# Easily expose attack activity much earlier and protect your business

## Drive Down Risk, Time to Detect and Remediation Effort

**Chris Roberts** – Business Development Manager, Security Operations

# Setting the Scene

The current state of play and security threat landscape

# State of the Nation

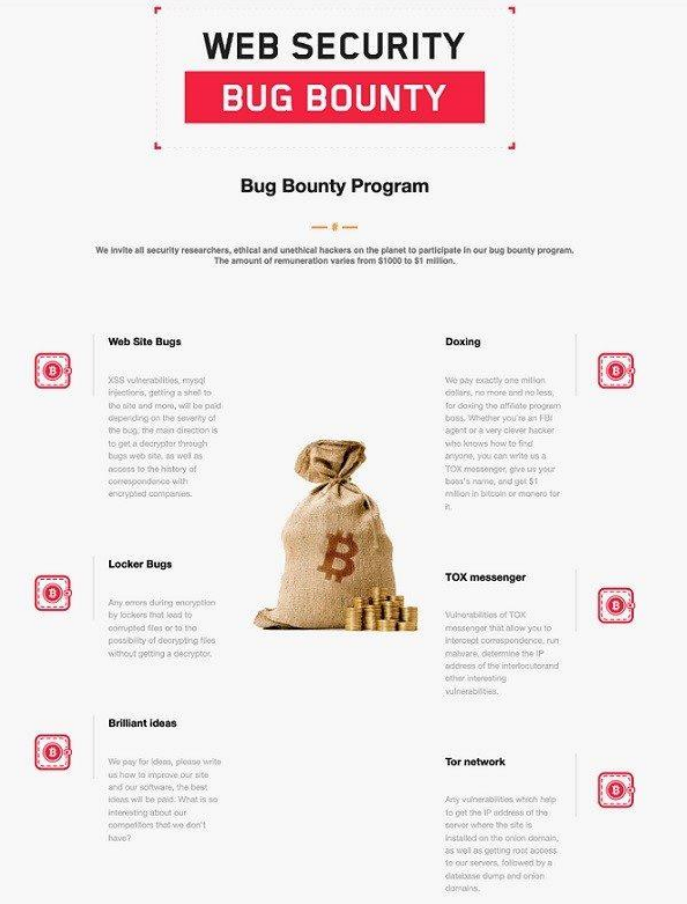
- ***Netgear VPN Routers***
  - 'Multiple security vulnerabilities in its business grade….can't be fixed….replacement router'
- ***Hackers Exploiting Critical Bug in Zyxel firewalls***
  - NSA warned to patch immediately
  - Over 15,000 vulnerable devices online
- ***USB Router Option***
  - Edimax, D-Link, TP-Link, etc routers vulnerable
- ***NAS Vulnerabilities***
  - Potential data theft or code execution
- ***Printer Vulnerabilities***
  - Remote code execution risk
  - Immediate patching advice
- ***Realtek SOC Vulnerabilities***
  - Zero touch exploit – millions of devices
  - Execute code, intercept traffic
  - ASUSTek, Belkin, Buffalo, D-Link, Edimax, TRENDnet, Zyxel, etc


- ***DDoS botnet 'Enemybot'***
  - Uses TOR for C2C
  - Targets routers, IoT and IT devices
  - https://www.fortinet.com/blog/threat-research/enemybot-a-look-into-keksecs-latest-ddos-botnet
- ***Lightning Stealer***
  - Targets 30 browsers
  - Steals bookmarks, browser history, cookies, crypto wallets, Telegram data, Discord tokens, and Steam user's data
  - https://blog.cyble.com/2022/04/05/inside-lightning-stealer/
- ***Onyx Ransomware***
  - Overwrites files larger than 2MB
  - Demands a ransom regardless
- ***Nokoyawa Ransomware***
  - Unique encryption keys
  - Contact through TOR browser

# The Threat Evolves

## Ransomware Gangs are Increasingly Confident

- 10x ransomware infections
- More exfiltration this year
- WFA changing risks
- IT & OT converging
- IoT device explosion
- Attack surface expansion
- As a service capabilities
- Insurance cover changing
- Separation of duties
- Expanded RaaS offers



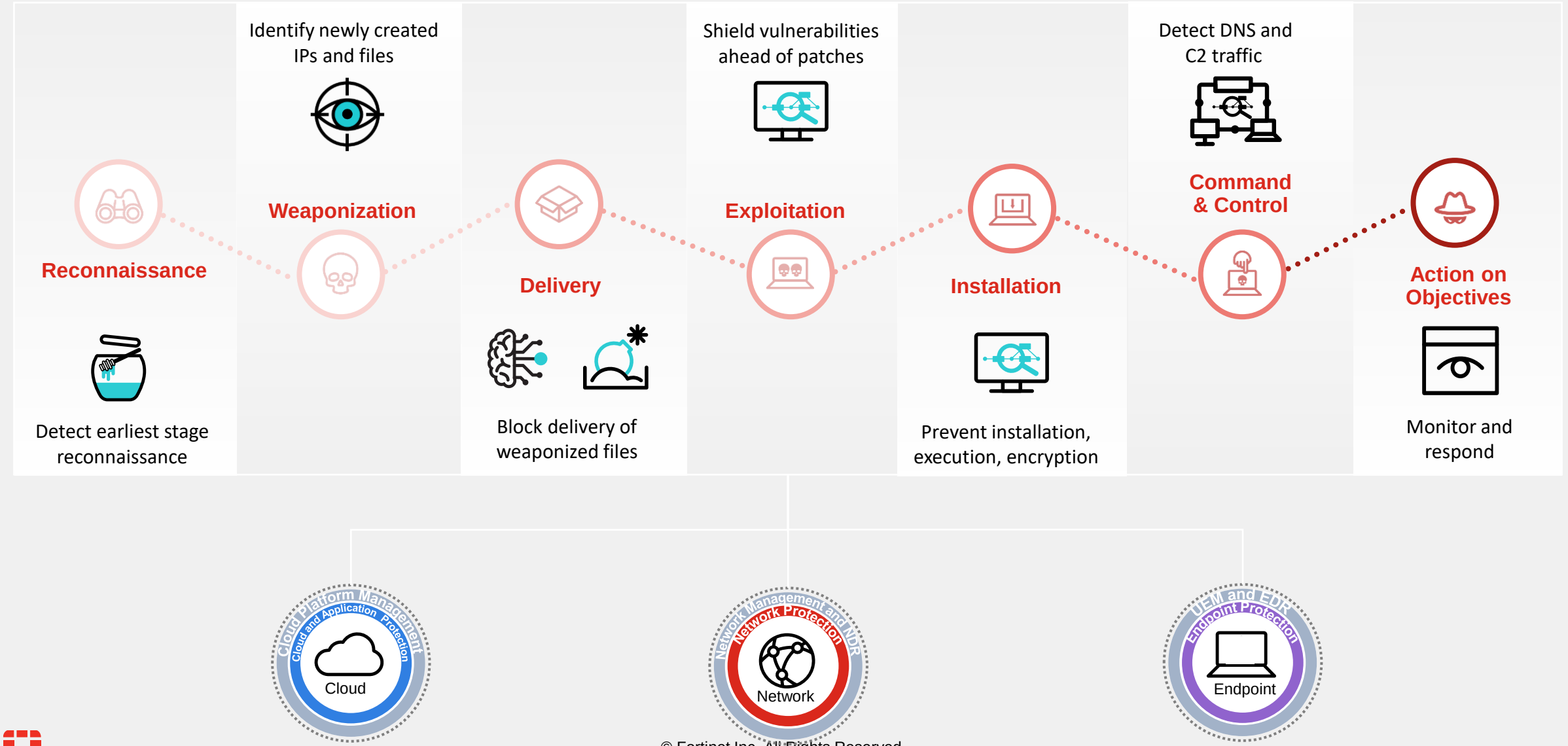

- ***LockBit***
  - In wild since 2019
  - Targets Windows and Linux
  - Version 3.0 debuted in March 2022
  - RaaS model
  - Support services – negotiation, etc
  - 20% fee for use of RaaS platform
  - Critical Infrastructure off limits for encryption only
  - Former Soviet countries also off limits
  - Bug Bounty ($1k - $1m)
- ***RedAlert***
  - Targets Windows and ESXi
  - Multiple threats including DDoS and employee calls
- ***Dark Web Hacker***
  - $3k ransom demand
  - Desktop wallpaper with QR code
  - Deletes shadow copies

# The Numbers Keep Going Up

FortiGuard Lab Statistics - Q2 2022

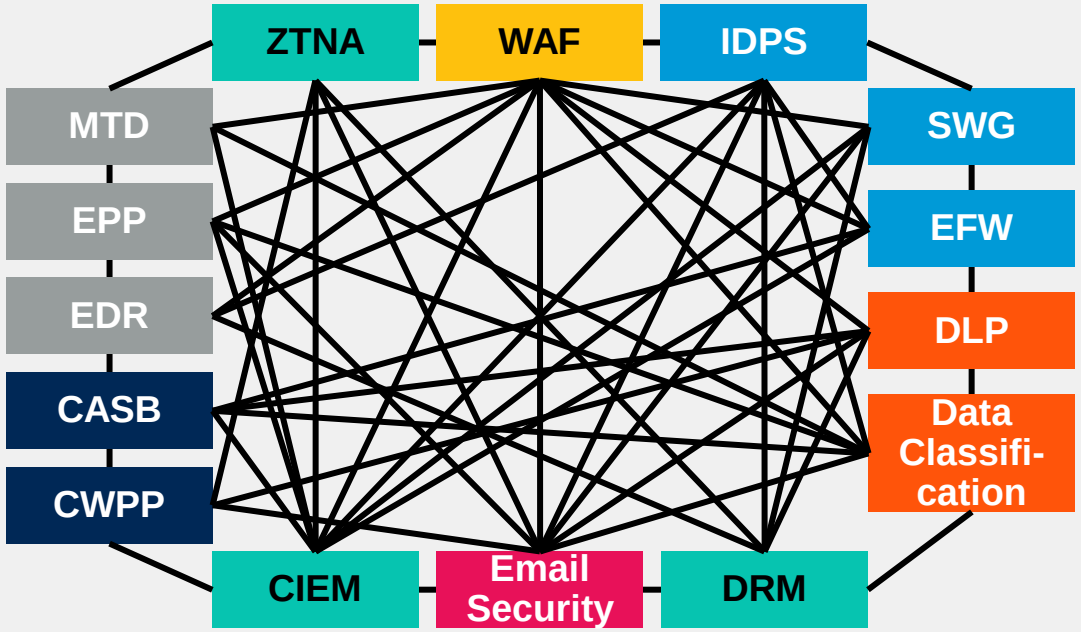
# Integrated, AI-Powered Prevention and Detection

## Across the attack surface and along the cyber kill chain



# Gartner Cybersecurity Mesh Architecture

Gartner



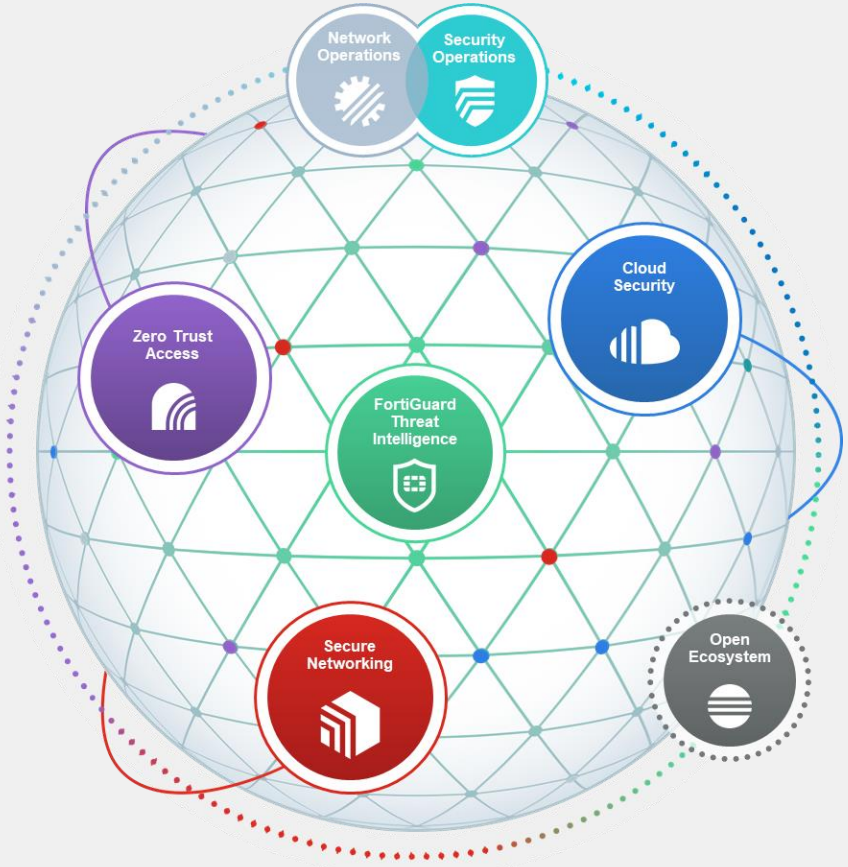

Executive Guide to Cybersecurity Mesh, 2022

Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.

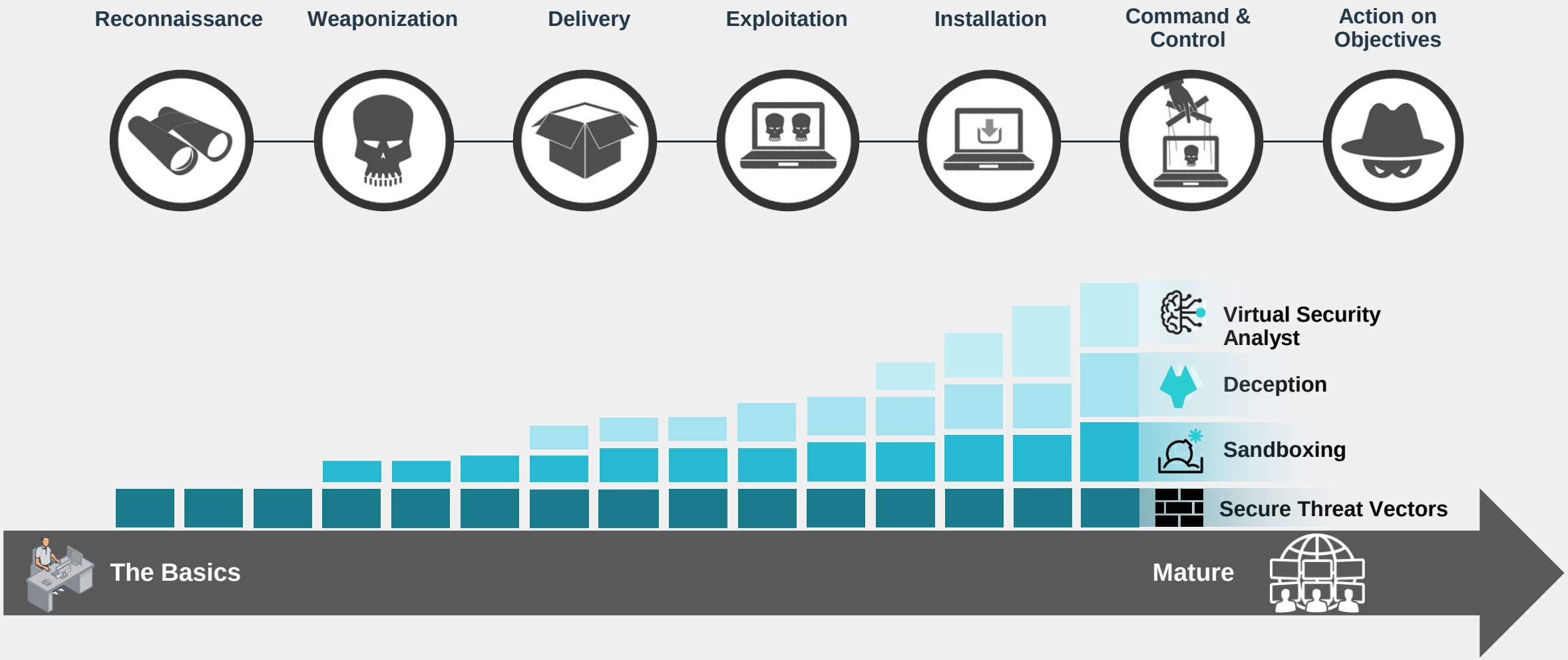
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

FORTINET



# Security Framework for Digital Security

## SOC Maturity Model



# FortiDeceptor

How Deception can be a Critical Component of your Defensive Strategy

# Why Now - Well-defined and Proven Technology

Gartner Coverage

Cyber Deception Technology is recognized by Gartner as the most effective method to detect advanced threats.

*"Prioritize deception-based detection approaches for environments that cannot use other security controls due to technical reasons (for example, IoT, SCADA or medical environments) or due to economic reasons (for example, environments with highly distributed networks)."*

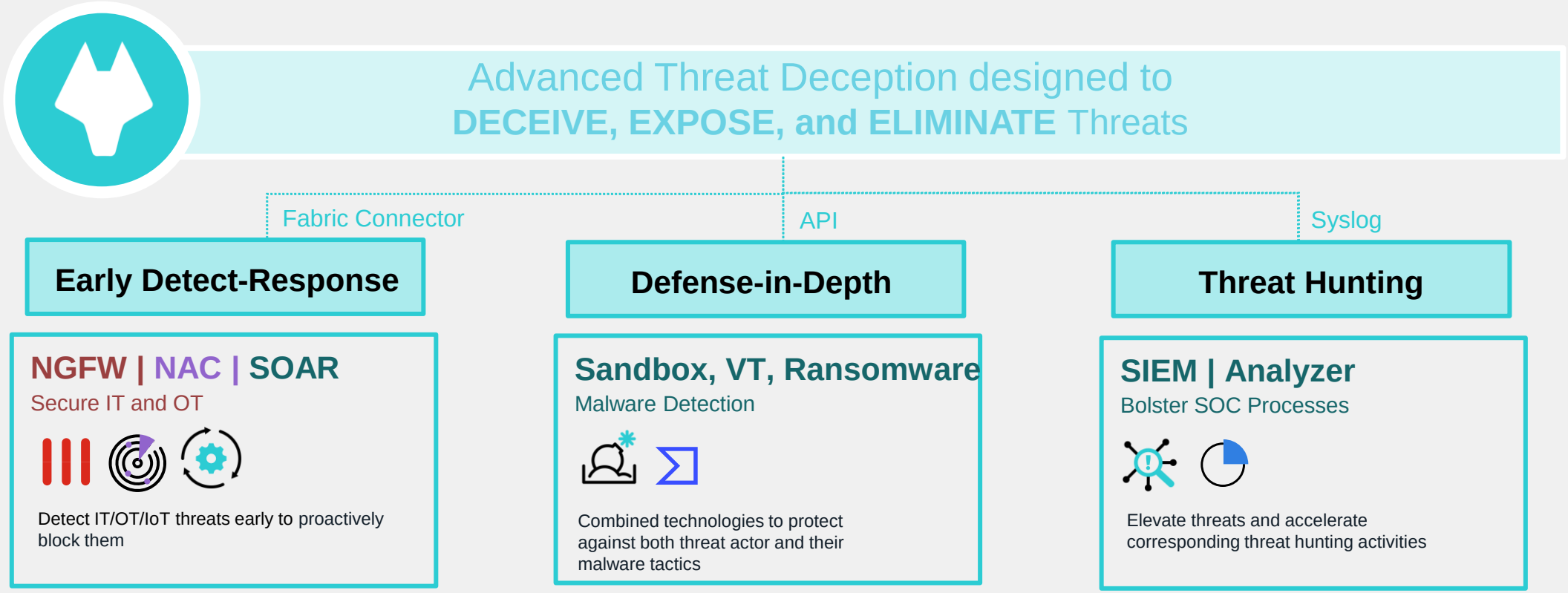
- Gartner Hype Cycle for Threat-Facing Technologies, 2018

*"Security organization dealing with skill-set shortages are prioritizing low friction approaches such as Deception over resource intensive approaches such as SIEM, UEBA, EDR or NTA".*

- Gartner Hype Cycle for Threat-Facing Technologies, 2018

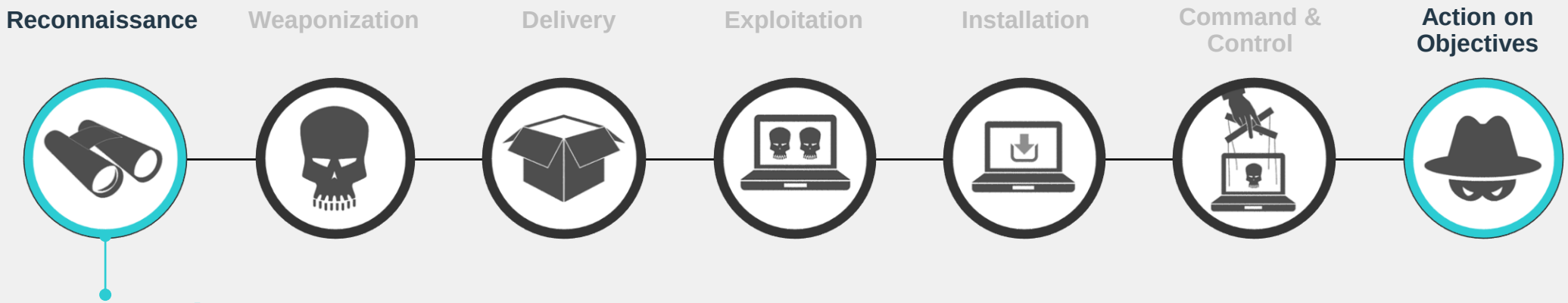
# Use-cases

Early Detect-Response, Defense-in-Depth, Threat Hunting



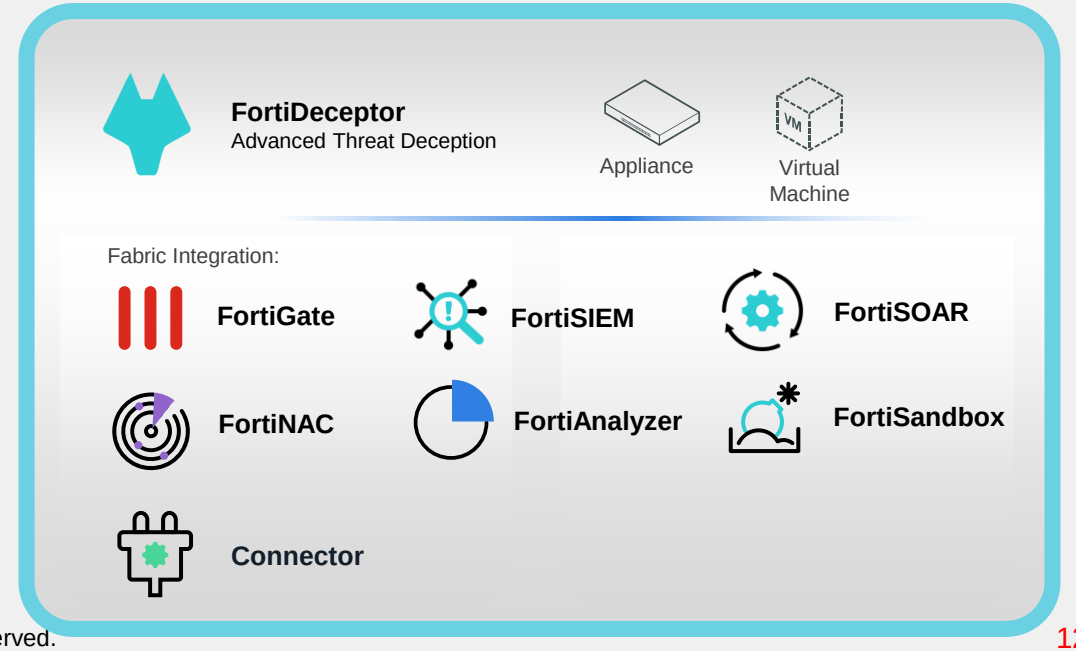
# FortiDeceptor – Deception based Technology

## Disrupt Threat Actors




### Solution

An advanced threat deception designed to DECEIVE, EXPOSE, and ELIMINATE external and internal threats early in the attack kill chain and proactively block these threats before any significant damage occurs.



# Why FortiDeceptor?

**An advanced threat deception designed to DECEIVE, EXPOSE, and ELIMINATE external and internal threats early in the attack kill chain and proactively block these threats before any significant damage occurs.**

**FortiDeceptor**
Advanced Threat Deception

Appliance

Virtual Machine

Fabric Integration:

**FortiGate**

**FortiSIEM**

**FortiSOAR**

**FortiNAC**

**FortiAnalyzer**

1 **Protects both OT and IT**

- SCADA/ICS profile e.g. Rockwell Ethernet/IP, Siemens S7, Bacnet, IPMI, Modbus and etc.
- Windows and Linux with Git, VPN, SMB, SQL, etc. applications, and honeytokens
- Aligns with Purdue Model

2 **Unintrusive and Easy**

- No re-plumbing and taking SCADA/ICS offline
- No operational delay to perform its duties
- Automated discovery of network and assets
- AI-based recommended deployment

3 **Early detection and response**

- Early unambiguous detection of an external/internal threat actor touching a decoy
- Automated response via Security Fabric

# Decoy Potential

## Windows Decoy

- Windows 7
- Windows 10
- Windows Server 2016
- Windows Server 2019

## Windows Lure/ Tokens

- SMB
- RDP
- TCP Port Listener
- SQL (server)
- Cache Credentials
- Fake Network Connection
- HoneyDocs (Office & PDF)
- SQL ODBC
- SAP Connector
- FTP

## VPN Decoy

- FortiOS

## Lures Available

- SSLVPN

## Linux Decoy

- Ubuntu 16.0.4
- CentOS

## Linux Lure/ Tokens

- SSH
- SAMBA
- SMB
- RDP
- GIT
- FTP
- ESXi
- ELK

## IoT Decoys

- Cisco Router
- IP Camera
- Printers (HP, Lexmark, Brother)
- UPS

## Cloud Decoys

- AWS
- AZURE
- GCP

## Application Decoys

- SAP
- ERP
- POS
- Medical

## SCADA Decoy & Lures

- HTTP
- FTP
- TFTP
- MODBUS
- S7COMM
- BACNET
- IPMI
- TRIXONEX
- GUARDIAN-AST
- IEC 60870-5-104
- EtherNet/IP (Rockwell)
- DNP3
- Triconex  (Schneider Electric)


FORTINET