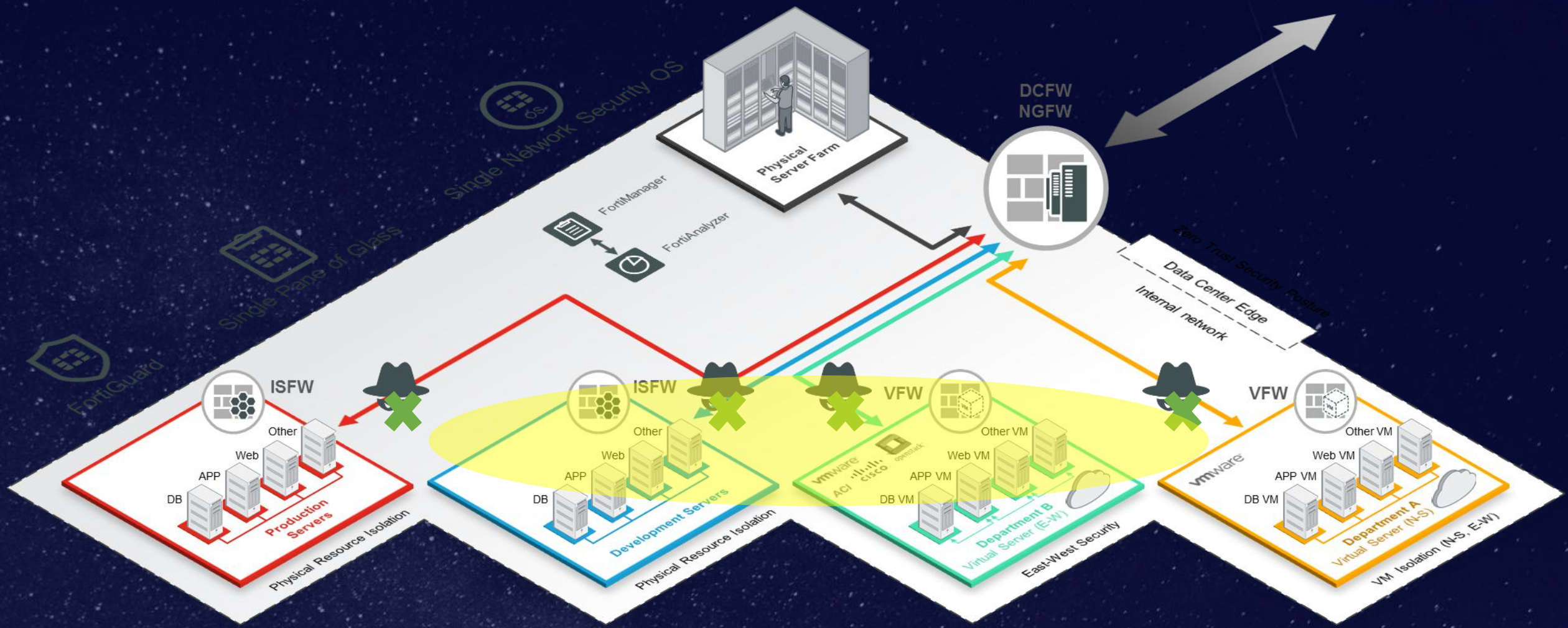
37万 & 6万
入侵 & 恶意文件检测，每分钟

威胁等级	已知无威胁	很大程度上无威胁	有可能无威胁	威胁性未知	有些怀疑	非常可疑	已知威胁
安全技术	白名单	**信誉系统:** 文件，IP，应用，邮件应用签名，数字验证的文件				**启发式信誉验证:** 文件，IP，应用，邮件通用签名	**黑名单特征库**

Sandboxing

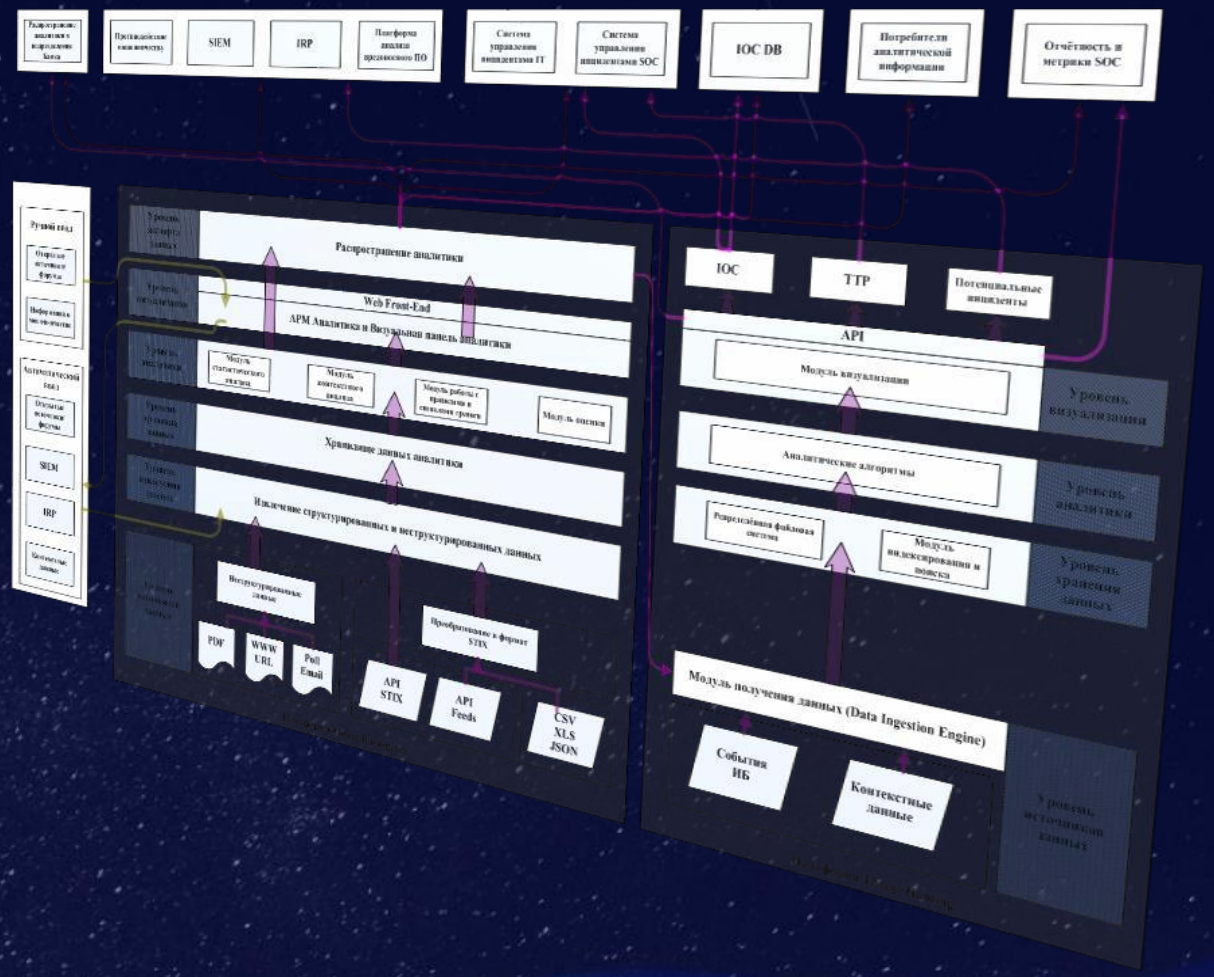
Source:
Verizon 2016 Data Breach Investigations Report, April 2016

高级可持续性威胁（APT）在内网横向移动怎么办？

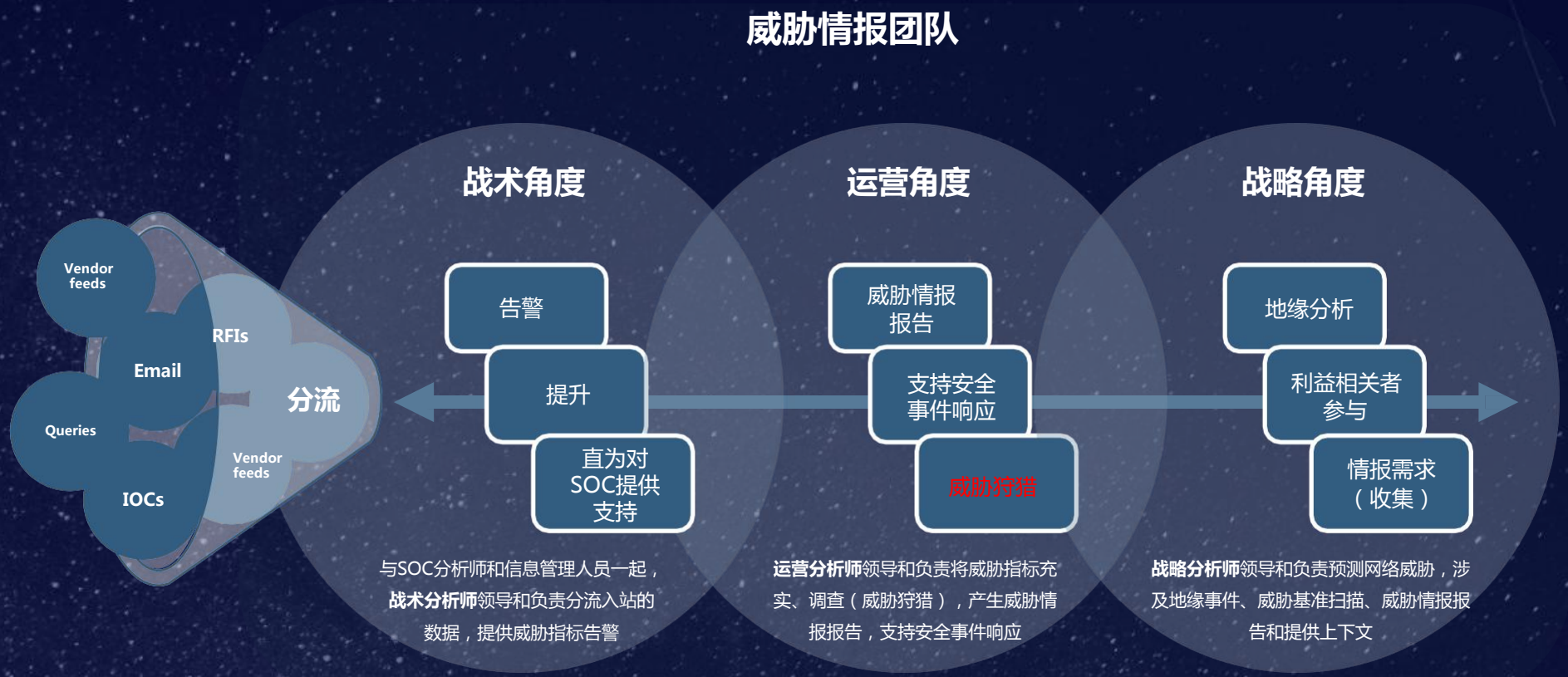


威胁情报功能设计与实施

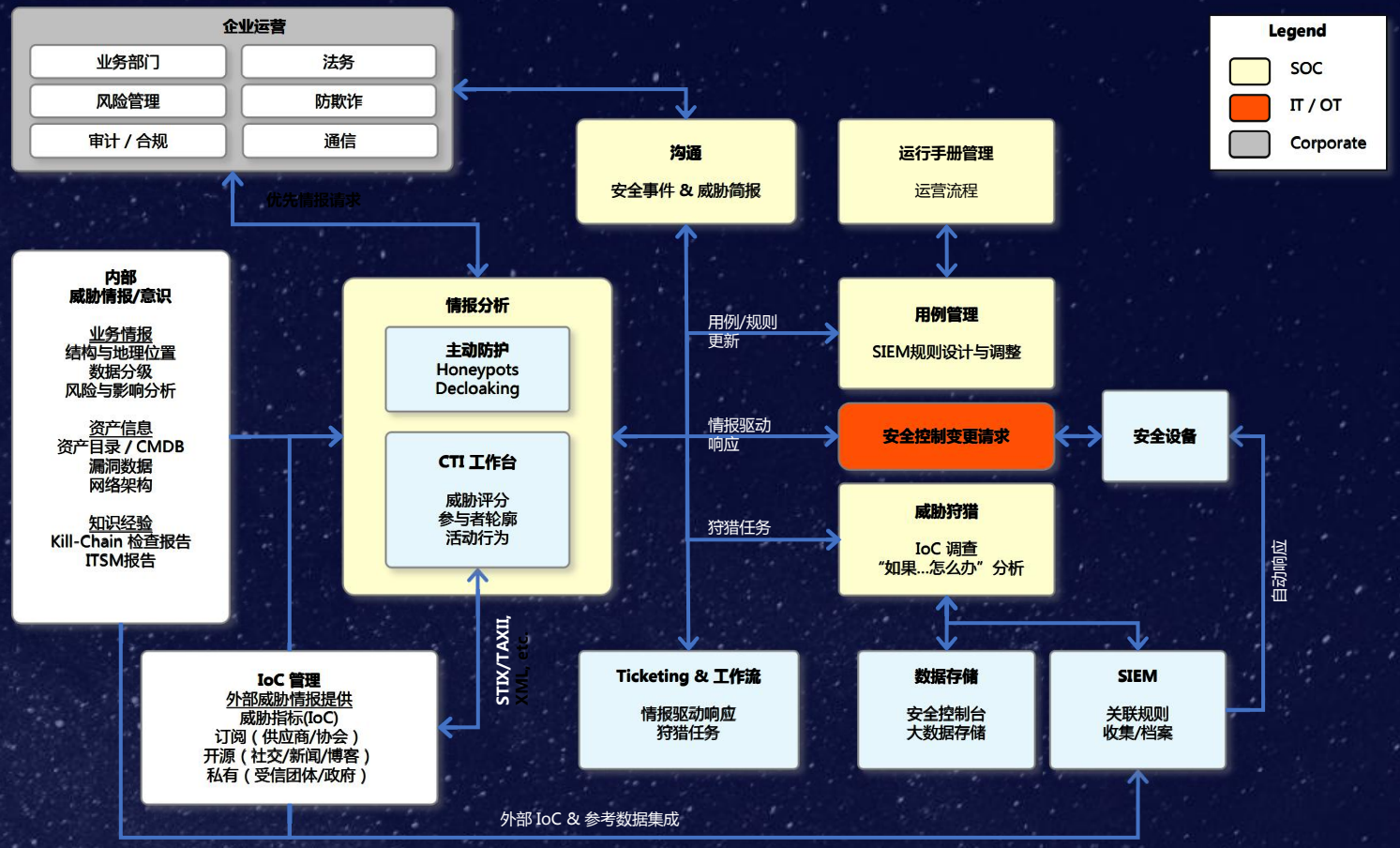
在SOC环境中建立威胁情报功能，这是在日常的SOC操作强制性的指导和协助SOC分析师进行分析，并与业务和风险办公室对接，确保在风险和威胁方面，维持用户暴露于最低限度不变。



威胁情报分析工作应涵盖情报功能的完整连续性



威胁情报运营模型



Fortinet威胁情报输入

全球威胁情报分享机构

MyCERT
Malaysia Computer Emergency Response Team

KISA

ICST

INTERPOL

SAN FRANCISCO
ELECTRONIC CRIMES
TASK FORCE

SOLTRA

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

INFRAGARD
PARTNERSHIP FOR PROTECTION

MALWARE
INVESTIGATOR

UNAM
CERT

STIX

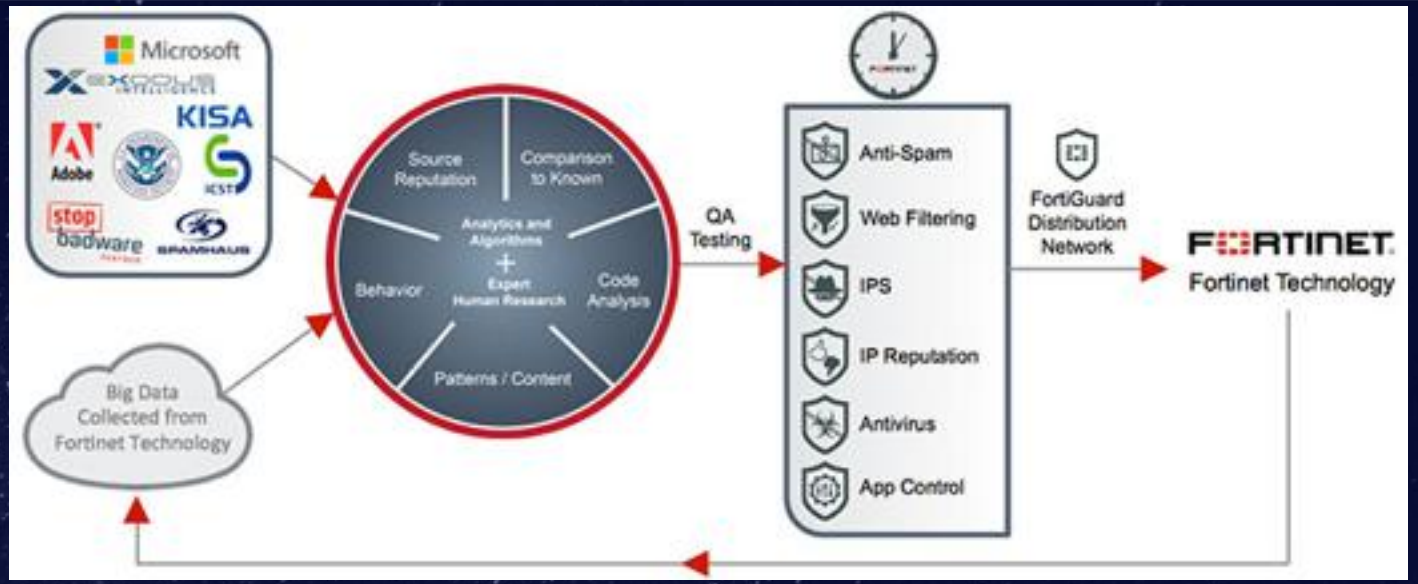
TAXII

MITRE

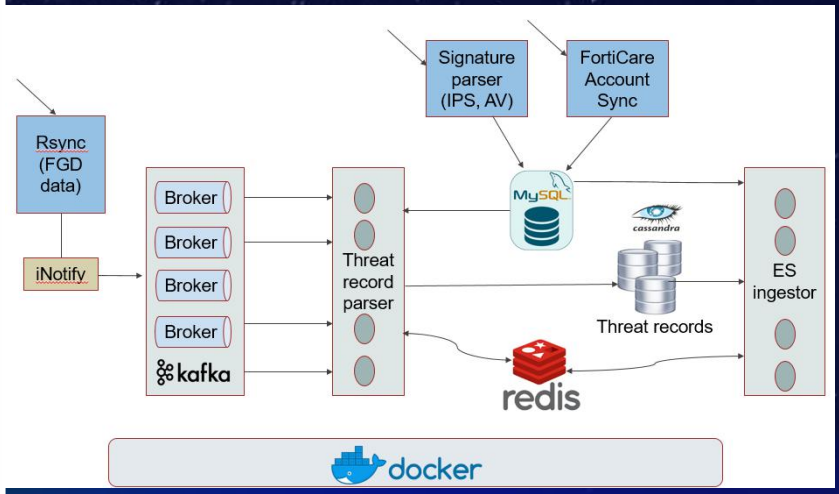
verizon

OASIS
Advancing open standards for the information society

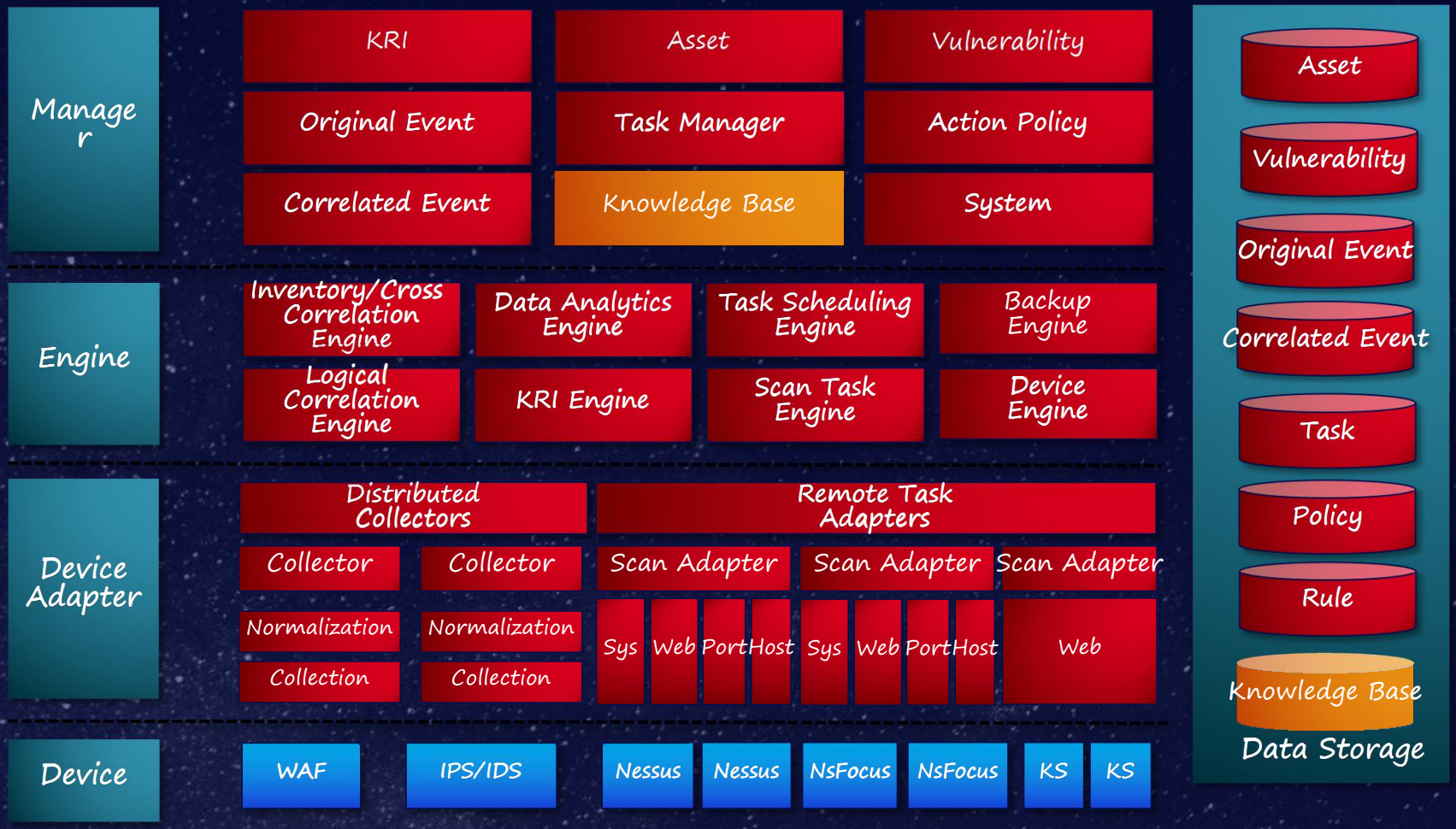
Fortinet威胁情报输出



	Old System	New System
Data amount / day	205 GB	432 GB
Unique IPS sigs / hour	1,450	2,600
Unique Malware sigs / hour	4,400	8,100
Unique devices / day	319,000	463,000



Fortinet威胁情报平台设计架构



Fortinet威胁情报平台闭环

FORTINET SECURITY FABRIC

BROAD

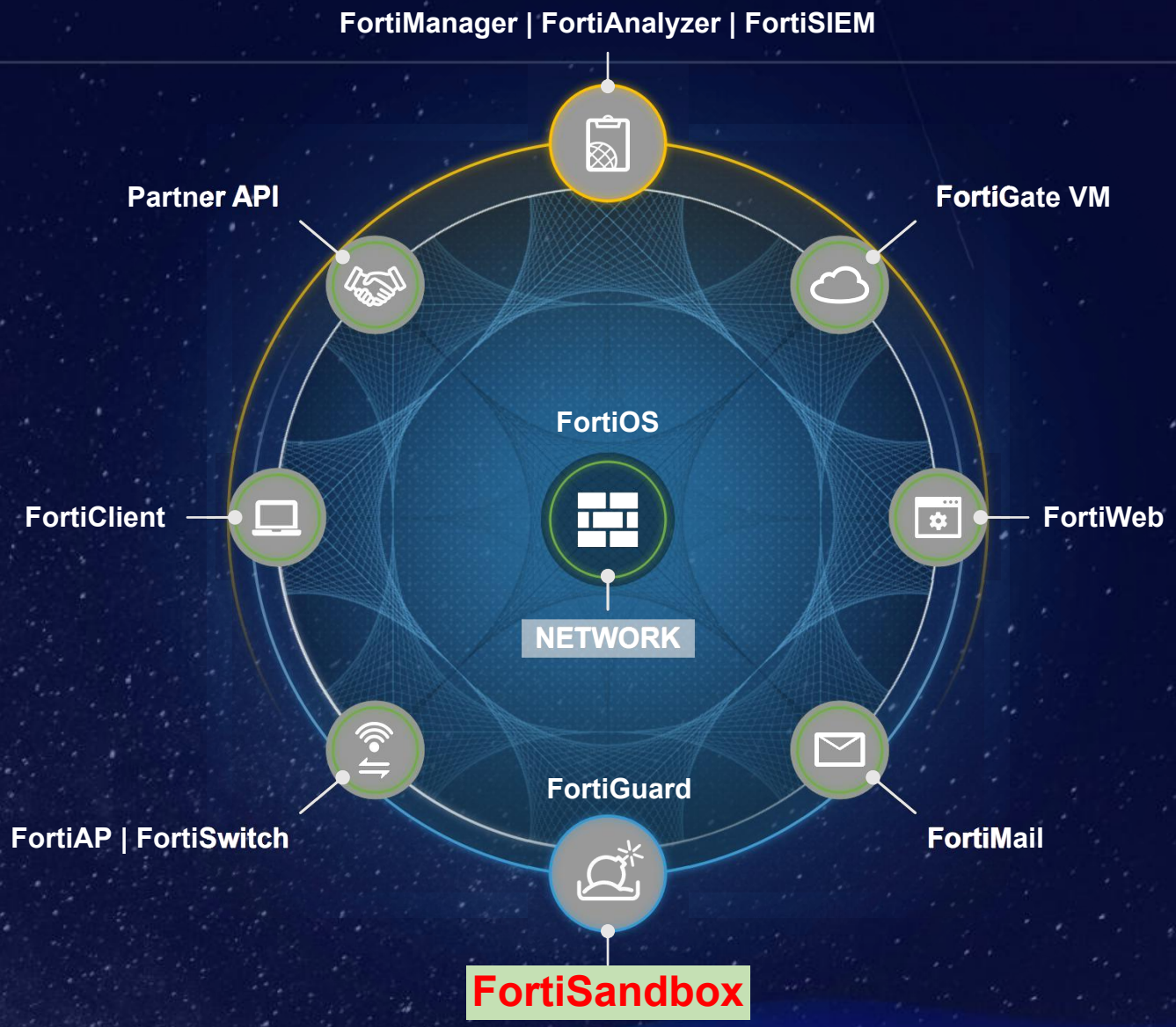
Visibility & Protection of the Digital Attack Surface

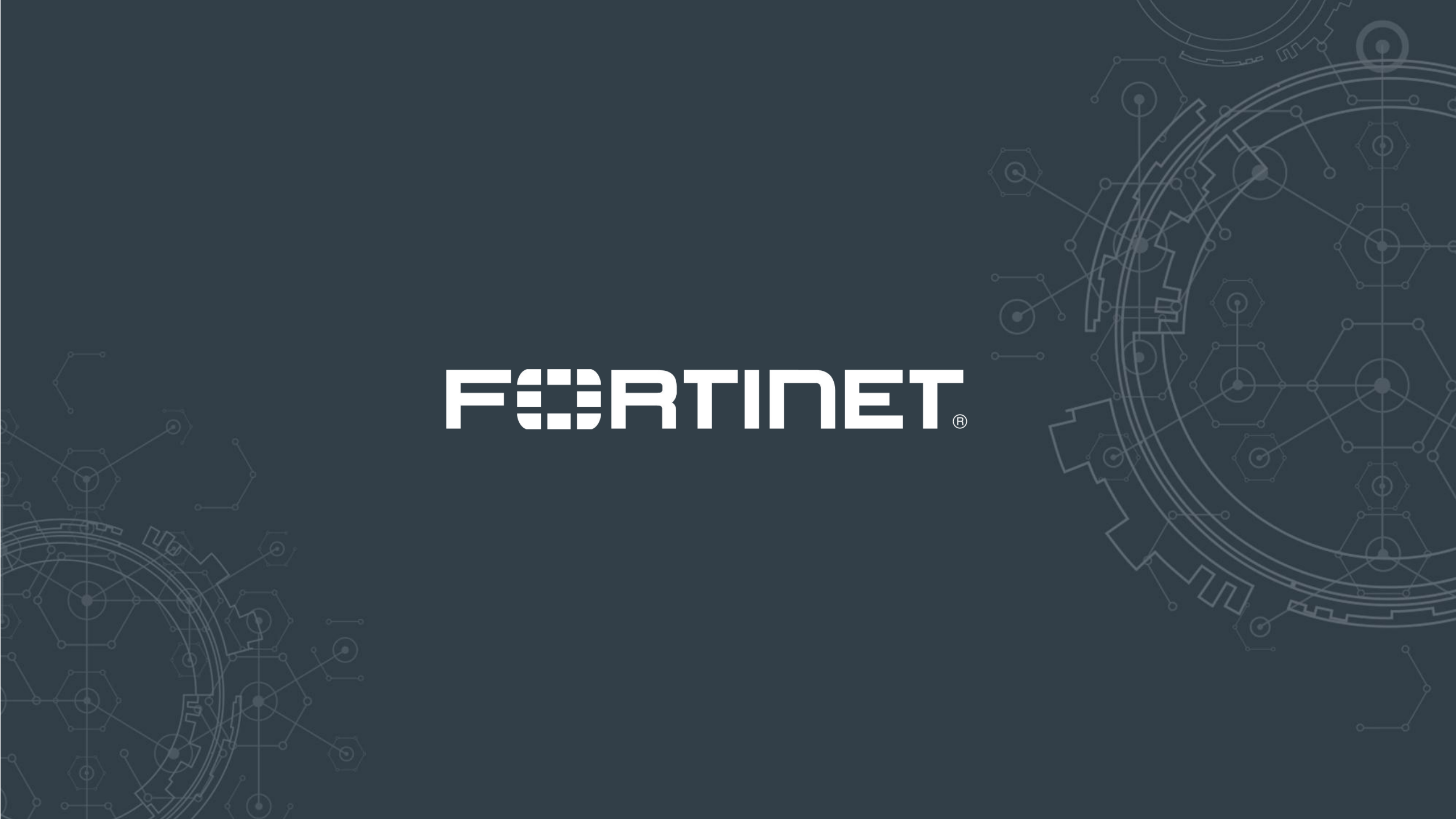
INTEGRATED

Detection of Advanced Threats

AUTOMATED

Response & Continuous Trust Assessment




FORTINET®