FORTINET®

FortiSIEM Overview

A fresh approach to Cybersecurity

3 Business Problems

ATTACKS

Internal or External- need to detect immediately

COMPLIANCE

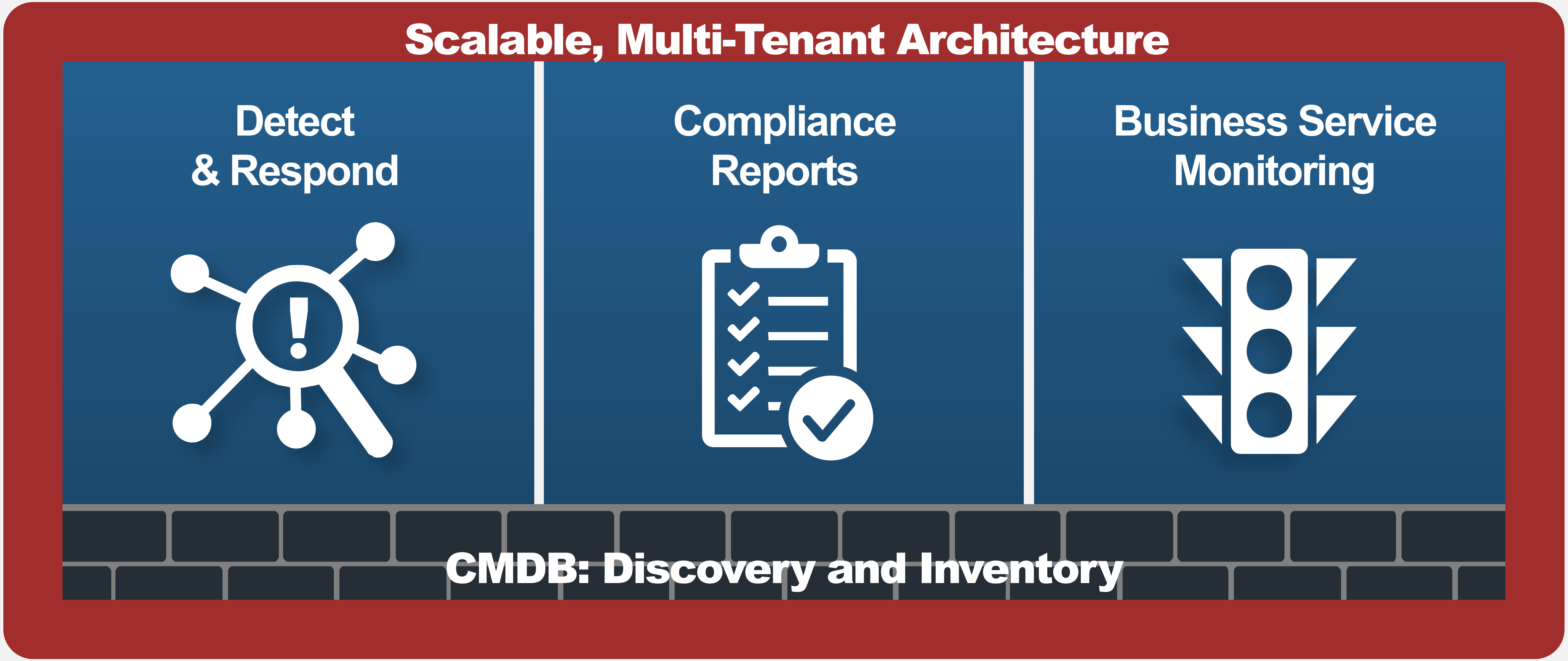
Time-consuming to generate required reports

SLAs

Critical Business Services need high availability

How FortiSIEM…

Accelerates Security Operations



Scalable, Multi-Tenant Architecture

Detect & Respond

Compliance Reports

Business Service Monitoring

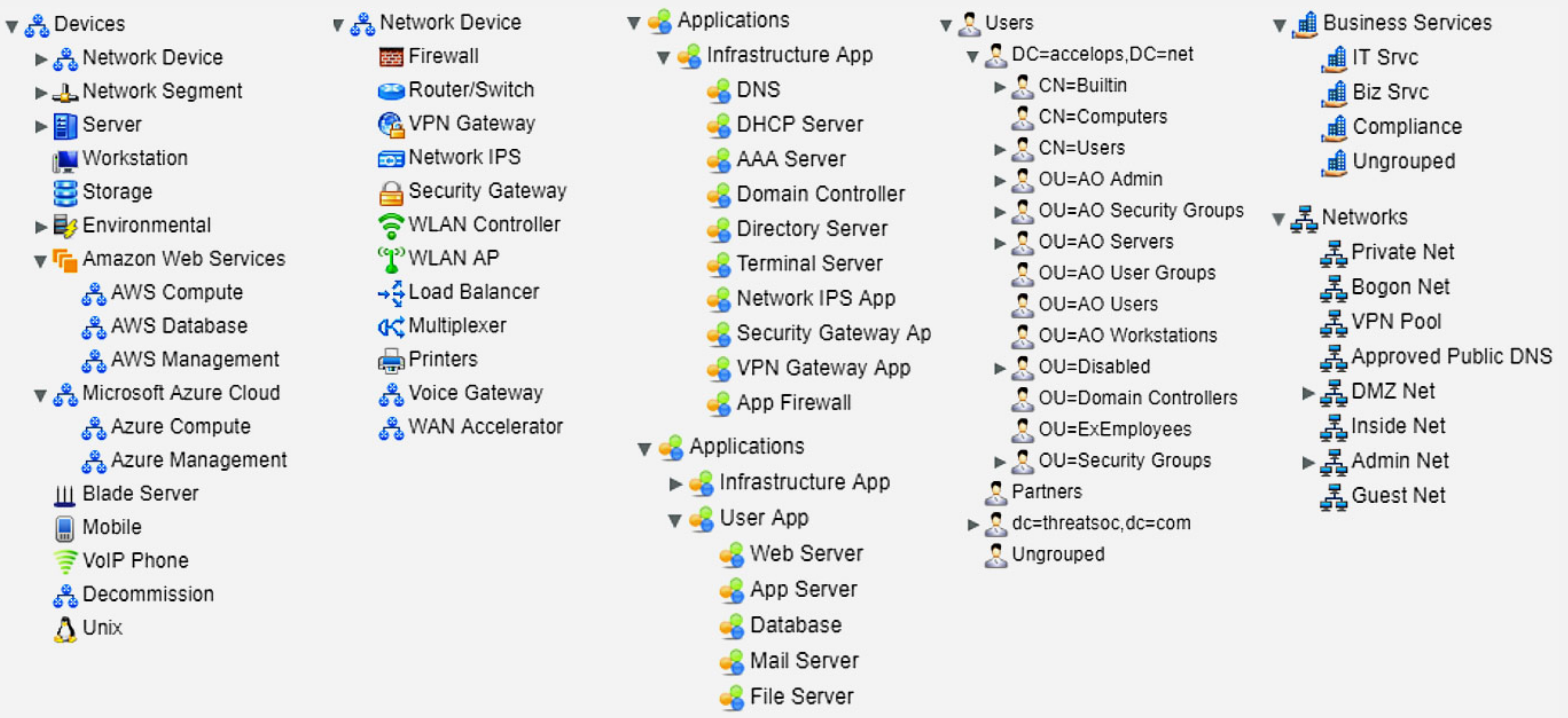
CMDB: Discovery and Inventory

CMDB: Discovery & Inventory

- Simplifies configuration of Rules, Business Services & Reports
  - » Automatic grouping based on device profile
- Real-time asset discovery & classification
  - » Network devices, applications, servers & users
  - » Discover rogue devices
- User discovery & monitoring
- Network topology discovery
- Configuration change detection
- File integrity monitoring

FortiSIEM

CMDB: Devices, Apps, Users, Biz Services & Networks



- Devices
  - Network Device
  - Network Segment
  - Server
  - Workstation
  - Storage
  - Environmental
  - Amazon Web Services
    - AWS Compute
    - AWS Database
    - AWS Management
  - Microsoft Azure Cloud
    - Azure Compute
    - Azure Management
  - Blade Server
  - Mobile
  - VoIP Phone
  - Decommission
  - Unix

- Network Device
  - Firewall
  - Router/Switch
  - VPN Gateway
  - Network IPS
  - Security Gateway
  - WLAN Controller
  - WLAN AP
  - Load Balancer
  - Multiplexer
  - Printers
  - Voice Gateway
  - WAN Accelerator

- Applications
  - Infrastructure App
    - DNS
    - DHCP Server
    - AAA Server
    - Domain Controller
    - Directory Server
    - Terminal Server
    - Network IPS App
    - Security Gateway Ap
    - VPN Gateway App
    - App Firewall

- Applications
  - Infrastructure App
  - User App
    - Web Server
    - App Server
    - Database
    - Mail Server
    - File Server

- Users
  - DC=accelops,DC=net
    - CN=Builtin
    - CN=Computers
    - CN=Users
    - OU=AO Admin
    - OU=AO Security Groups
    - OU=AO Servers
    - OU=AO User Groups
    - OU=AO Users
    - OU=AO Workstations
    - OU=Disabled
    - OU=Domain Controllers
    - OU=ExEmployees
    - OU=Security Groups
  - Partners
  - dc=threatsoc,dc=com
  - Ungrouped

- Business Services
  - IT Srvc
  - Biz Srvc
  - Compliance
  - Ungrouped

- Networks
  - Private Net
  - Bogon Net
  - VPN Pool
  - Approved Public DNS
  - DMZ Net
  - Inside Net
  - Admin Net
  - Guest Net

Detect & Remediate

- Real-time analytics (patented)
  - Ingest over 500K EPS sustained
- UEBA: Baselining & Machine Learning
- Remediation Library/SOC Playbook
- Device context from CMDB
- External threat feeds
- Dynamically add support for new log formats and devices (Parsers)

Compliance Reporting

- 100s of Compliance Reports
  - PCI – HIPAA – FERPA - FISMA
  - SOX, NERC, COBIT, ITIL,
  - ISO, GLBA, GPG13
  - NIST, SANS Critical Controls
- Uses CMDB for:
  - Device configuration change detection
  - User monitoring
  - File integrity monitoring

Monitor Business Services

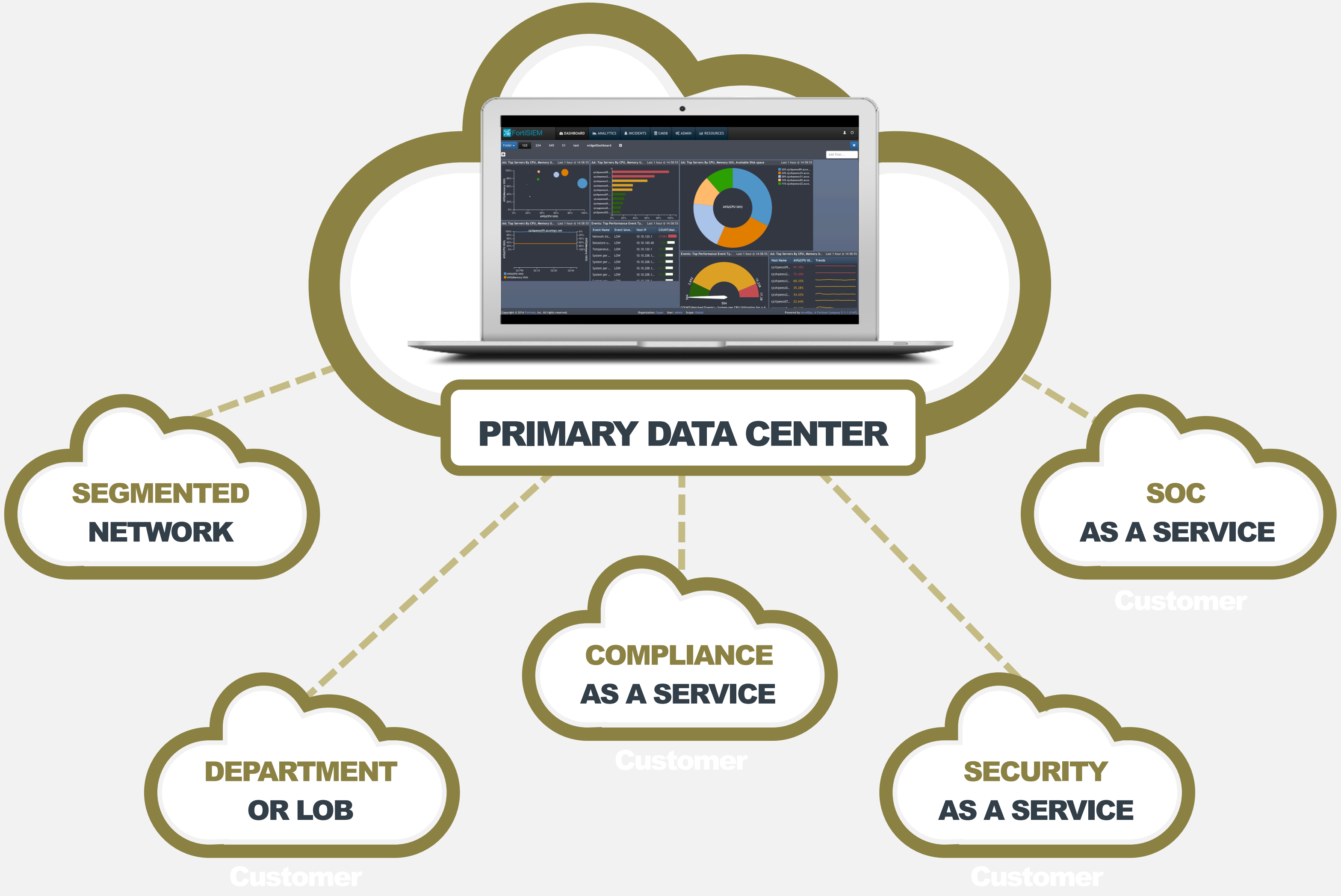
- Group CMDB discovered devices and applications into a “Business Service”
- Dashboard displays overall status of the Business Service
  - » Drill down to see which devices/software services are impacting the Business Service
- Quickly see which Business Services would be impacted if a device or application fails or is taken out of service
- Flexible Health Monitoring:
  - » Devices: SNMP & APIs
  - » Applications: Synthetic Transactions
- Multiple alert options

FortiSIEM

Multi-Tenant Architecture for Enterprises & MSSPs

Key Features

- Role Based Access Control
- Robust visibility enforcement
- Flexible deployment options



FortiGuard TIS Architecture

Organizations

- Technology
- Education
- Finance
- Manufacturing
- Government
- Healthcare

320K+ total

Devices

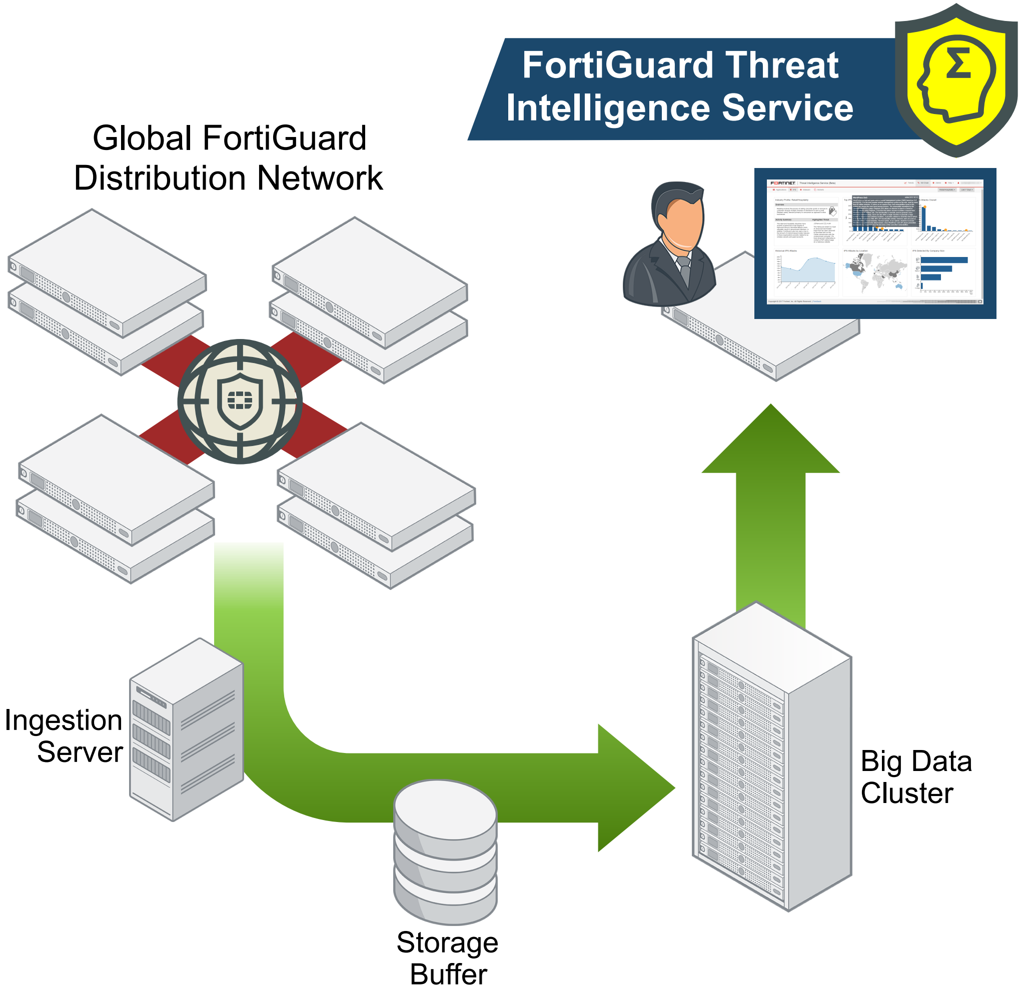
- Firewalls
- Sensors
- Access Points
- Switches
- Desktops & Laptops
- Mobile & Tablets

2.5M total

Threats

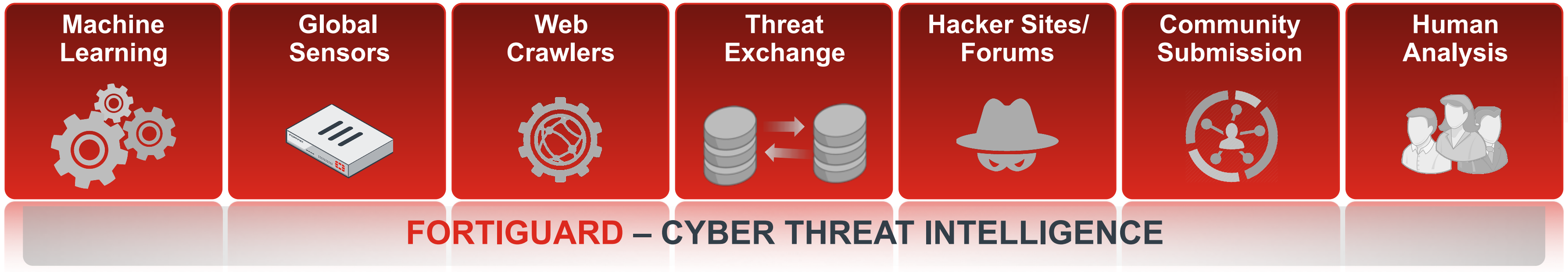
- Botnets
- Applications
- Vulnerabilities
- Malware
- Malicious URLs
- Malicious Emails

50B per day

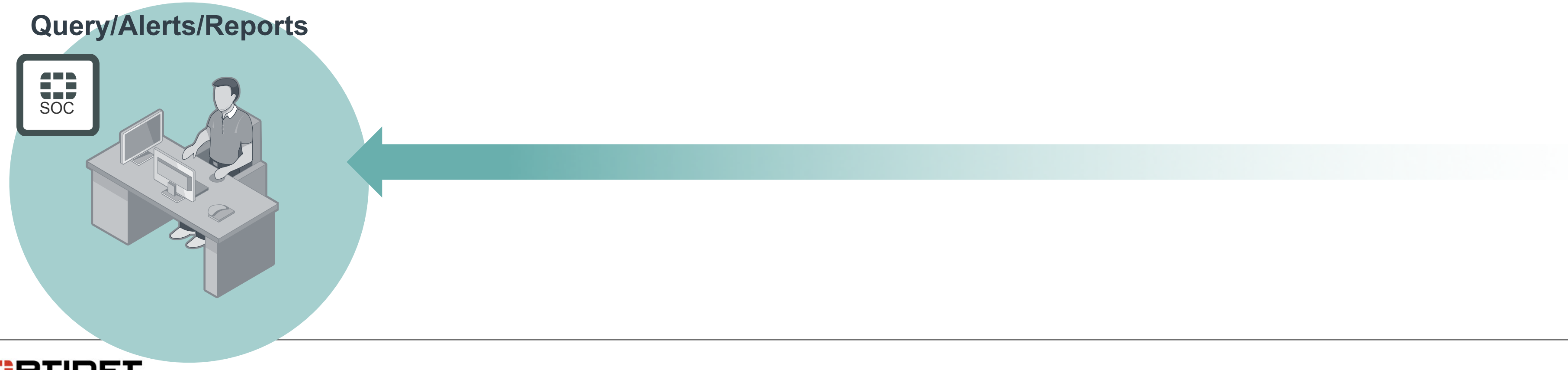


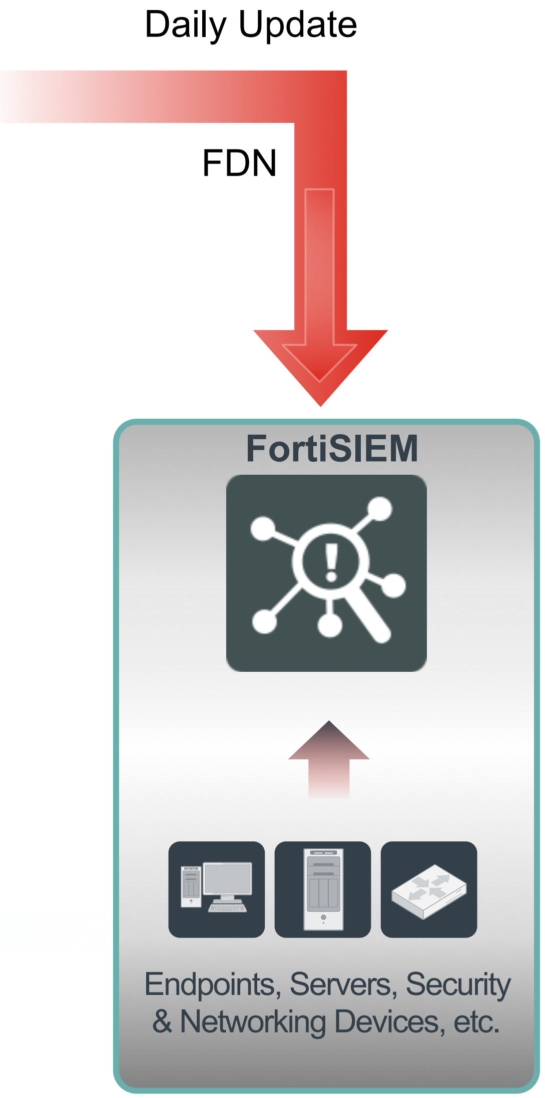
FortiGuard Threat Intelligence Service
Global FortiGuard Distribution Network
Ingestion Server
Storage Buffer
Big Data Cluster

FortiSIEM Indicators of Compromise (IOC)

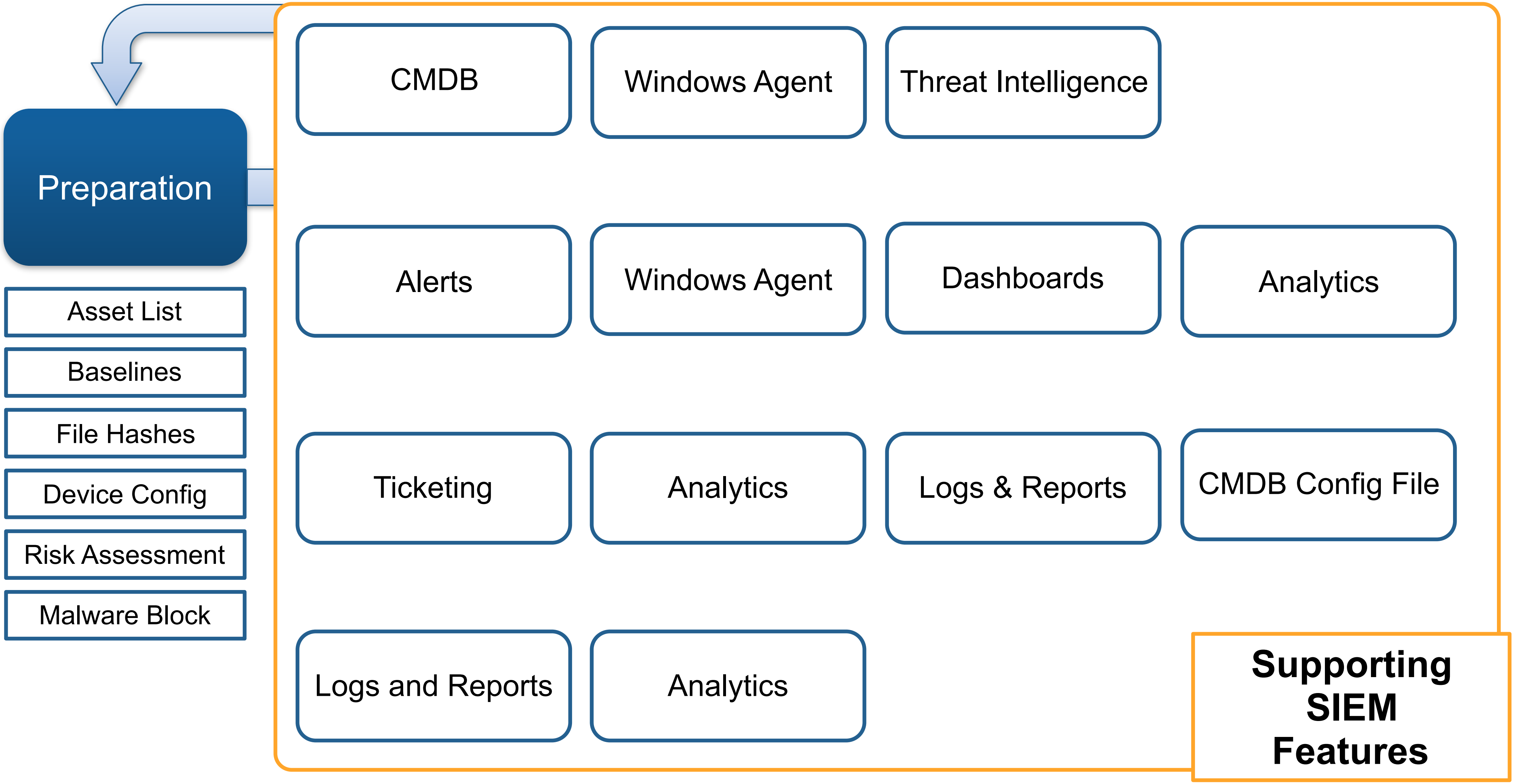


- **NUMBER OF INDICATORS** - > 1 Million Entries
- **TYPES OF INDICATORS** - Domains, IP Addresses and URLs. Post infection list – Know Malicious
- **THREAT NAME/TYPE** - C2 Botnet, SpywareC2, Sinkhole
- **REAL TIME** – Real time correlations as well as historical reporting



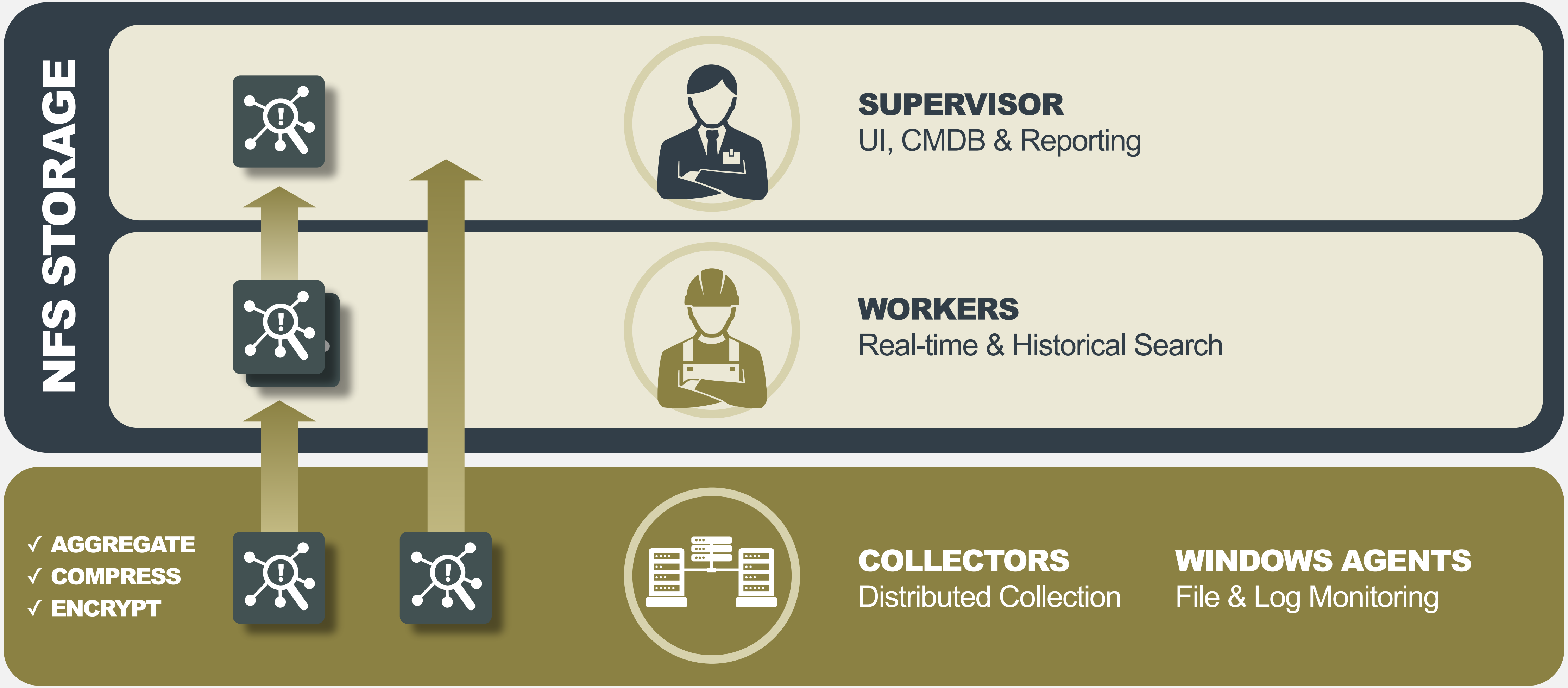


FortiSIEM and Security Incident Response



FortiSIEM

Scalable Architecture



SUPERVISOR
UI, CMDB & Reporting

WORKERS
Real-time & Historical Search

- √ AGGREGATE
- √ COMPRESS
- √ ENCRYPT

COLLECTORS
Distributed Collection

WINDOWS AGENTS
File & Log Monitoring

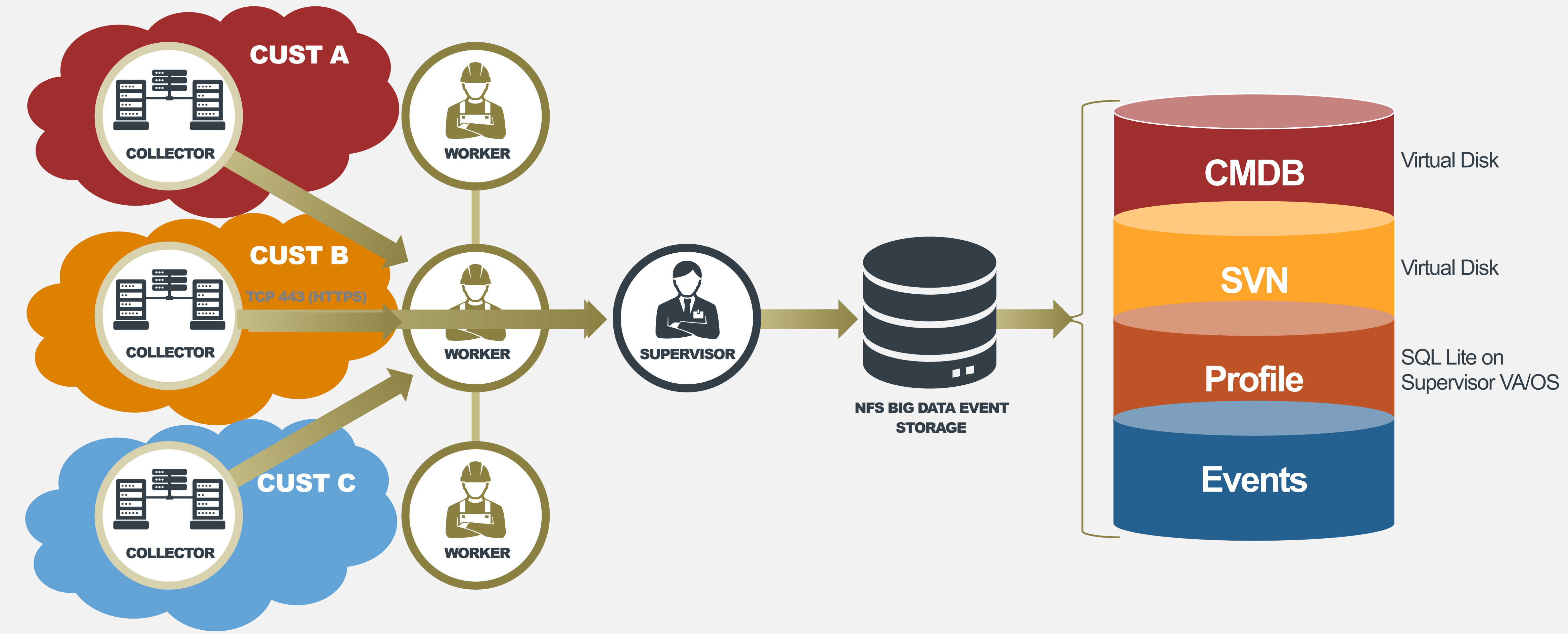
MSSP

- 3 Methods of customer data separation
  - Collector
  - IP
  - Multitenant Collector

- 2 Levels Architecture
  - Global – see all customers, data, incidents
  - Local Level

FortiSIEM

Rapid Scale Architecture



Licensing

- Key areas to determine license size
  - **Number and type (Device or Endpoints) of devices being monitoring**
  - Total number of EPS
  - Windows Agents (SIEM)

FortiSIEM licensing

- Devices
  - SKUs come with 1 Device + 10 EPS
  - Device: Sends logs and/or is monitored
  - Example: Firewall
- End Points
  - SKUs come with 1 End Point + 2 EPS
  - End Point: Sends logs and/or is monitored
  - Example: Workstation, Low EPS Switch or other device
- Advanced Windows Agents
  - Installed Software Detection
  - Registry Change Monitoring
  - File Integrity Monitoring

FORTINET®