FORTINET®

FortiDeceptor

Integra OneCon

Chris Breger - Systems Engineer

Kevin Thibault - Systems Engineer

Fortinet is one of the largest cybersecurity companies in the world.

Founded: **October 2000**

Founded by: **Ken Xie and Michael Xie**

Headquarters: **Sunnyvale, CA**

Fortinet IPO (FTNT): **November 2009**

Listed in both: **NASDAQ 100 and S&P 500 Indices**

Member of: **2023 Dow Jones Sustainability World and North America Indices**

Global Customer Base
775K+
Customers

1,354
Global Patents

2023 Billings
$6.4B+
(as of Dec. 31, 2023)

~$2.5B+
Investment in Innovation since 2017, with 91% R&D
(as of Dec. 31, 2023)

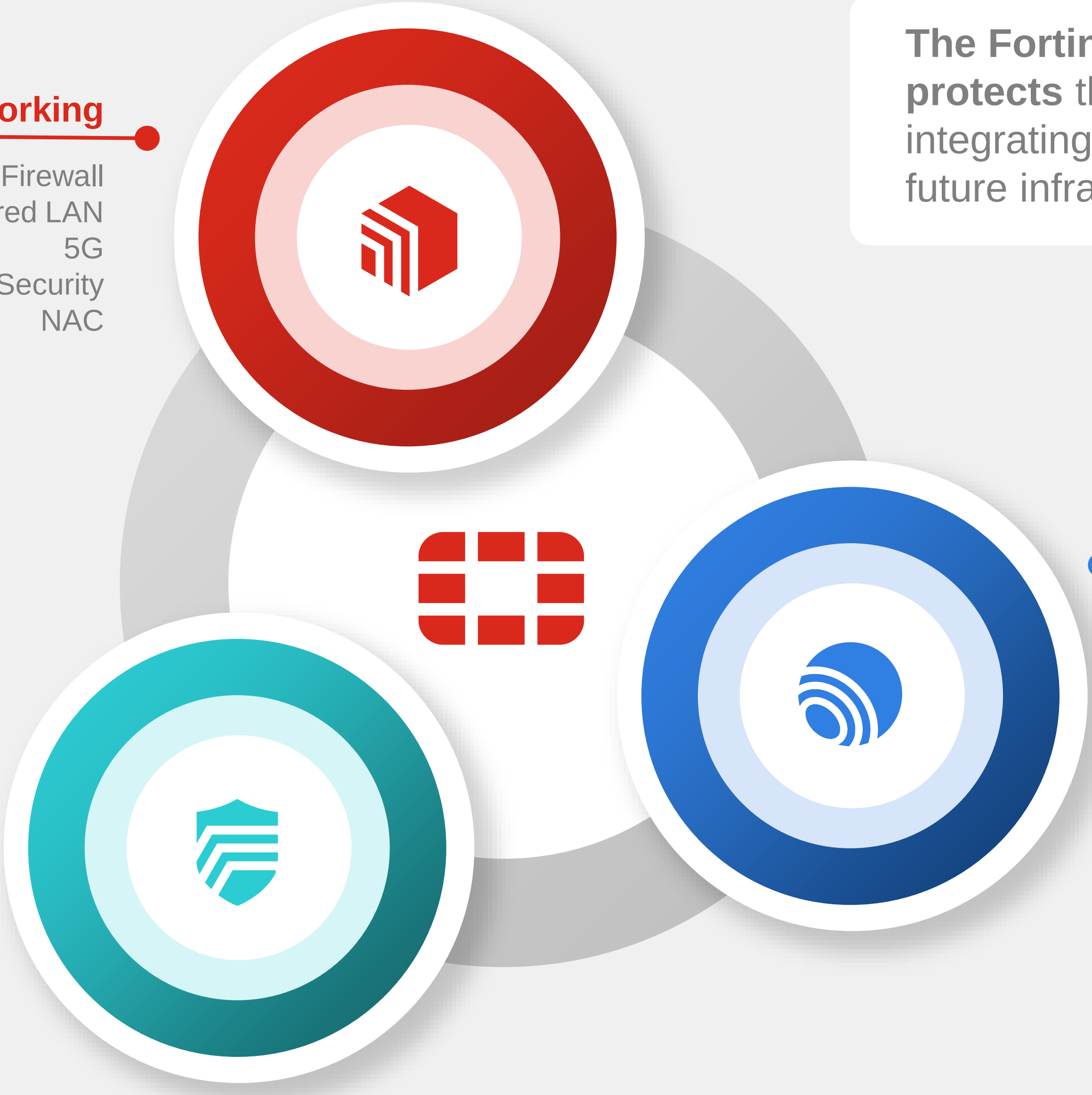
Market Capitalization
$46.1B
(as of June 30, 2024)

Security Investment Grade Rating:
BBB+ Baa1

The Broadest Platform in Cybersecurity

50+ tightly integrated product lines

The Fortinet cybersecurity platform protects the entire attack surface while integrating tightly into your current and future infrastructure



Secure Networking

Network Firewall
Wireless and Wired LAN
5G
OT Security
NAC

Unified SASE

SD-WAN
SSE
Single-Vendor SASE
ZTNA
DEM
Cloud Firewall
WAF

Security Operations

SOC Platform
Endpoint Protection
Network Detection & Response
CNAPP
Data Protection
Identity
Exposure Assessment

What is Deception?

Diverting attackers to fake assets to protect enterprise’s real assets

Decoys
Fake assets, fake network devices, fake applications and fake services

Lures
Fake services of the honeypots / decoys

Network traffic
Fake network traffic beaconing (SMB,CDP, UPnP, and more)

Breadcrumbs (tokens)
Fake resources placed on real IT assets and point to the fake systems

Prioritize alerts from the deception — High-fidelity alerts that require your immediate attention

Challenges Facing Security Teams

Detecting attackers is challenging

- On average, global dwell time is 21 days
- Unable to detect lateral movements

Security teams are stretched

- High rate of false positive alerts, < 5% are investigated

Securing legacy/unmanaged systems (OT, IoT, IoMT)

- Air-gap protection diminishes
- Assets do not provide their own telemetry (e.g., IoMT/OT/IoT)
- Unpatched/unmonitored critical devices

Break out of the darkness and quickly detect in-network threat activity across all attack surfaces

FortiDeceptor in Action…

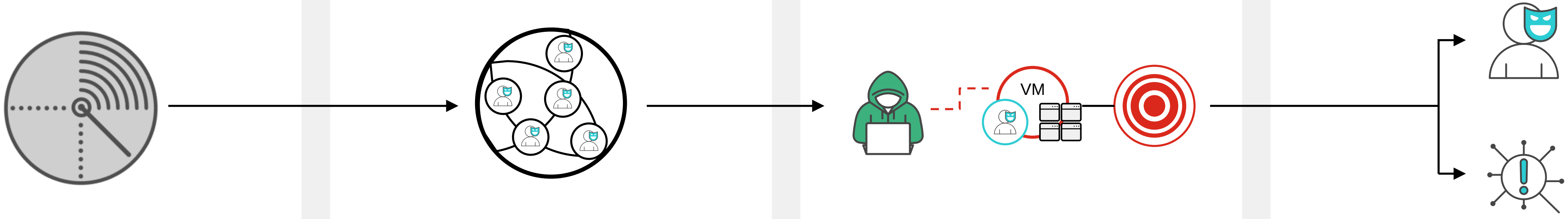
Detect early. Contain cyberattacks. Reduce risk.

1 Active/passive asset inventory discovery

2 Automated/manual decoys and tokens deployment

3 Attacker engages with a decoy

4 Attack is automatically blocked



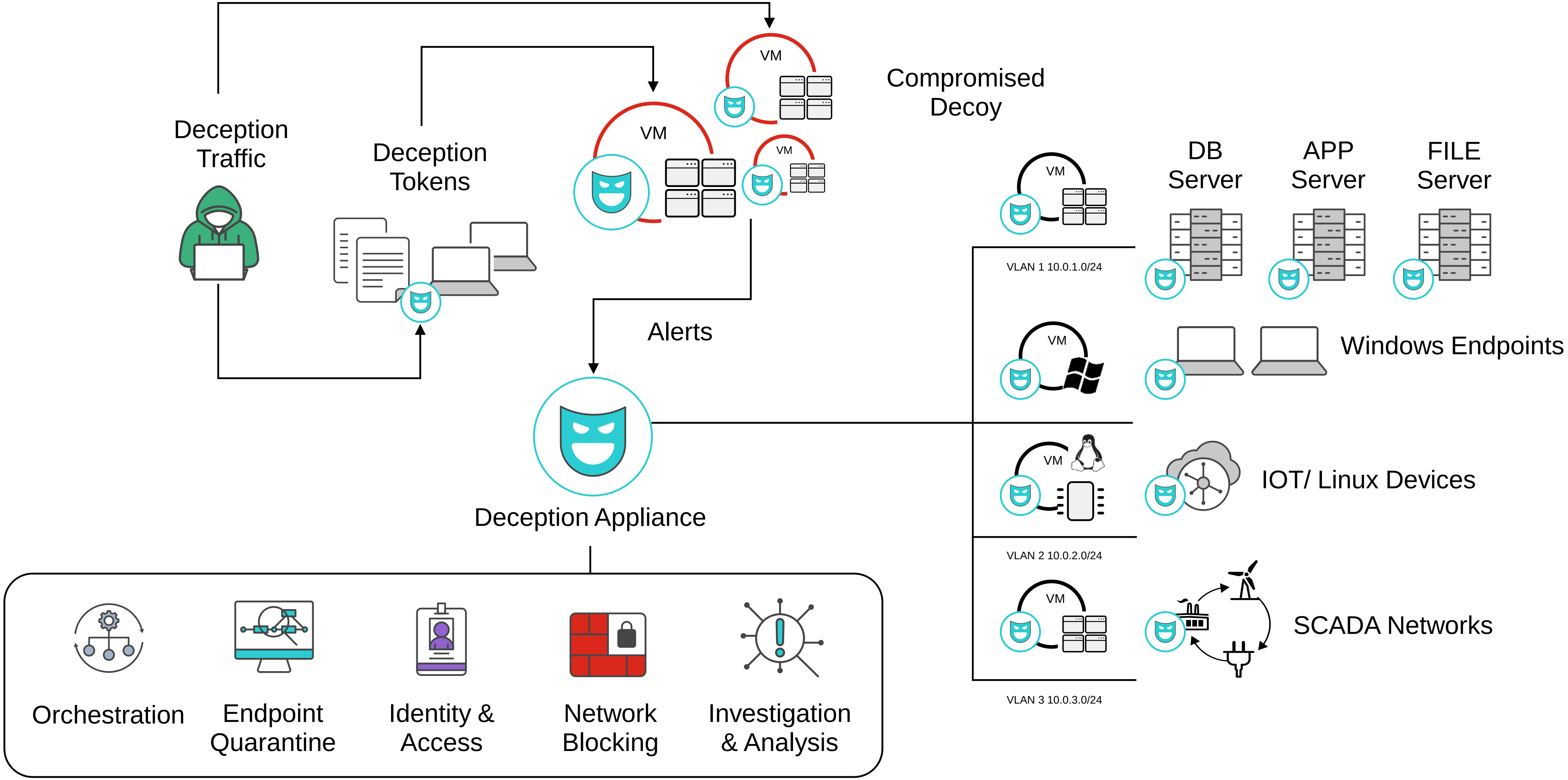
Automated Decoy Generation and Placement Optimization

Real-Time Detection and Threat intelligence

Automated Quarantine, Actionable Intelligence

Comprehensive detection, closing visibility gaps, diverts attackers from sensitive assets to shift the balance to defender’s advantage

How Deception Works



Decoys & Lures Overview

For a complete list, please see the Admin Guide

Local Windows Decoys

- Windows 7
- Windows 10

Custom Windows Decoys

- Windows 7
- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- RedHat Enterprise Linux 7.9

Windows Lure / Token

- SMB
- RDP
- SMTP
- ICMP
- FTP
- TCP Port Listener
- NBNSSpoofSpotter
- SWIFT Lite 2
- SQL (MS-Server)
- Cache Credentials
- SQL ODBC
- SAP Connector
- HoneyDocs (Office / PDF / Excel)

VPN Decoys

- FortiOS

VPN Lures

- SSLVPN
- SSL VPN DMZ

Linux Decoy

- Ubuntu 16.0.4
- Ubuntu 18.0.4,20.0.4
- CentOS
- MacOS
- RedHat 7,8,9
- Outbreak Alerts
- True-NAS

Linux Lure / Token

- SSH
- SAMBA
- TCP Port Listener
- ICMP
- Radius
- FTP
- ESXi
- ELK
- GIT
- MariaDB (MySQL)
- Tomcat (Webserver)
- SCADABR (MGMT)
- Citrix
- Webmin
- NGINX

IoT Decoys

- Cisco Router
- TP-Link Router
- IP Camera
- Printers (HP, LX, BR)
- UPS
- SWIFT VPN Gateway
- HP Switch
- MicroTik Router/NetGear MR60

VoIP Decoys

- SIP
- XMPP
- MQTT
- 4G/5G-3GPP

Application Decoys

- SAP
- ERP
- POS

Cloud Decoys

Azure
aws
Google Cloud

Medical Decoys

- PACS / Infusion Pump
- DICOM
- SPACECOM
- INFUSOMAT (Braun)

SCADA Decoys

- Schneider
  - Modicon M241
  - PowerMeter PM-5560
  - EcoStrucure BMS Server
  - SCADAPack 333E
- Siemens
  - S7-200 PLC
  - S7-300 PLC
  - S7-1500 PLC
- Rockwell
  - Rockwell PLC
  - 1769-L16ER/B LOGIX5316ER
  - 1769-L35E Ethernet Port
- Niagara
  - Niagara4 Station
  - NiagaraAX Station
- Phoenix Contact AXC 1050
- MOXA NPORT 5110
- GUARDIAN-AST
- GE PLC 90 (SRTP)
- Liebert Spruce UPS
- VAV-DD BACnet controller
- Kamstrup 382
- Ascent Compass MNG
- IPMI Device
- Modicon M580
- PowerLogic ION7650
- Emerson iPro by Dixell
- C-More HMI
- Lantronix XPORT
- EV-CPO (electric Vehicles)

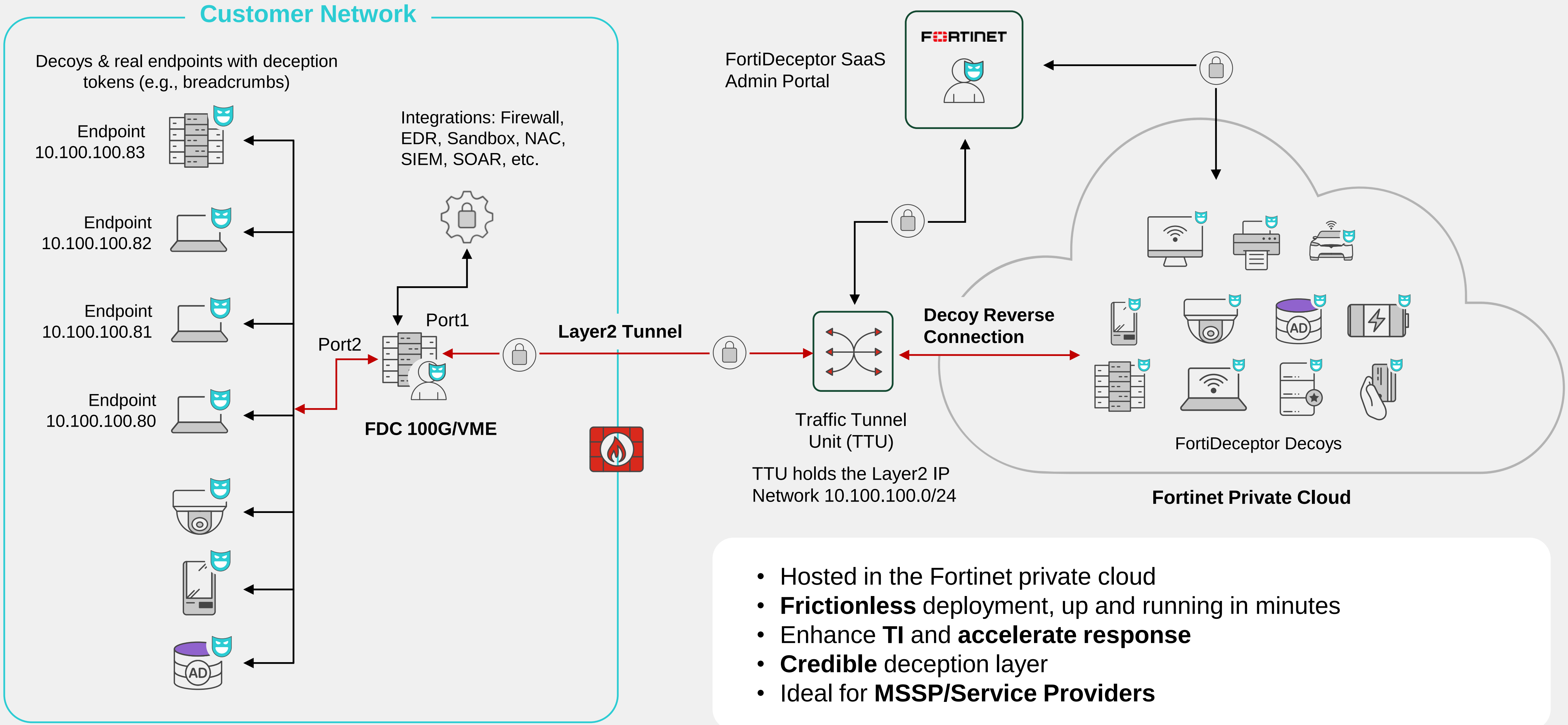
SCADA Lures

- HTTP/HTTPS
- FTP
- TFTP
- SNMP
- TELNET
- MODBUS
- S7COMM
- BACNET
- IPMI
- MOXA
- TRICONEX
- ENIP (EtherNet/IP)
- DNP3
- IEC 60870-5-104
- PROFINET
- KAMSTRUP
- Guardoan-AST

Schneider Electric
SIEMENS
Rockwell Automation
TRIDIUM
VERTIV
General Electric

FortiDeceptor-as-a-Service

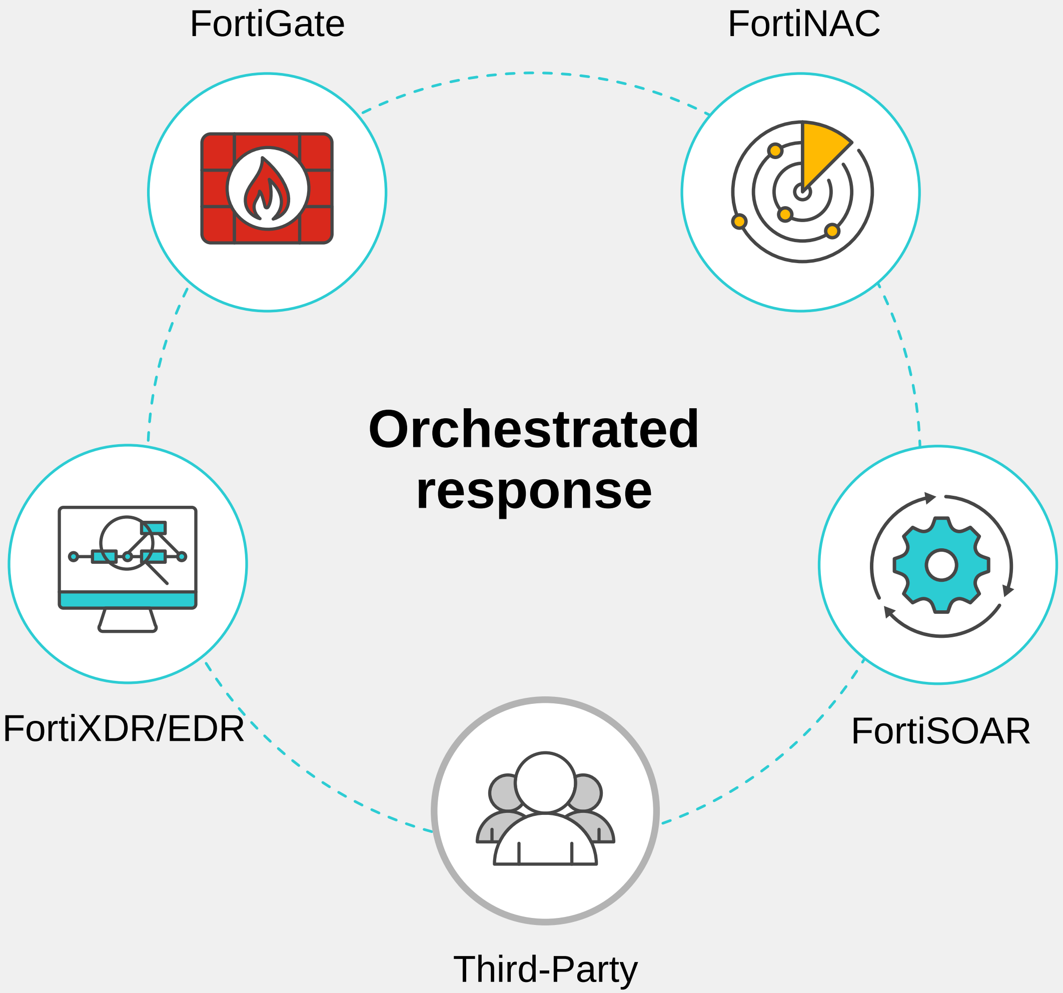
Divert attacks outside and keep your network, safe


Customer Network
Decoys & real endpoints with deception tokens (e.g., breadcrumbs)
Endpoint 10.100.100.83
Endpoint 10.100.100.82
Endpoint 10.100.100.81
Endpoint 10.100.100.80
Integrations: Firewall, EDR, Sandbox, NAC, SIEM, SOAR, etc.
Port1
Port2
FDC 100G/VME
Layer2 Tunnel
FortiDeceptor SaaS Admin Portal
FORTINET
Traffic Tunnel Unit (TTU)
TTU holds the Layer2 IP Network 10.100.100.0/24
Decoy Reverse Connection
AD
FortiDeceptor Decoys
Fortinet Private Cloud

- Hosted in the Fortinet private cloud
- **Frictionless** deployment, up and running in minutes
- Enhance **TI** and **accelerate response**
- **Credible** deception layer
- Ideal for **MSSP/Service Providers**

Fortinet Security Fabric and Third-Party Integrations

Enriched threat intelligence, automated response



FortiGate

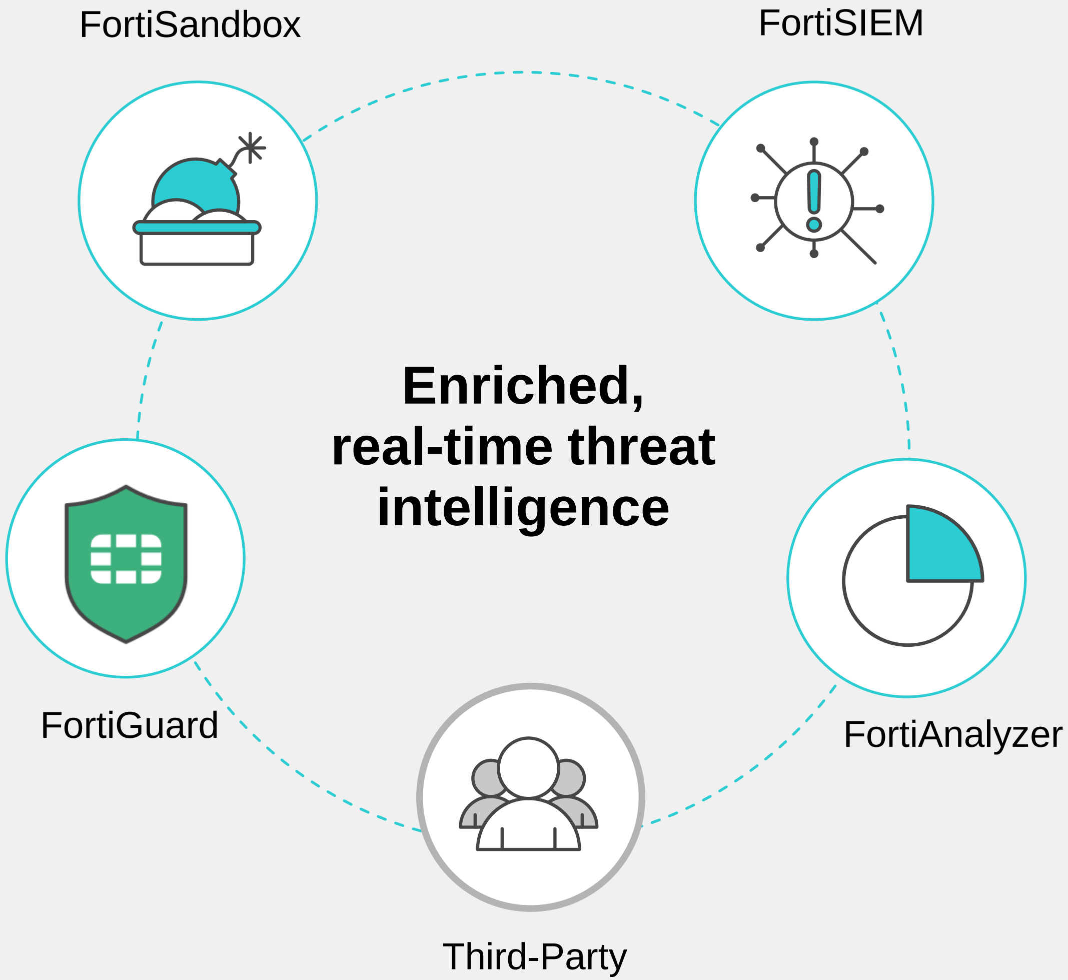
FortiNAC

Orchestrated response

FortiXDR/EDR

FortiSOAR

Third-Party



FortiSandbox

FortiSIEM

Enriched, real-time threat intelligence

FortiGuard

FortiAnalyzer

Third-Party

FORTINET®