



Fortinet Automated Security

Cybersecurity Challenges for 2023



Breaches and Data Loss

5,199

Confirmed data breach incidents in 2022

Verizon. Data Breach Investigations Report. Jun 2023.

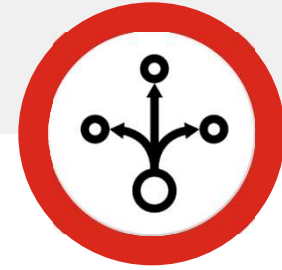


Ransomware

50%

Of organizations fell victim to a ransomware attack in 2022

Fortinet. 2023 Ransomware Survey. Apr 2023



Complexity

52%

Of organizations believe security operations are somewhat / significantly harder than 2 years ago

ESG Research. SOC Modernization. Oct 2022.



2023 Public Data Breaches

Twitter 200M users sold for \$2 each
PayPal
MailChimp – social engineering – 133 accounts compromised
T-Mobile – 37M customers, 3 months undetected
Reddit – stolen credentials
Atlassian – stolen credentials
Activision – employee credentials, 2 months undetected
US House of Representatives – 170.000 users healthcare data sold on the dark web
ChatGPT – leaked PII data cross users
Western Digital – undisclosed impact
MSI - 1.5TB of IP (source code, BIOS, private keys), \$4M ransom
KFC, Pizza HUT: employees PII – driver license, ID card
US Government: 237.000 employees data stolen
PharMerica: 5.8M customer PII
Suzuki: cyberattack with production impact of 20.000 cars
MOVEit: file sharing platform hacked. Affected customers British Airways, BBC
Reddit: 80GB confidential data, \$4.5M payout
Mondelez: 50.000 employee data stolen; 3 months undetected
UPS Canada: customer data stolen followed by phishing attack
American Airlines: 8000 pilot data stolen
PokerStars: 110.000 customers, MOVEit vulnerability
Norwegian Government: 12 ministries affected
Police Service of Northern Ireland: all policemen data stolen
Discord: 760.000 users data stolen (username, password)
Duolingo: 2.6M users data stolen
Forever21: 500.000 customer data stolen
Sony: 6000 files stolen
Air Europa Spain: credit card data stolen

**AVERAGE COST OF A DATA BREACH
WORLDWIDE**

4.35m USD

**SHARE OF ORGANIZATIONS THAT PAY
RANSOM AFTER A RANSOMWARE
ATTACK**

46%

**ALL LOSSES COVERAGE BY CYBER
INSURANCE AFTER A RANSOMWARE
ATTACK**

39%



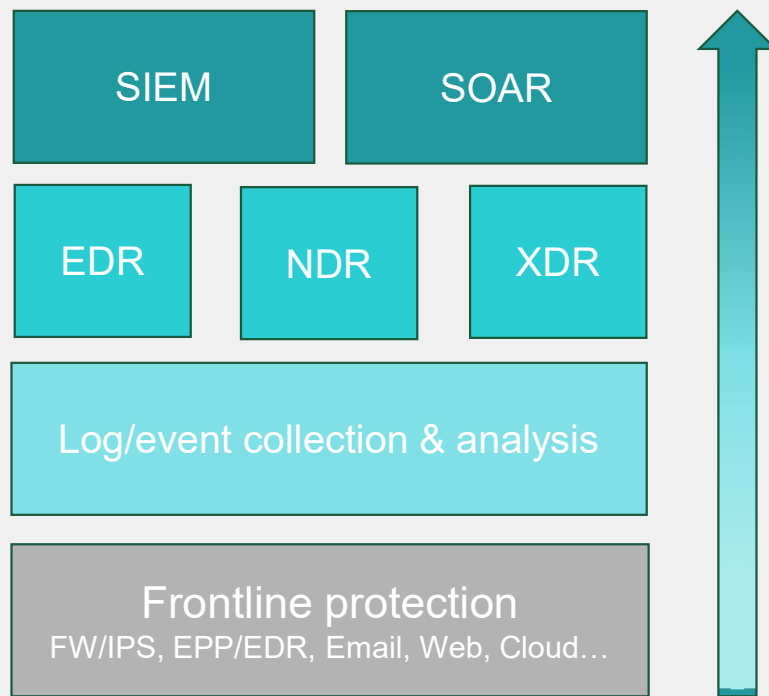


How Fortinet Can Help

Applying AI to Speed Detection and Containment



Simple View of Advanced Detection & Response



Enterprise-wide detection

Centralized & automated investigation & response

Specialized advanced detection & response

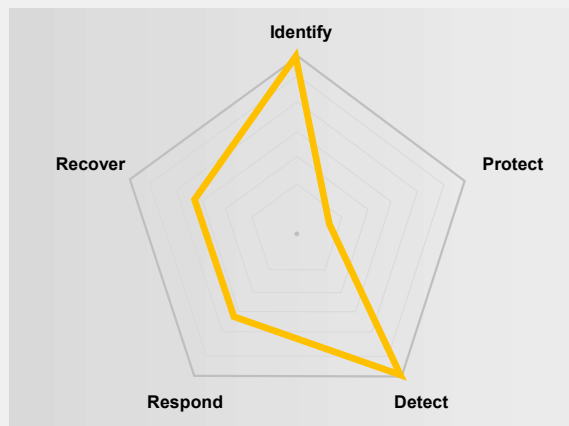
Cross-domain advanced detection & response

Correlation + analysis, detection, compliance

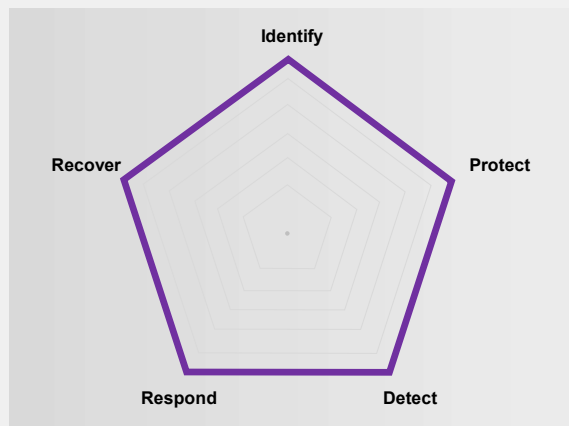
Immediate prevention at the point of attack



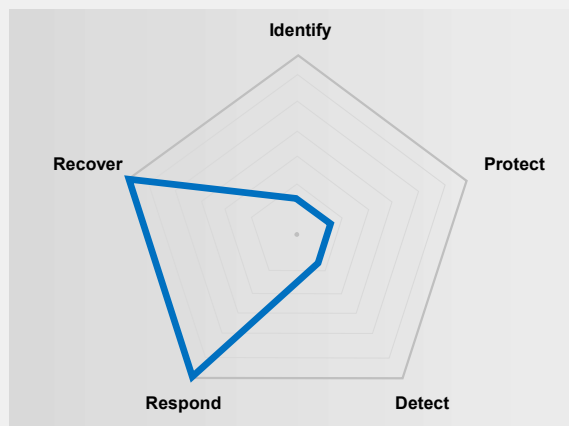
SOC Toolset Technical Focus



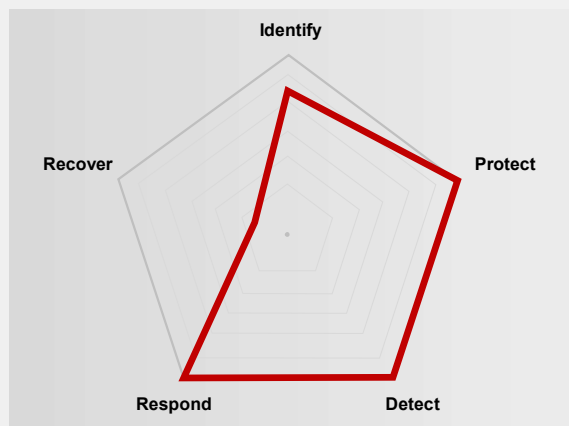
FortiSIEM



**FortiEDR
(endpoint)**



FortiSOAR

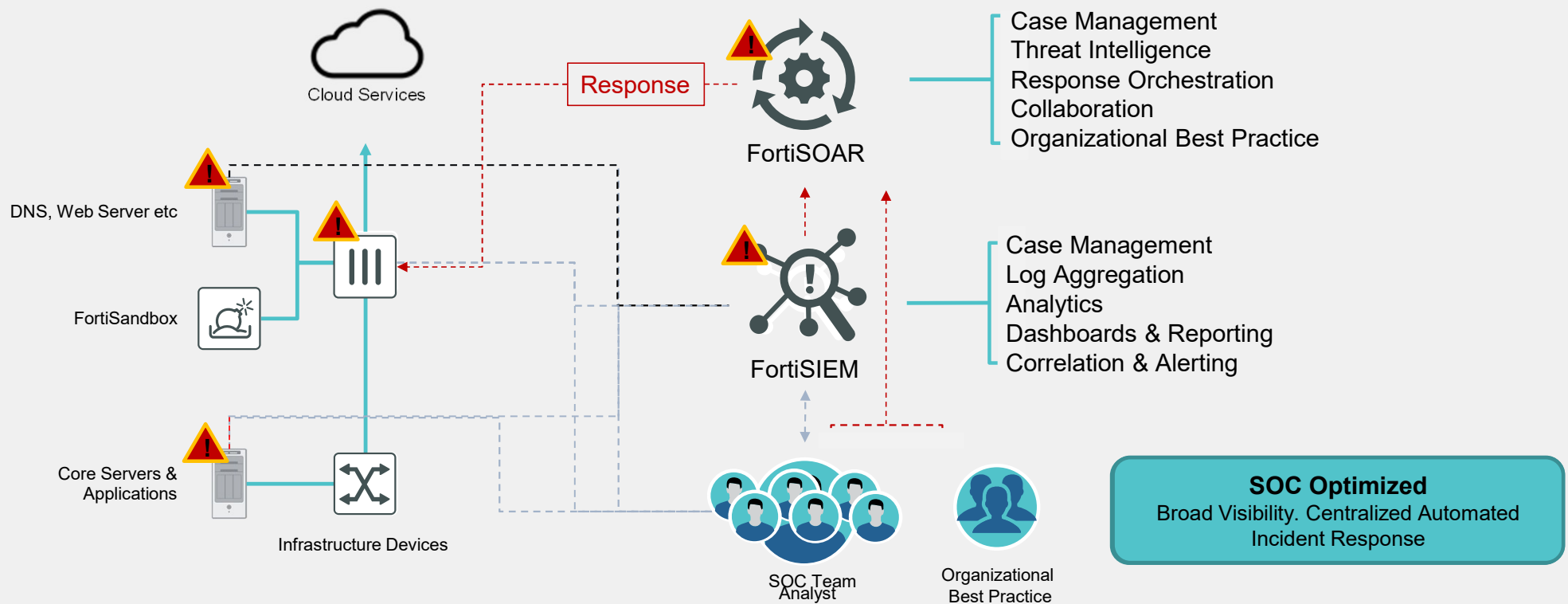


**Advanced Network Security
(E.g. Fortinet Security Fabric)**



Categories based on NIST Cybersecurity Framework
<https://www.nist.gov/cyberframework>

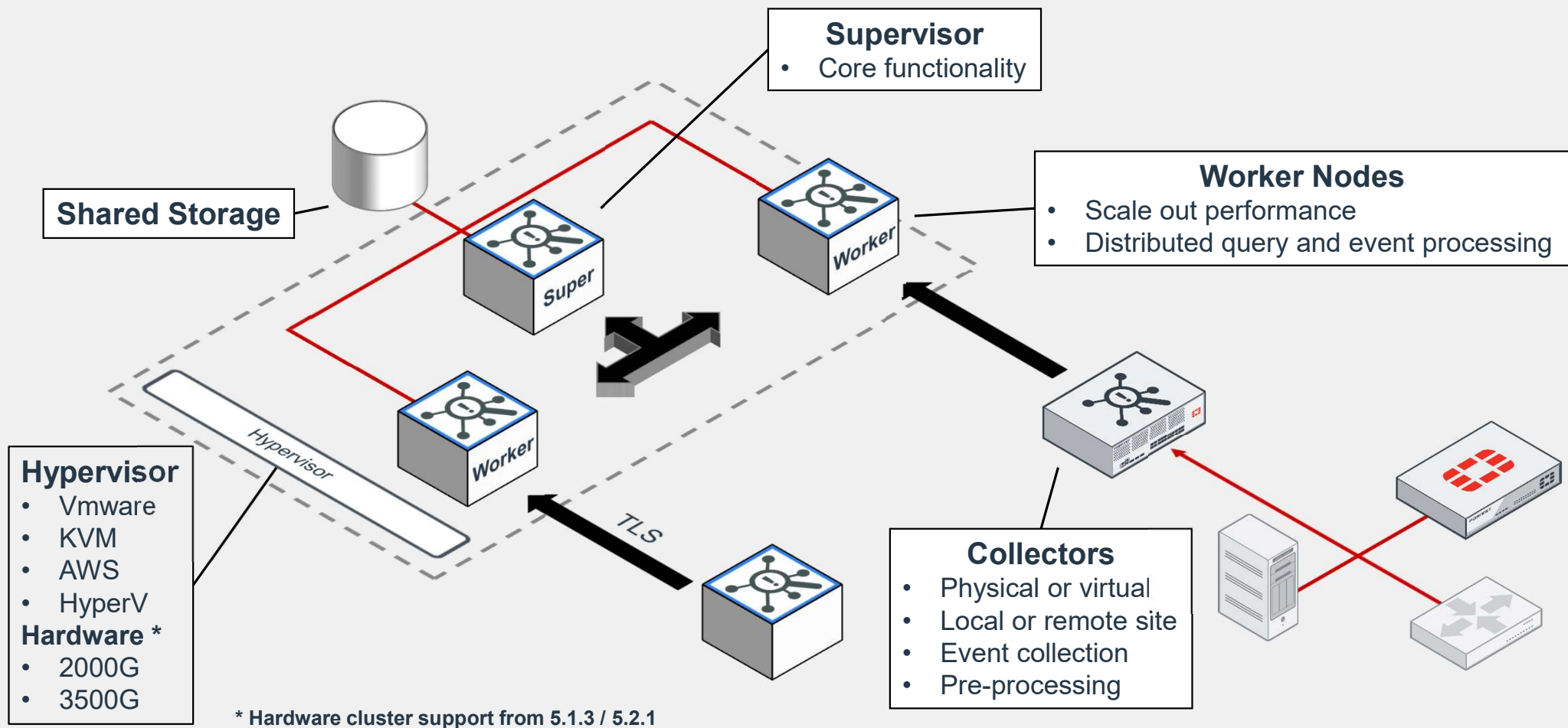
SecOps Tools – Optimizing Advanced SOC Response



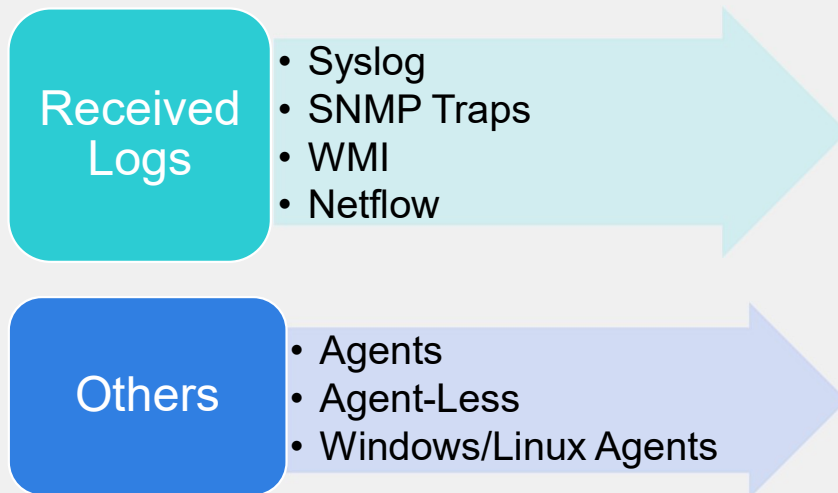
The background of the slide is a solid blue color. In the top left corner, there is a faint, light blue graphic consisting of a square with rounded corners and a line that loops around it. In the bottom left corner, there is a faint, light blue grid of small dots. On the right side of the slide, there is a large, stylized 'X' shape formed by several overlapping triangles in various shades of blue and teal. The text 'FortiSIEM' is written in a bold, white, sans-serif font, positioned in the middle-left area of the slide.

FortiSIEM

Scalable Architecture



How Does a FortiSIEM Work?



“Original Log Data”

```
May 6 17:55:48 squid[1773]: [ID 702911 local4.info] 192.168.20.39 1715
2.2.2.2 172.16.10.6 3128 674 - - - - - [06/May/2008:17:55:48 -0700] GET
"http://mail.abc.com/mail/?" HTTP/1.1 302 1061 568
"http://www.abc.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-
US; rv:1.8.1.14) Gecko/20080404 Firefox/2.0.0.14" TCP_MISS:DIRECT
```



“Normalized”

• Timestamp	= "May 6 17:55:48"
• Reporting Device	= "192.168.20.39"
• URL	= "http://mail.abc.com/mail/?"
• Severity level	= "Low"
• Browser (User Agent)	= " Mozilla/5.0 (Win..."



TestEvent_B Source_IP=10.0.52.5 Test Attack Type B Destination_IP=192.168.2.2 accessing website
www.test_b5.com downloading wwreqwer34q345qwerfasfasyw445636

<regex><![CDATA[TestEvent_B Source_IP=<srcIpAddr:gPatIpV4Dot> Test Attack Type B
Destination_IP=<destIpAddr:gPatIpV4Dot> accessing website <uriStem:gPatStr> downloading
<hashMD5:gPatStr>]]></regex>

Regex	Matches
a	The character "a"
aB	The string "aB" (but not "ab")
Fortinet	The string "Fortinet"
E-T	The string "E-T"
A z	Character "A" or character "z"
a b c	Character "a" or "b" or "c"

Regex	Matches
\s	White space character
\s+	One or more whitespace characters
\d	A single digit
\d+	One or more digits
\w	Word character (letter, number or _)
\w+	One or more word characters

```
<pattern  
name="gPatIpV4Dot"><![CDATA[\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}]]></pattern>  
<!-- Matches an IPv4 address -->
```

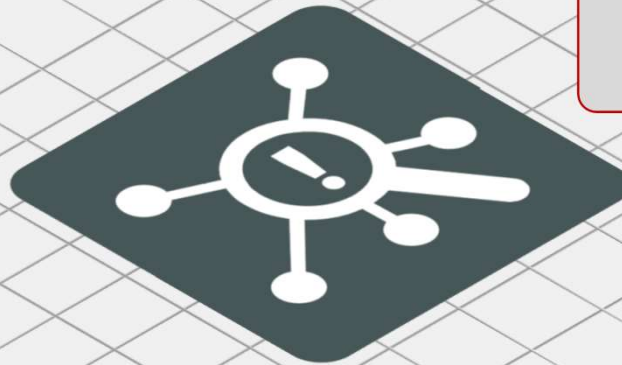


Combined SOC & NOC Analytics

Solving the SOC Visibility Puzzle

Security Events

Web Application
AAA Server
Database
Cloud Application
Firewall/ IPS/ VPN
Router/ Switch/ WLAN
Vulnerability Scanner



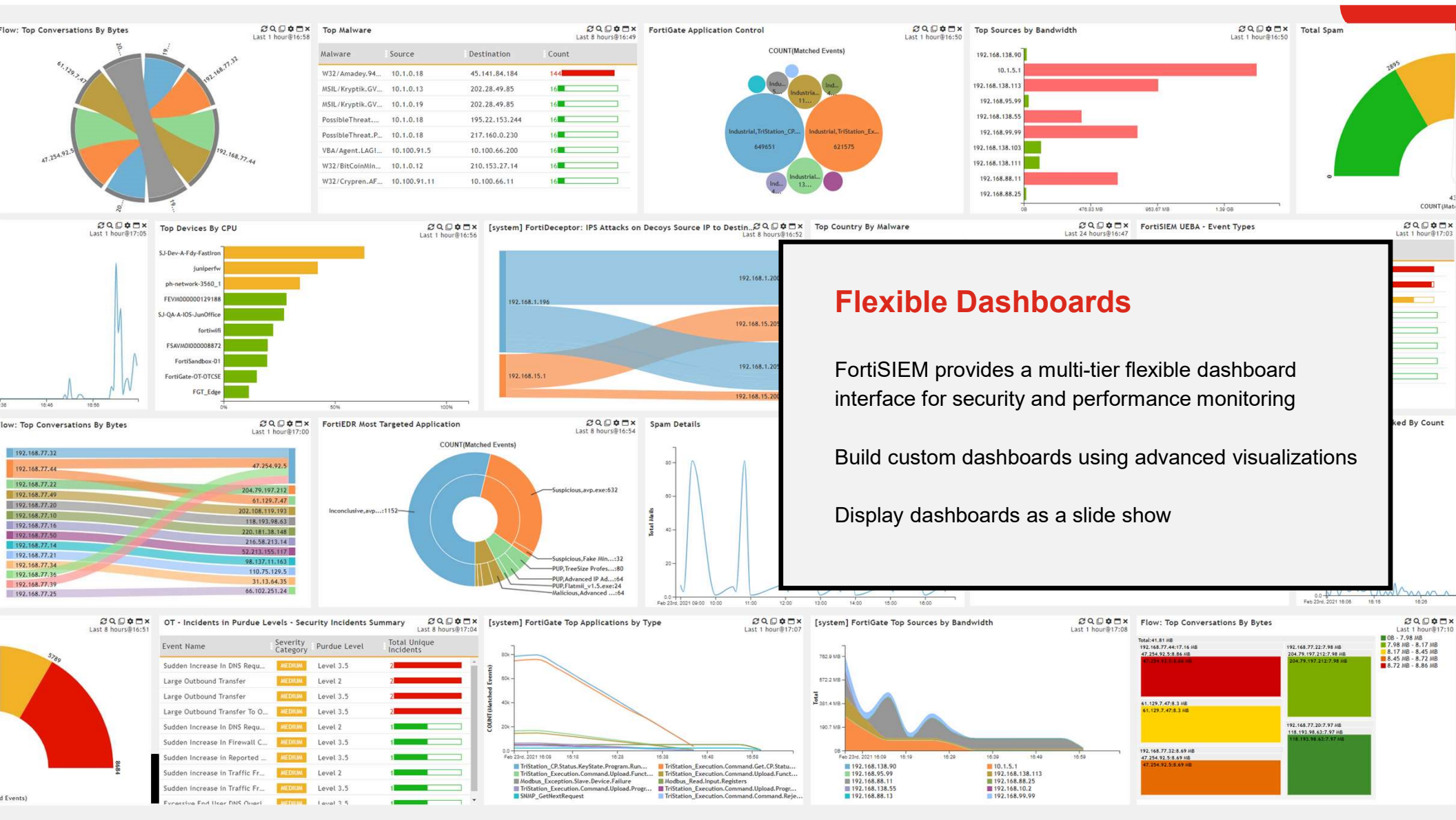
Performance Metrics

CPU
Memory
Storage
Uptime
Services
Interface Utilization

Combined SOC & NOC

Integrated CMDB | FortiGuard Threat Intelligence
Increased Functionality | Increased Visibility | Reduced Time to Respond





Flexible Dashboards

FortiSIEM provides a multi-tier flexible dashboard interface for security and performance monitoring

Build custom dashboards using advanced visualizations

Display dashboards as a slide show

CMDB Overview

The screenshot displays the FortiSIEM CMDB interface. The top navigation bar includes DASHBOARD, ANALYTICS, INCIDENTS, CASES, CMDB, RESOURCES, TASKS, and ADMIN. The CMDB section shows a summary of assets: 7 Routers, 11 Firewalls, 10 Windows, 3 Unix, 0 ESX, 0 AWS, and 0 Azure. The left sidebar lists various device categories under 'Devices', including Network Device, Server, and Virtual Infrastructure. The main content area shows a list of firewalls under 'CMDB > Devices > Network Device > Firewall'. The table lists firewalls with columns for Name, IP, Type, Status, Discovered, Method, Agent Policy, Agent Status, Monitor Status, Event Status, AWS Account, and AWS Instance. The 'FortiGate90D' firewall is highlighted. Below the table, the 'Summary' tab is selected, showing details for 'FortiGate90D'. The details include General information (Name, Device Type, Importance, Contact Info, Description), Health Overview (Availability Health: Up, Performance Health: Up, Avg CPU Util: 100%, Avg Mem Util: 41%), Incidents (last 24 hrs), and Statistics (Created, Last Discovered, Last Updated, Interfaces, Processors). Red arrows point from text boxes to specific elements in the interface.

Device Summary

Auto Asset Discovery & Auto Asset Categorization

Configuration Auditing

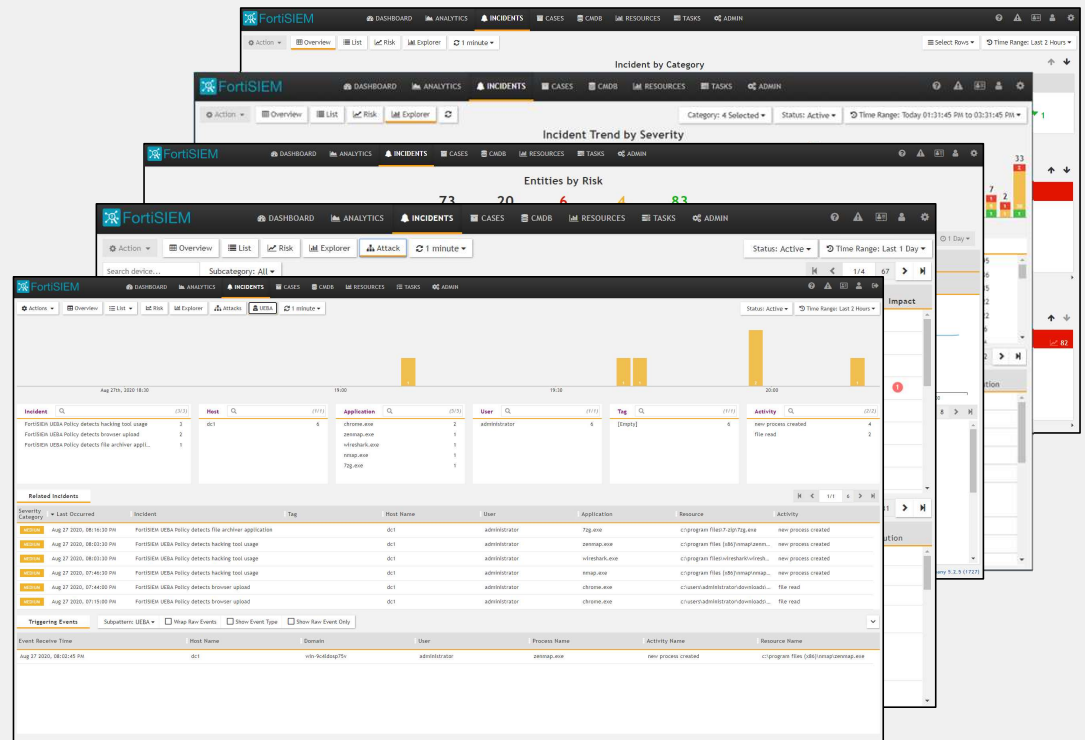
Device Detail



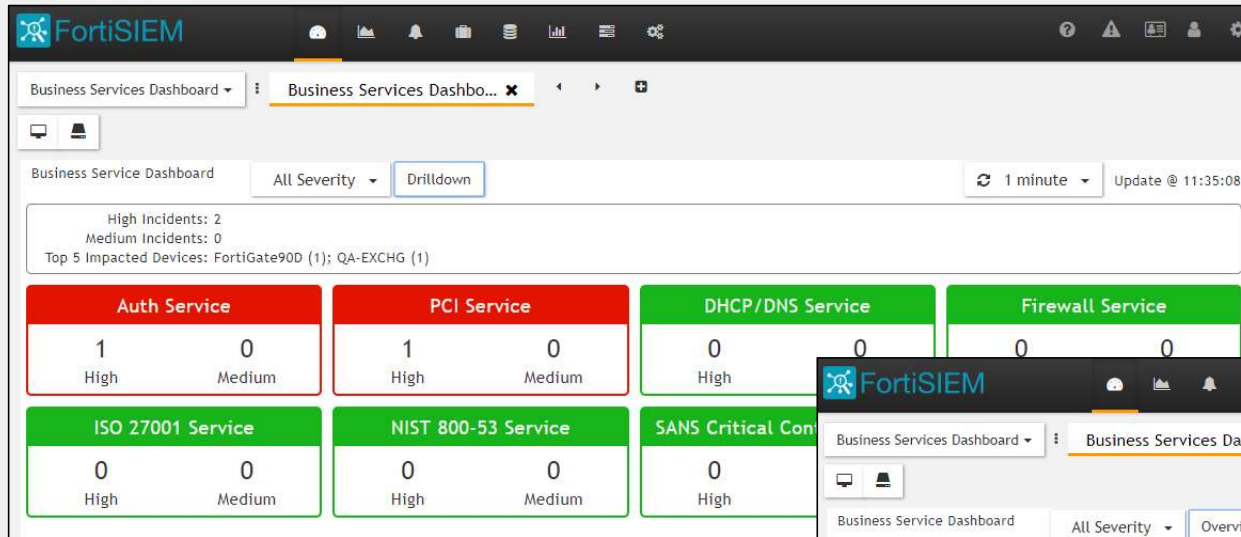
Relevant and Accessible Incident Information

Incident Dashboards Prioritize Incident Information

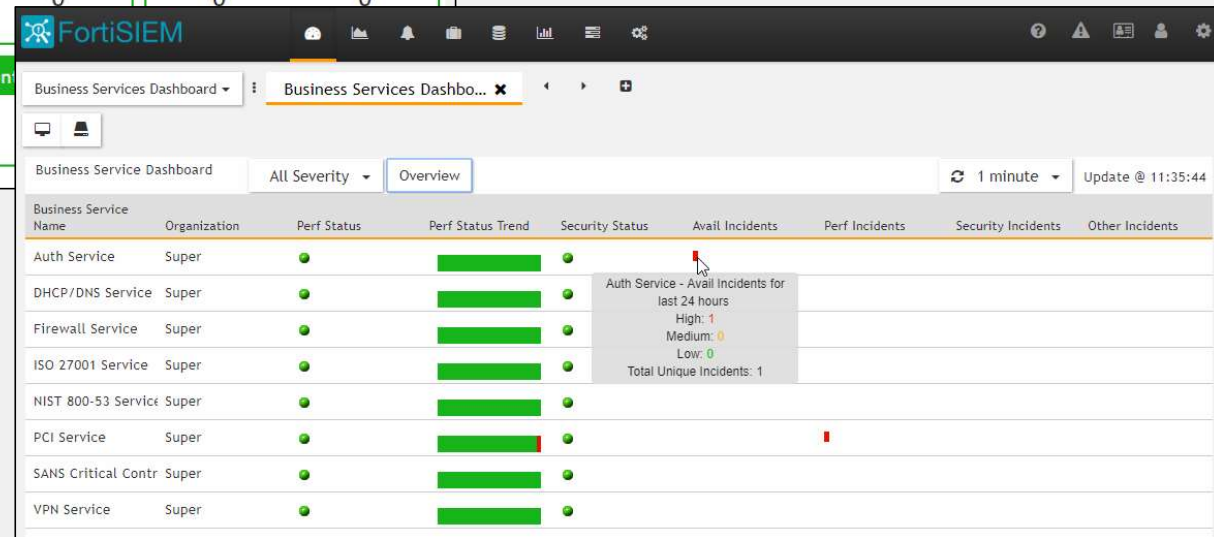
- ➔ Incident Overview Dashboard
 - Top level incident overview
- ➔ Incident Explorer Dashboard
 - Interactive incident investigations
- ➔ Risk Dashboard
 - Device and user risk & incident timeline
- ➔ Attack Dashboard
 - MITRE ATT&CK tactic alignment
- ➔ UEBA Dashboard
 - UEBA anomaly focused incidents



CMDB Business Services



- Group disparate devices
- Monitor via dedicated dashboards
- Report, alert and monitor critical services



FortiSIEM Key Features Overview



Asset Discovery

- Comprehensive & granular
- Contextual awareness
- Vulnerability awareness



Scalable, Rapid Integration

- Custom device support
- Scale out architecture



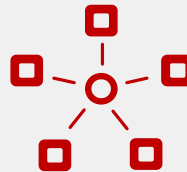
Automated Workflow

- Incident response
- Case management
- Automated remediation



Single Pane of Glass

- Comprehensive single GUI
- Unified NOC & SOC features
- PAM



Unified Platform

- Multi-tenancy
- Role based access control



FortiGuard Intelligence

- FortiGuard threat feed
- Domain, IP and URL IOCs



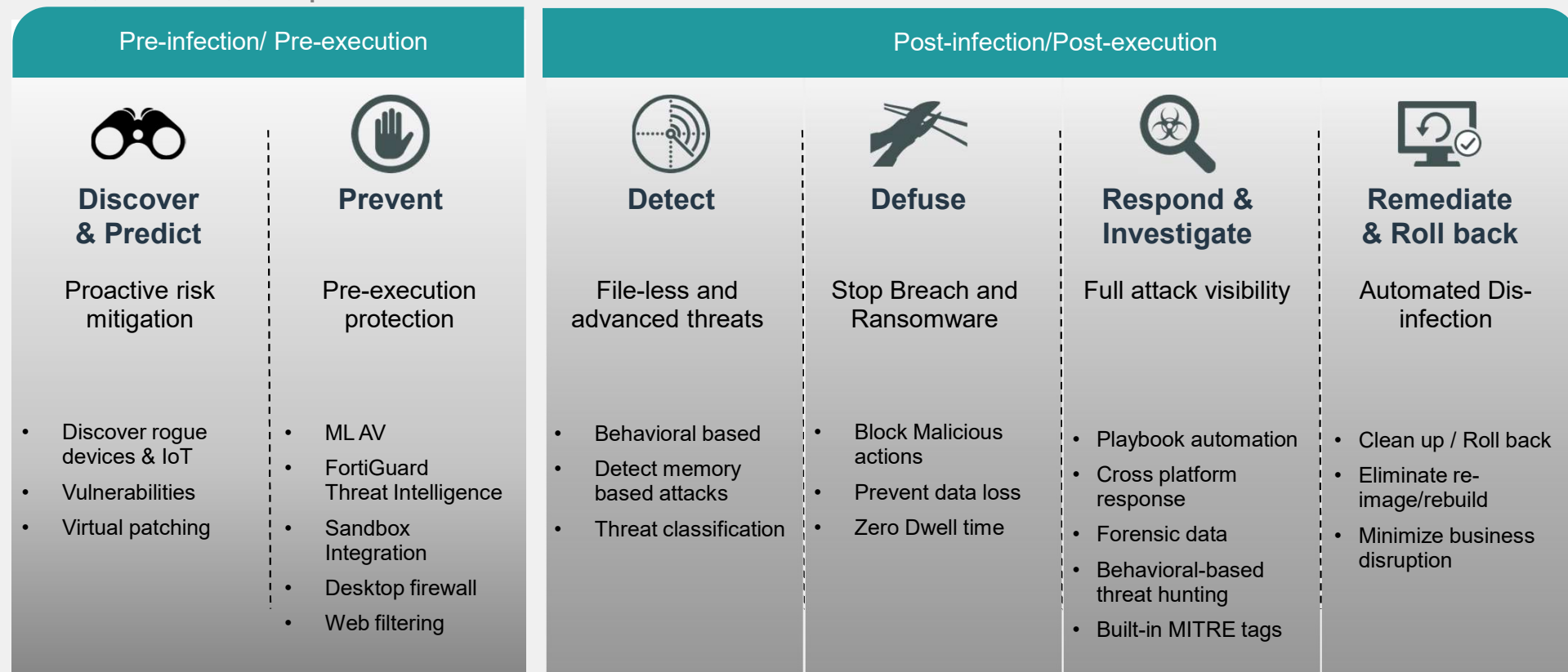
The image features a blue background with abstract geometric shapes. On the left, there are faint, light blue lines forming a square and a circle. In the bottom left corner, there is a grid of small white dots. On the right side, there are large, overlapping triangles in various shades of blue and teal, creating a dynamic, geometric pattern. The text "FortiEDR" is prominently displayed in the center-left area.

FortiEDR

FortiEDR – Cloud Native EPP + EDR



Detect, Defuse, Respond and Remote Remediation

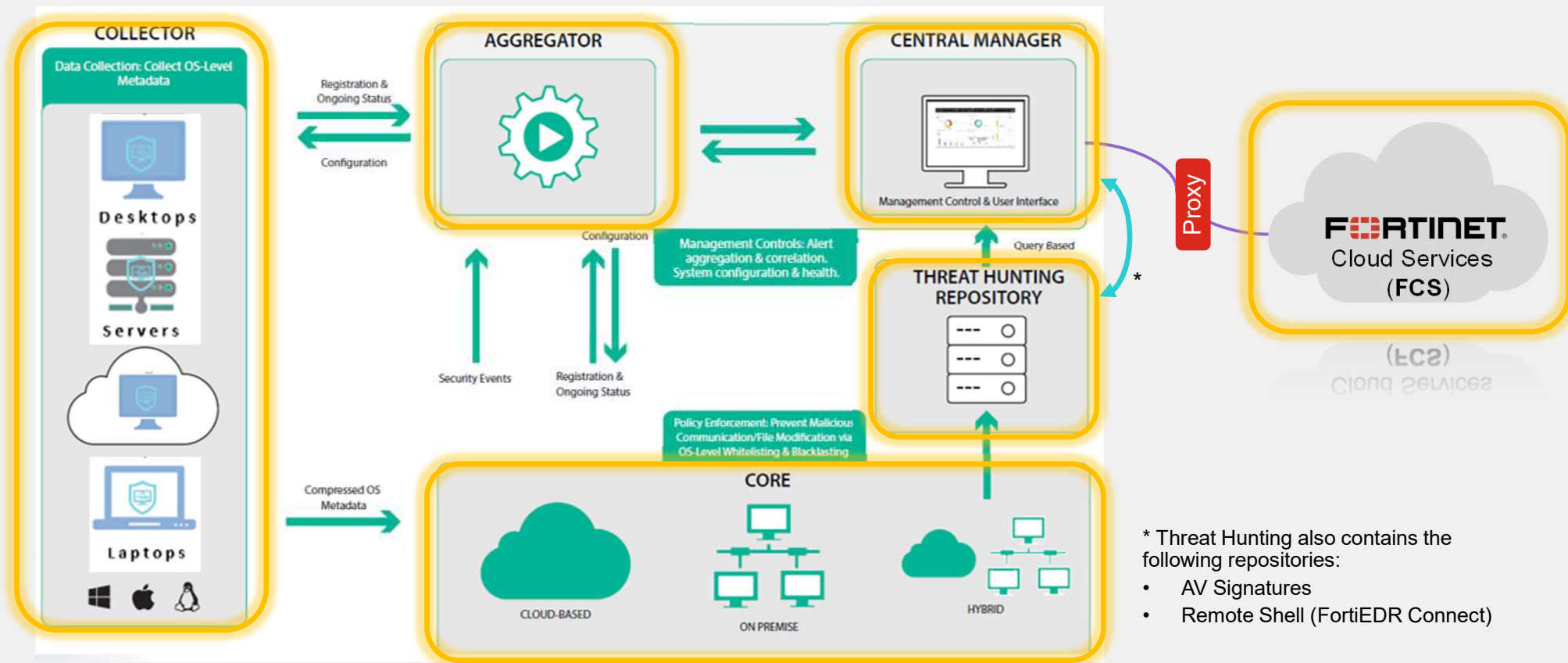


Automation | Cloud . Hybrid . Air-gap deployment | OS coverage



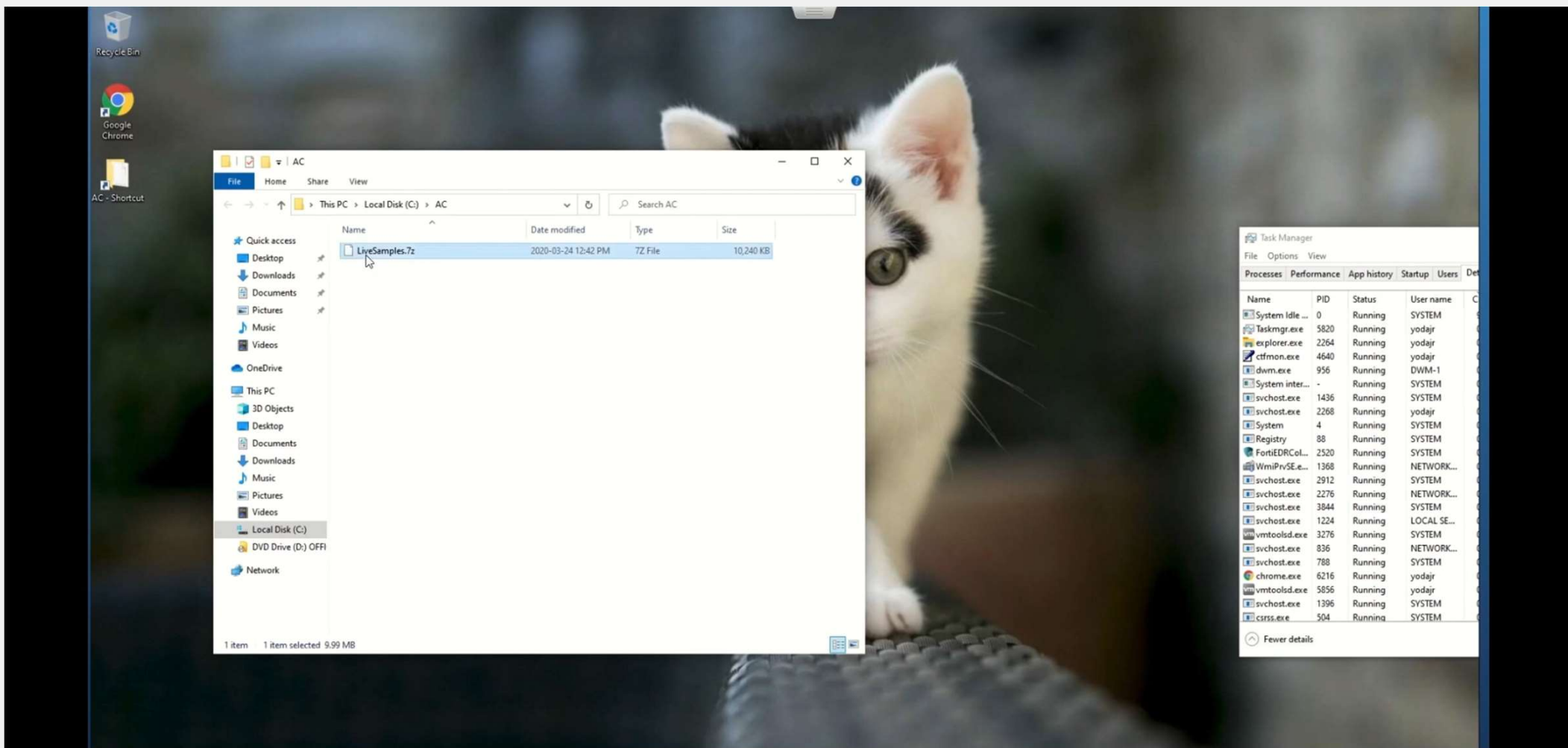
Solution Components Overview

Communication Architecture



- * Threat Hunting also contains the following repositories:
- AV Signatures
 - Remote Shell (FortiEDR Connect)





demogolp1

DASHBOARD

EVENT VIEWER 84

FORENSICS

COMMUNICATION CONTROL 198

SECURITY SETTINGS

INVENTORY 1

ADMINISTRATION 128

Protection

acaldwell

Event 96396
0-wannacry.exe

Event 96525
clickme.exe

Add Exception

Retrieve

Remediate

Isolate

Export

Raw Data Items: AllSelected1/1

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN	
ACWin10D	Windows 10 Pro	clickme.exe	Malicious	File Service Access	07-Apr-2020, 15:26:00	30-Apr-2020, 11:17:20	
RAW ID: 1933011675		Process Type: 32 bit	Certificate: Unsigned	Process Path: \Device\HarddiskVolume2\AC\ClickMe\clickme.exe		User: ACWIN10D\yodajr	Count: 3

PARENT PROCESS CREATION

PARENT PROCESS CREATION

PARENT PROCESS CREATION

PARENT PROCESS CREATION

PARENT PROCESS CREATION

PARENT PROCESS CREATION

PARENT PROCESS CREATION

PARENT PROCESS CREATION

SERVICES ACCESS ATTEMPT

SERVICES ACCESS ATTEMPT

Process ID: 3088

Source Process: \Device\HarddiskVolume2\Windows\System32\svsadmin.exe

Target: SHADOW COPY ACCESS

Company: Microsoft Corporation

Description: Command Line Interface for Microsoft® Volume Shadow Copy Service

Version: 10.0.18362.1 (WinBuild.160101.0800)

Product: Microsoft® Windows® Operating System

Comments: Command Line: delete shadows /all /quiet

Process Hash (SHA-1): 980510AE54462EB2F892C002B8828ED011D85C10

Process Owner: ACWIN10D\yodajr

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
<input type="checkbox"/> Main -\Device\HarddiskVolume2\Windows\System32\svsadmin.exe	No	Signed				980510AE54462EB2F892C002B8828ED...
<input type="checkbox"/> \Device\HarddiskVolume2\Windows\System32\KernelBase.dll	No	Signed	3	0x7ffa8bd0000	0x7ffa8e73000	696331A75FC931A4CCAE7A7337D3807...
<input type="checkbox"/> \Device\HarddiskVolume2\Windows\System32\combase.dll	No	Signed	1	0x7ffaaf0000	0x7ffaab316000	11D223F7B91E29007D8B01E15D4620...
<input type="checkbox"/> \Device\HarddiskVolume2\Windows\System32\ntdll.dll	No	Signed	1	0x7ffa8a90000	0x7ffa8a90000	B734D54E7E67DDA158CB592A44593B...
<input type="checkbox"/> \Device\HarddiskVolume2\Windows\System32\combase.dll	No	Signed	1	0x7ffaaf0000	0x7ffaab316000	11D223F7B91E29007D8B01E15D4620...
<input type="checkbox"/> \Device\HarddiskVolume2\Windows\System32\combase.dll	No	Signed	12	0x7ffaaf0000	0x7ffaab316000	11D223F7B91E29007D8B01E15D4620...



FortiEDR Fabric Integration



FortiGate

- Telemetry sharing, automatic blocking of malicious destination IP



FortiNAC

- Extended response - move endpoints to remediation VLAN



FortiSandbox

- Threat intelligence sharing



FortiSIEM

- Alerts and Logs



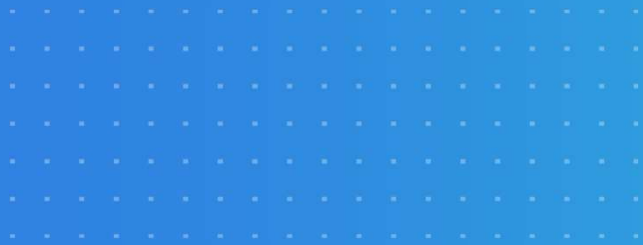
FortiSOAR

- Extended workflow automation



The logo consists of a light blue square with rounded corners. Inside the square, there is a dark blue line that forms a partial square frame on the left and bottom, and a curved line on the right side.

FortiDeceptor





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



Honeypots vs Deception

Deception — Much More Than a Honeypot

Traditional Honeypots

Deception Technology

Authenticity



Ease of deployment and operation



Scalability



Interaction



Capture Lateral Movement



Automated Threat Response



AI-driven Security Operations

DECEIVE | EXPOSE | ELIMINATE



Decoys & Lures

- Rich offering of Deception Decoys. (windows & Linux & FW & OT & IoT)
- Rich offering of Deception lures to expand the attack surface.
- Deception Decoys & lures deployment automation.



Incident Analysis & Threat intelligence

Alert analysis automation
Malware analysis automation
Generate Threat & actionable intelligence IOC's



Fabric integration

- Fortinet Fabric support for Mitigation & Remediation
- Generic REST-API wizard builder to integrate with any third part tools for Mitigation & Remediation



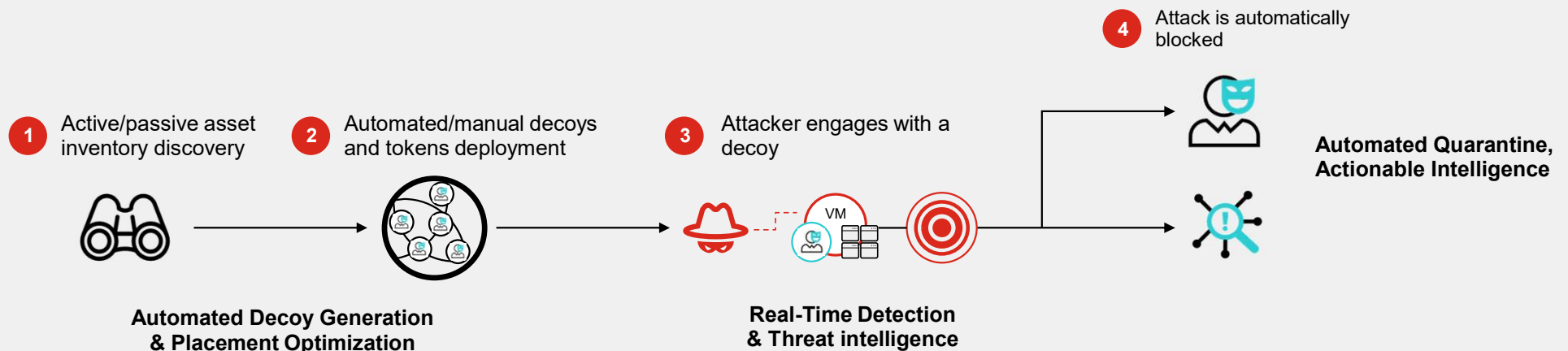
• System Features

- Enterprise management console
- Security reporting and analytics
- Support air-gap networks deployment
- SIEM support



FortiDeceptor in Action...

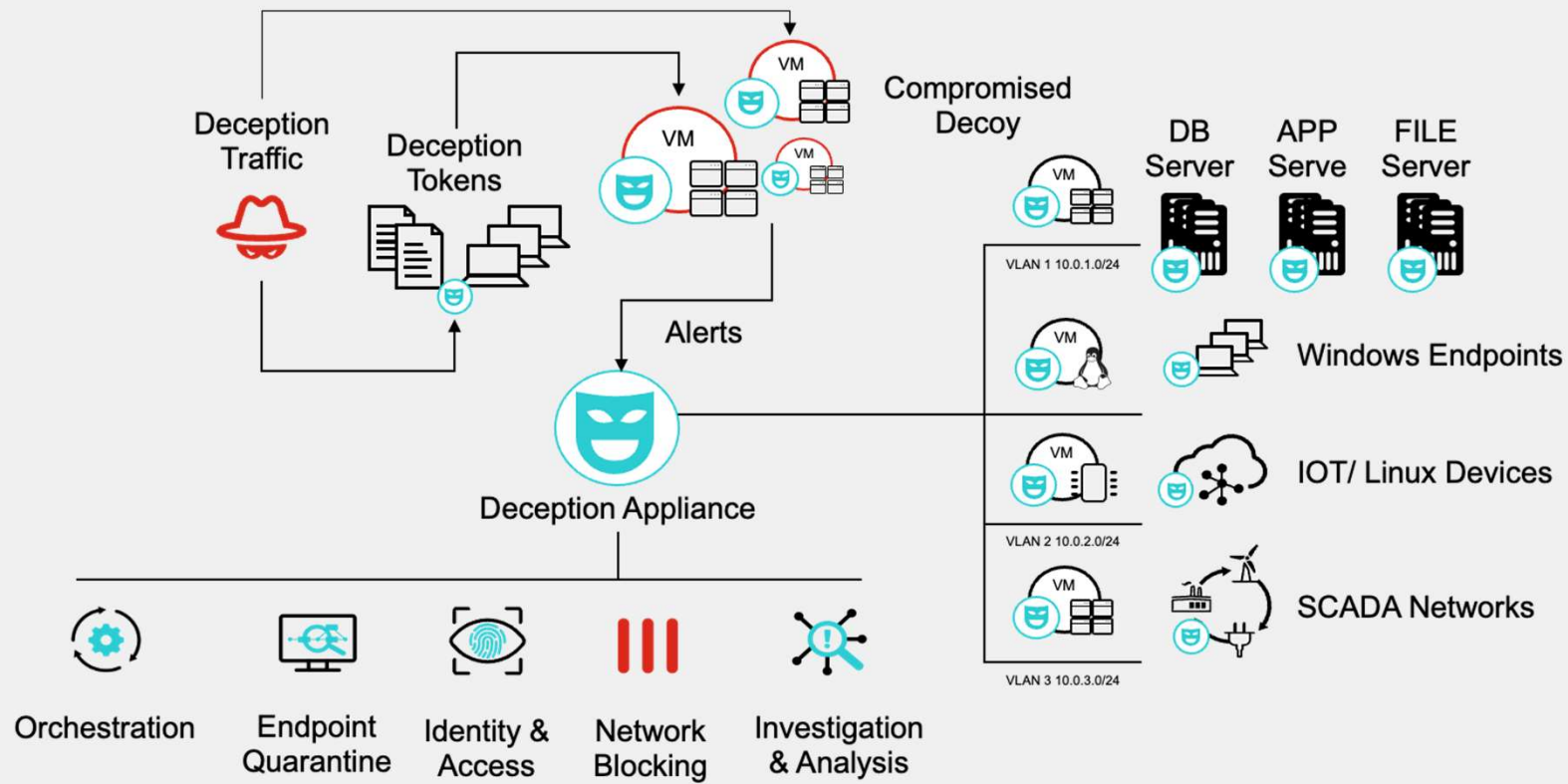
Detect early. Contain cyberattacks. Reduce risk.



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



How Deception Works



Decoys & Lures Overview

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
- CentOS
- MacOS
- Outbreak Alerts

Linux Lure / Token

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

IoT Decoys

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

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

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



FORTINET®