FORTINET

FortiDeceptor
A New Breach Protection Approach

Damien Lim, Product Marketing

Vinay Polurouthu, Technical Marketing

May 14th, 2019

Agenda

- Reality of Breaches
- Introduction to Deception
- Market Opportunity
- Demo
- Resources

Dealing with Breaches

A Deception Approach

The Reality of Data Breaches

Ponemon INSTITUTE

$3.86M Average total cost of a data breach [1]

2/3 Breaches
due to external attacks [2]

1/3 Breaches
due to internal attacks [3]

Minutes
It takes for initial compromise [4]

68% Breaches
took months to discover [5]

Notes/Sources:

1. 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute
2. Top external actor are organized crime as seen in Verizon 2018 Data Breach Report.
3. Top internal actors are Sys admin & end-users as seen in Verizon 2018 Data Breach Report
4. Verizon 2018 Data Breach Report
5. Verizon 2018 Data Breach Report

Icon made by Sherzod Mirzaakhmedov from www.flaticon.com

Compounded By

(ISC)²®

~3M

Global cybersecurity workforce gap

Source: (ISC)² CYBERSECURITY WORKFORCE STUDY, 2018.

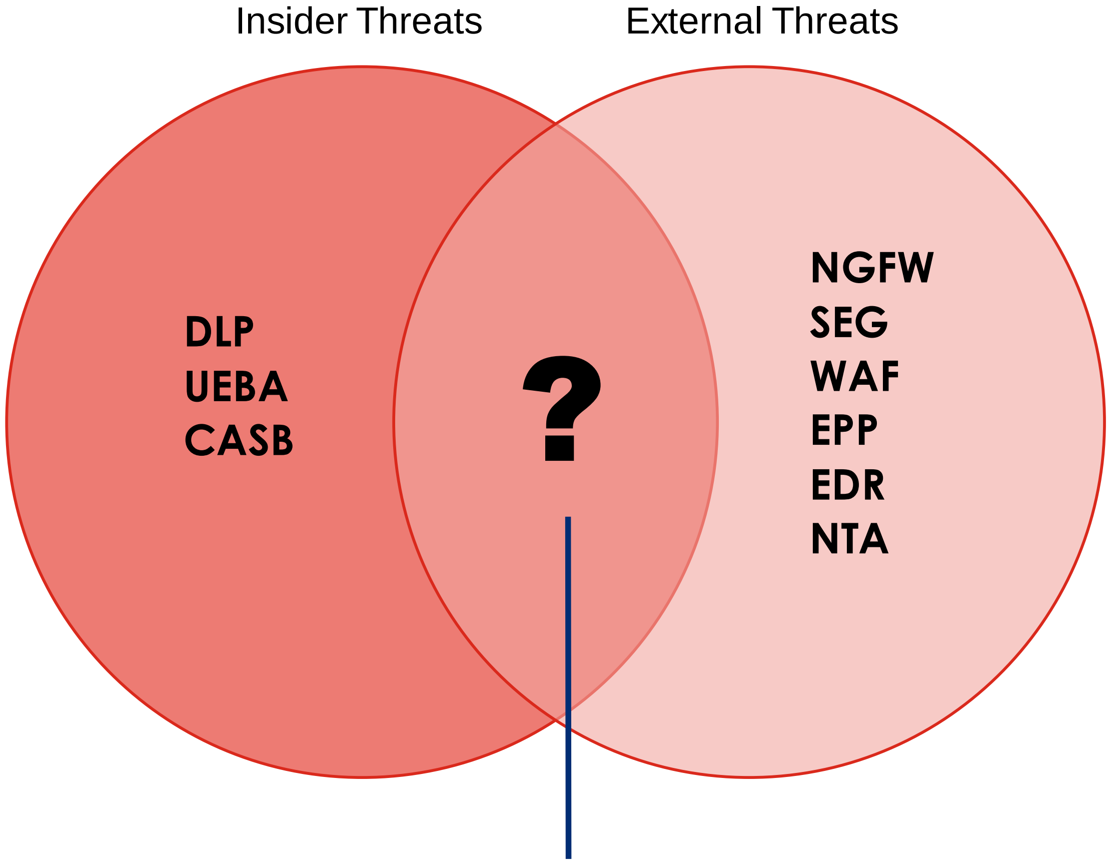
IDC

30

Unique Security Products

Source: IDC. Security Product Taxonomy. 2016.

A Two Solution Breach Protection Approach



Security solutions are focused on

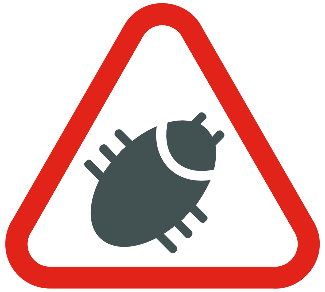
- External Threats or,
- Internal Threats

A solution for BOTH external AND internal threats

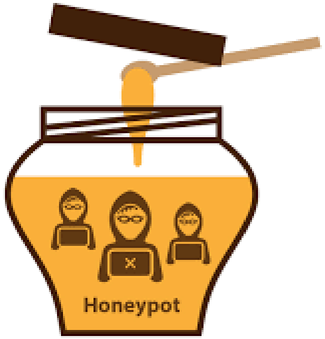
Deception is Widely Used in

Natural world

Human warfare



vs



Cybersecurity warfare

(attack vs defend)

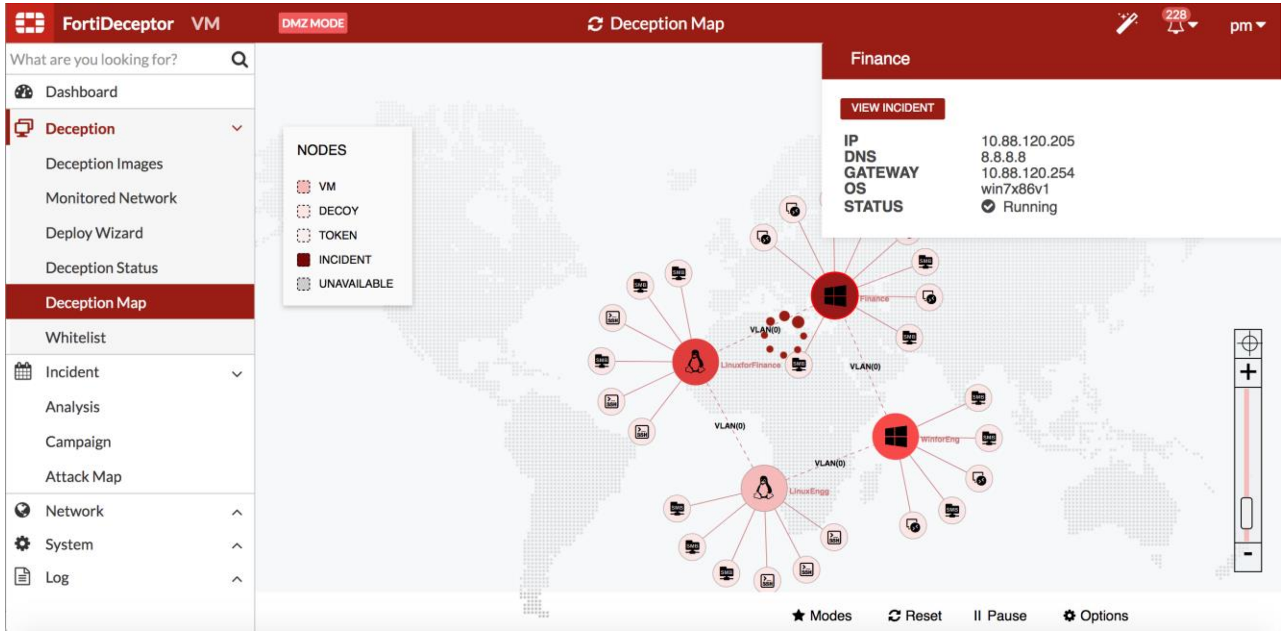
FortiDeceptor: Overview

An advanced threat deception solution that redirects both external and internal threats to decoys for analysis and unambiguous detection.

FortiDeceptor
Advanced Threat Deception

Appliance

Virtual Machine



Finance

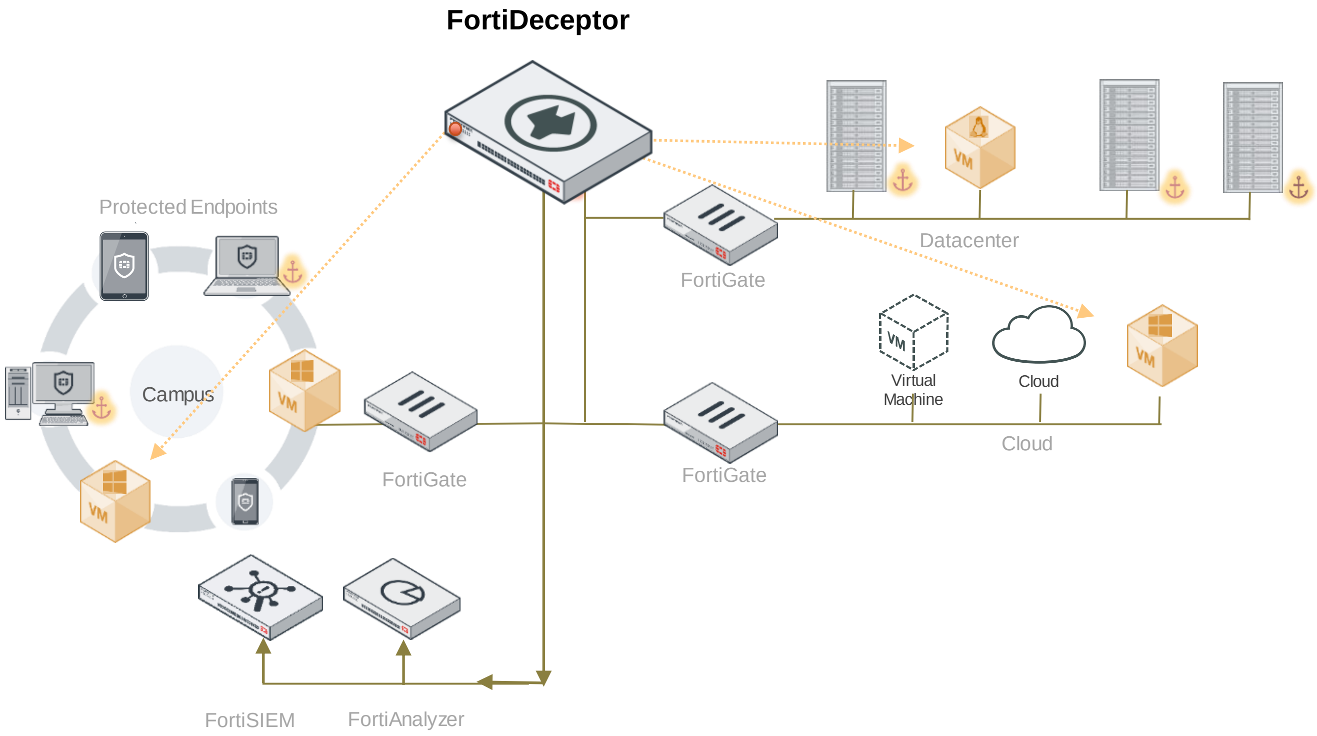
VIEW INCIDENT

IP 10.88.120.205
DNS 8.8.8.8
GATEWAY 10.88.120.254
OS win7x86v1
STATUS Running

* Tools, Tactics, Procedures

FortiDeceptor: LifeCycle

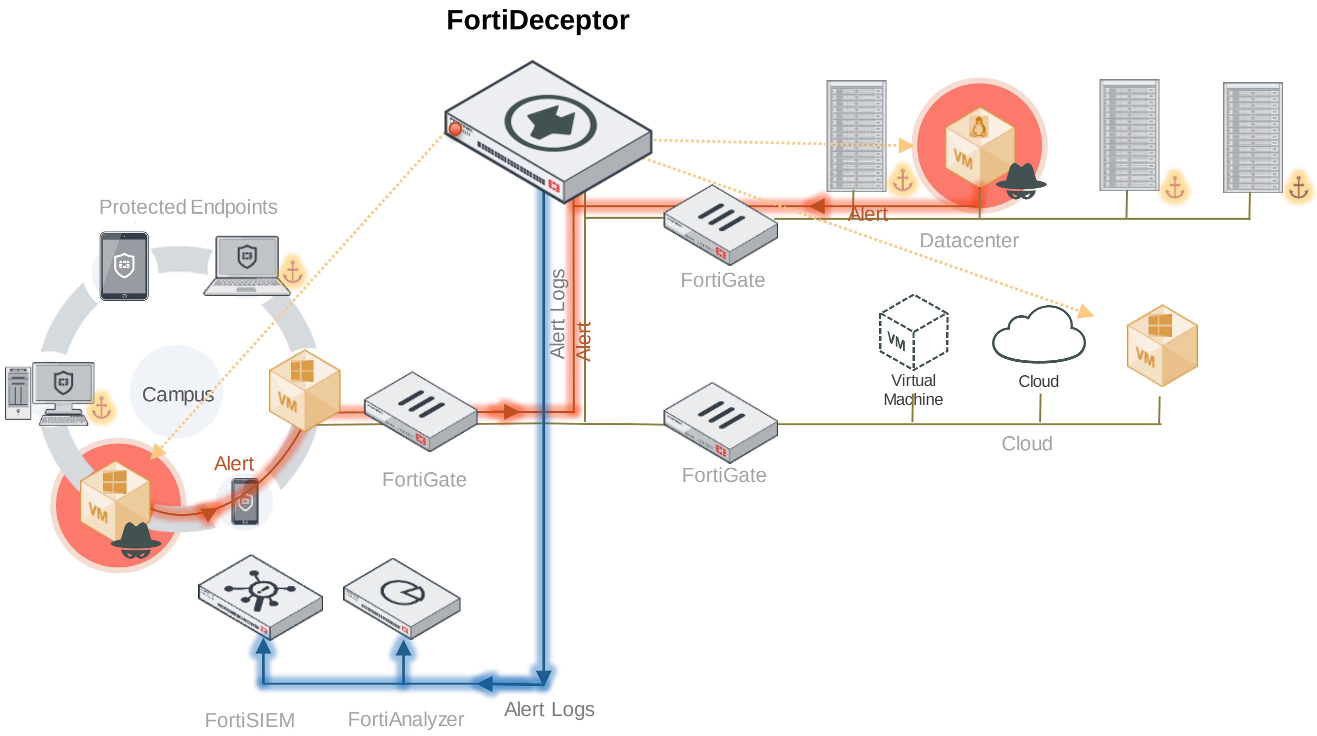
Deceive



- Redirect attacks to decoys that appear indistinguishable from real IT assets and are highly interactive
- Centrally manage and automate the deployment of deception VMs (Windows and Linux) and decoys (data, app, services)

FortiDeceptor: LifeCycle

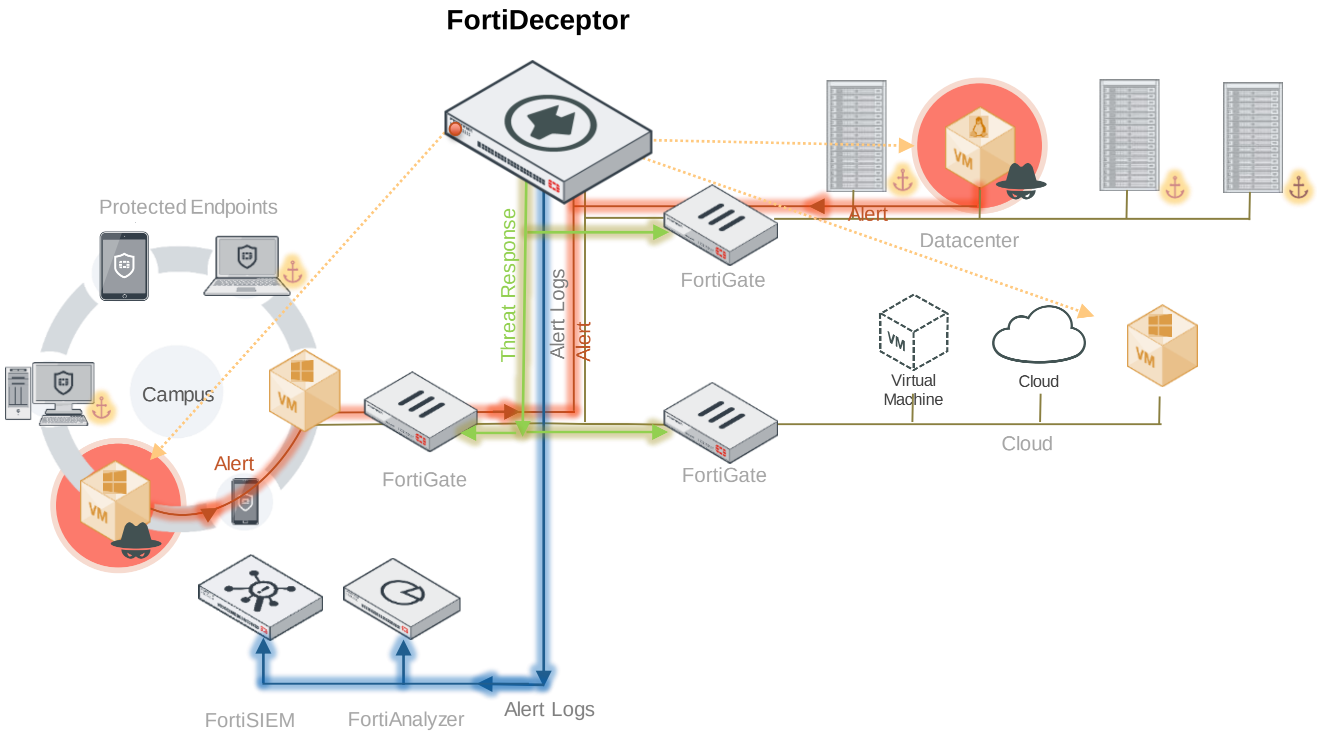
Deceive > Expose



- Acts as an early warning system that generates alerts for review and validation
- Consolidate detection and correlation of external and internal actor activities into a single pane view of threat campaign

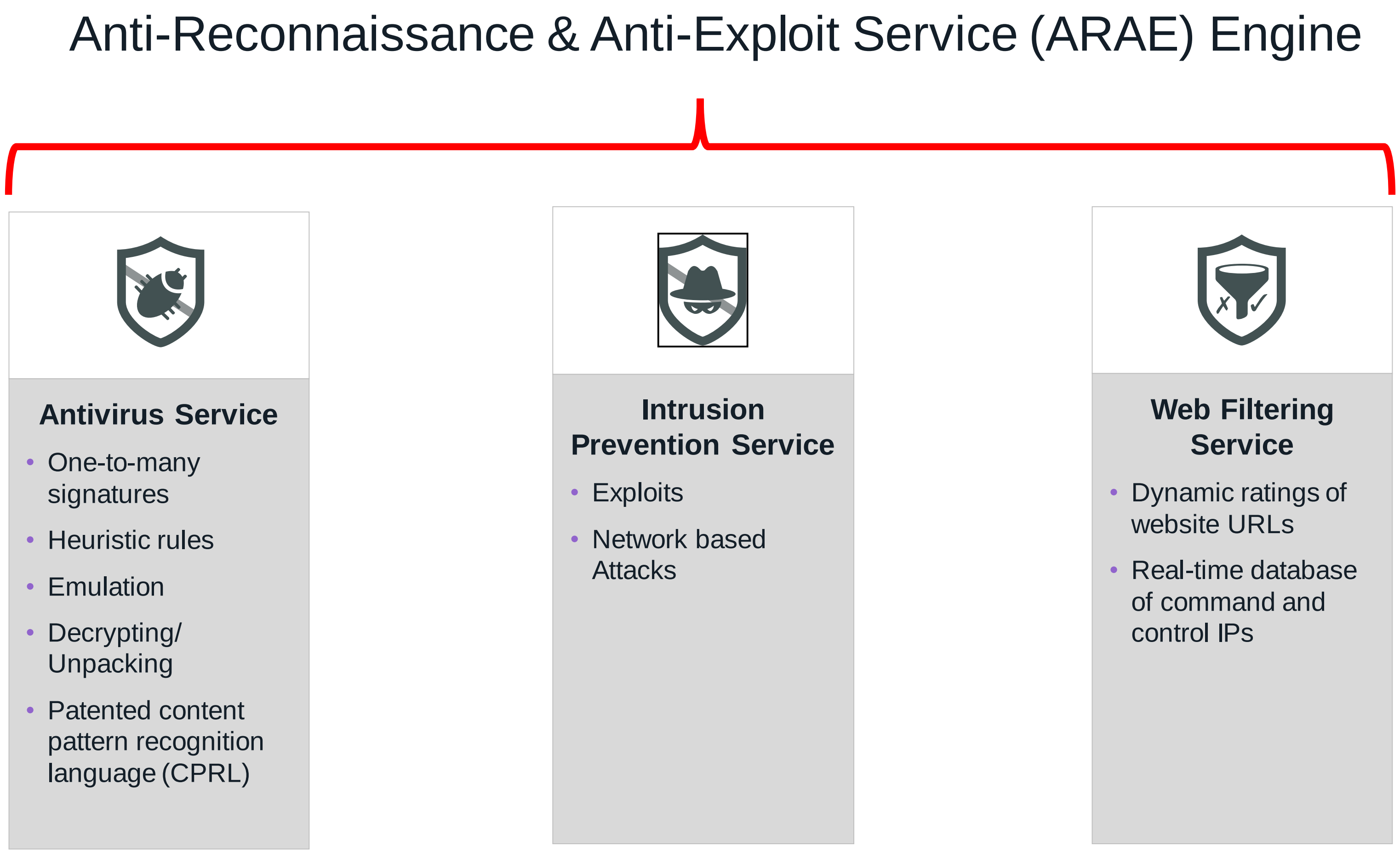
FortiDeceptor: LifeCycle

Deceive > Expose > Eliminate



- Manual/Automatic blocking of attackers before any real damage occurs
- Quarantine external and internal IP address

FortiDeceptor: FortiGuard Services



Anti-Reconnaissance & Anti-Exploit Service (ARAE) Engine

Antivirus Service

- One-to-many signatures
- Heuristic rules
- Emulation
- Decrypting/ Unpacking
- Patented content pattern recognition language (CPRL)

Intrusion Prevention Service

- Exploits
- Network based Attacks

Web Filtering Service

- Dynamic ratings of website URLs
- Real-time database of command and control IPs

SECURED BY FORTIGUARD®

FortiDeceptor: Flexible

DEPLOYMENT

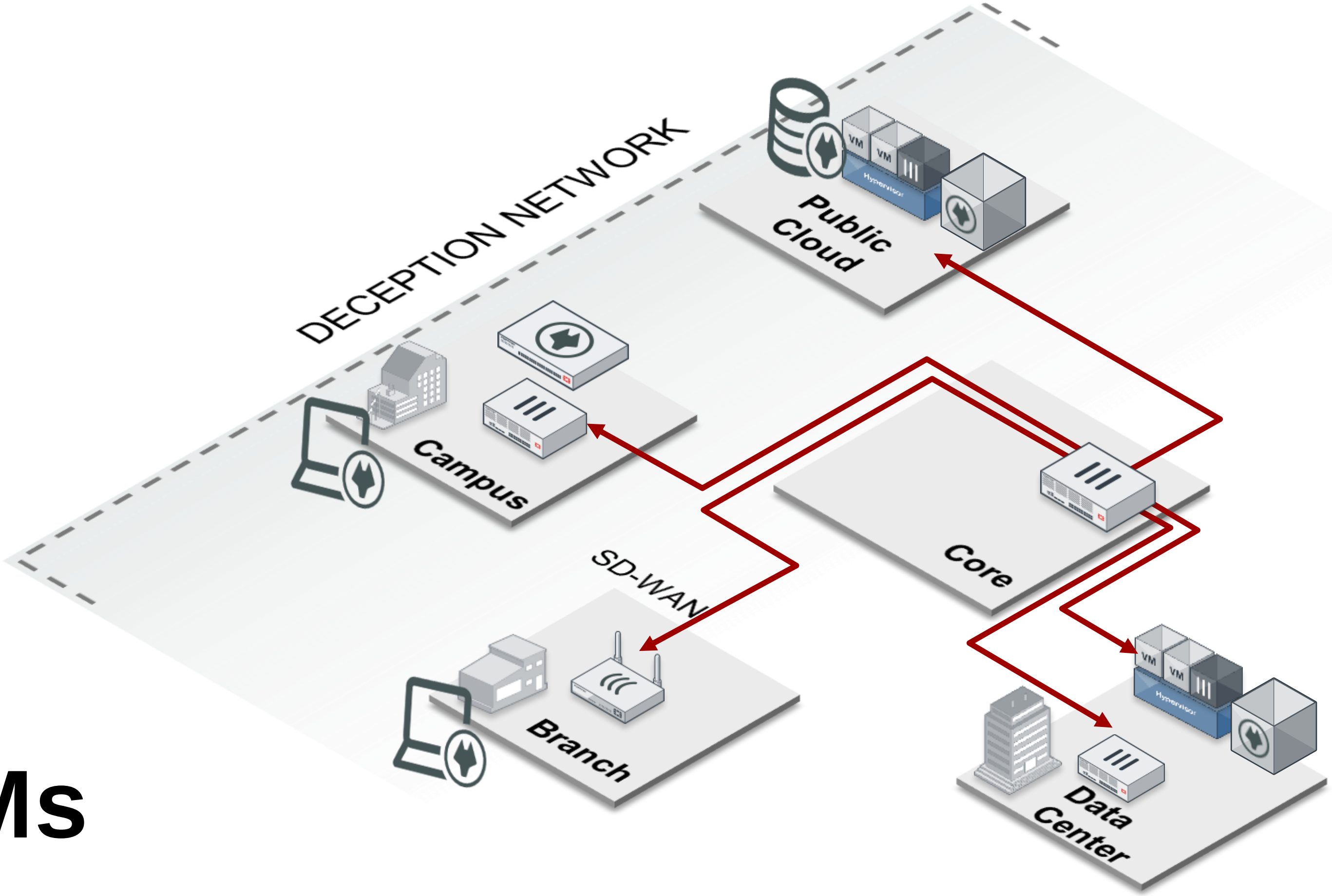
- On-Premise
- Public Cloud

DECOYS

- Branch
- Campus
- Data Center/Public Cloud

DECEPTION VMs

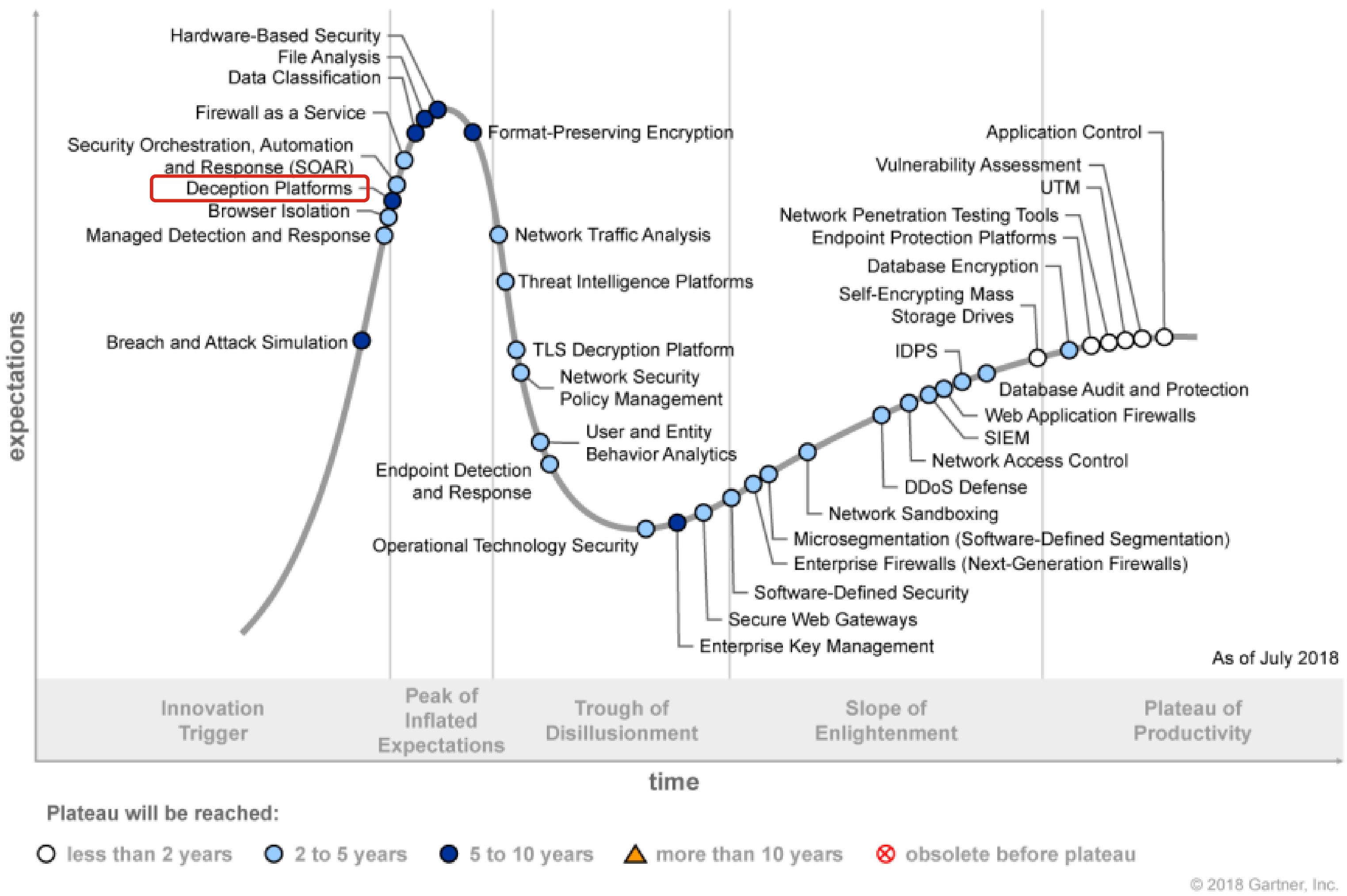
- Windows
- Linux



Market Opportunity

Deception is in the Early Stage

Figure 1. Hype Cycle for Threat-Facing Technologies, 2018



Source: Gartner (July 2018)

Deception Market Opportunity

Industry Analysts estimates*

$2.09B in 2021
(15% CAGR)

Strategic Assumption #1

By 2022, 25% of all threat detection and response projects will include deception features and functionality, either embedded in their current vendor's threat detection technology stack or through pure-play deception platforms, up from 5% today.
- Gartner 'Improve Your Threat Detection Function With Deception Technologies', 2019

Strategic Assumption #2

By 2022, only 5% of existing deception vendors will remain as stand-alone companies, and they will do so as specialists. The other 95% will be acquired, pivot market strategies or fail to maintain solvency.
- Gartner 'Deception Solution Providers Must Prepare for Market Consolidation', 2018

FORTINET

*No concrete data from major analysts e.g. Gartner, IDC, Forrester, Frost&Sullivan, etc

Fabric Enabled Deception is

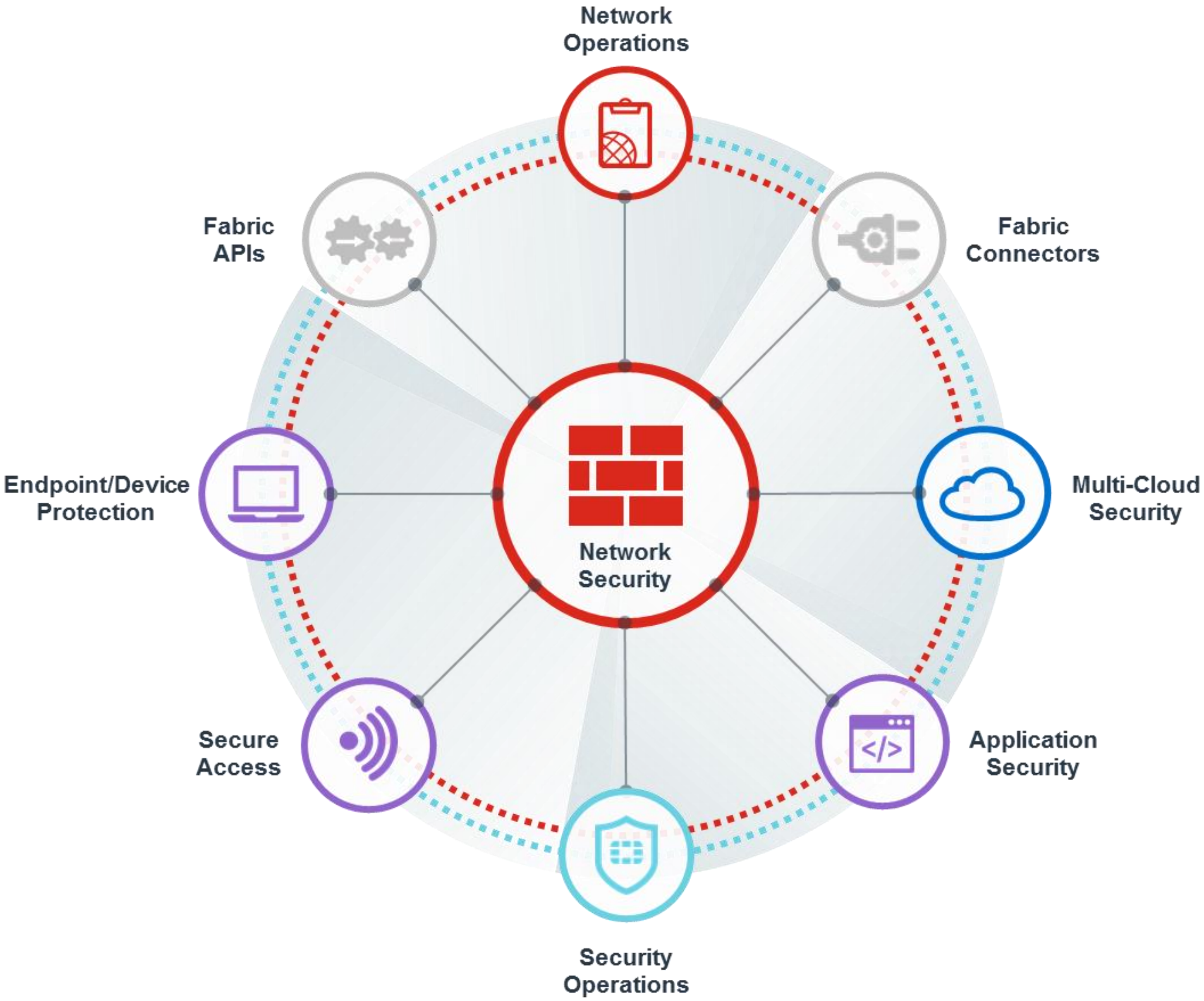
Breach protection approach that leverages deception to uncover external and internal threats early in the attack cycle and proactively block these threats before any significant damage occurs.

FortiDeceptor
Advanced Threat Deception

FortiSIEM

FortiGate

FortiAnalyzer



Q1FY19 v1.4.3

* Tools, Tactics, Procedures

Wait, How is this different than Sandbox?

	Advanced Threat Protection	
	FortiSandbox	**FortiDeceptor**
Goal	Deceive **suspicious object** to run in a simulated environment	Deceive an **attacker** into compromising a deception VM
Detection	Captures **malware behavior** to alert on malicious intent	Captures **attacker's behavior** to alert on malicious intent
Response	Share IoCs to provide real-time protection **during breach attempt**	Share IoCs to provide real-time protection **before breach attempt**
Attack Lifecycle/Cyber Kill Chain (Earliest Response)	**Mid stage**: Blocks exploitation and installation of unknown malware stage	**Early stage**: Redirects reconnaissance and blocks pre-breach attempts

They are complementary technologies

Account Profile

- Gartner Type A Enterprise aka ‘Lean forward Organization’
- Revenue: $1B or more
- Employee: 1,000 or more
- Business Unit: Security Operations
- Persona: CISO, Security Architect
- Products/Technology deployed: Sandbox, EDR, NGFW, SIEM, UEBA, NTA, SOAR, TIP
- Top 3 segments: Global financial services, healthcare, and government

Next Generation Fire Wall (NGFW), Endpoint Detection and Response (EDR), Security Information & Event Management (SIEM),
User & Entity Behavior Analytics (UEBA), Network Traffic Analysis (NTA), Security Orchestration, Automation & Response (SOAR), Threat Intelligence Platform (TIP)

Strategic Comparison

Strategic Assumption #2

By 2022, only 5% of existing deception vendors will remain as stand-alone companies, and they will do so as specialists. The other 95% will be acquired, pivot market strategies or fail to maintain solvency.

	Fortinet	Attivo Networks	TrapX	Illusive Networks
Acquisition	N/A, organically developed	Integration lead time prior, during and after	Integration lead time prior, during and after	Integration lead time prior, during and after
Global support	• 7 regional support centers • round-the-clock	US, India, Dubai support	US and UK support	US and Israel support
Product longevity & Roadmap commitments	1.7B cash 385,000 customers	Series C funding (44M) 100+ customers	Series B funding (28.6M) 300+ customers	Series B funding (30M) customers (not disclosed)
Native integration	FortiGate, FAZ, FSM	API Quarantine- major NGFW, Endpoint, Proxy, NAC partners	API Quarantine – major Endpoint, limited NGFW and, NAC partners	(not disclosed)
Automated Protection based on	IP	IP	IP	(not disclosed)

FortiDeceptor Ordering

1

Form Factors

- Appliance (FDC-1000F)
- VM (FDC-VM)

2

Licenses/Capacity

- VM Host based
- SKUs additive to accommodate more VMs (max 16 for appliance / VM)
- Flexibility to mix and match Windows and Linux VMs

3

Service/FortiCare

- 24x7 FortiCare
- ARAE (Anti-Recon & Anti Exploit)

Bundles

- N/A

SKU	DESCRIPTION
FDC-VM	FortiDeceptor-VM virtual appliance with 0 VMs, upgradable to max 16 VMs (256 decoys)
FDC-1000F	FortiDeceptor 1000F Appliance with 2 WIN VMs (include 1x Win7 and 1 x Win10 licenses) and 8 Linux VMs, upgradable up to max 16 VMs (256 decoys)
FDC-UPG-LNX	Expands FortiDeceptor capacity by 2 Linux VMs
FDC-UPG-WIN	Expands FortiDeceptor capacity by 2 Windows VMs. Includes 1 x Win7 and 1 x Win10 licenses

Note: ITF for 60 day evaluation license available

Demonstration

Vinay Polurouthu

Summary

BREACHES
External and Internal threats

EARLY WARNING
Redirect Attacks, Analyze and Respond

FABRIC INTEGRATION
Actionable visibility and block threats automatically

BROAD COVERAGE
Branch, Campus, and Cloud

EASE OF USE
Wizard-based provisioning and deployment, simple management

Resources

FUSE >> *Navigate to Marketing >> Products >> FortiDeceptor*

- Customer facing deck, Solution Brief, FAQ, Roadmap
- Discuss on ATP forum and FortiDeceptor forum

FortiDeceptor demo: https://www.fortinet.com/fortidemo.html

FortiDeceptor team

- Product: Jack Chan (Product Management), Damien Lim (Product Marketing), Vinay Polurouthu (Technical Marketing)
- Field Experts: Kevin Mahoney and Kash Valji

FORTINET®