VERVE
INDUSTRIAL PROTECTION

IT-OT End-Point Protection, Detection & Response

VERVE
INDUSTRIAL PROTECTION

Background on Verve Industrial Protection

- 25 Years' experience in industrial control systems design, management & security
- Operating across all control system vendors
- Power, O&G, Pharma, Paper, discrete manufacturing, etc.
- Turnkey IT-OT Service Management & Cybersecurity Offering:
  - Solution Design
  - Open-platform software to identify, protect, detect, respond and recover
  - Scalable and effective world-class managed services and support

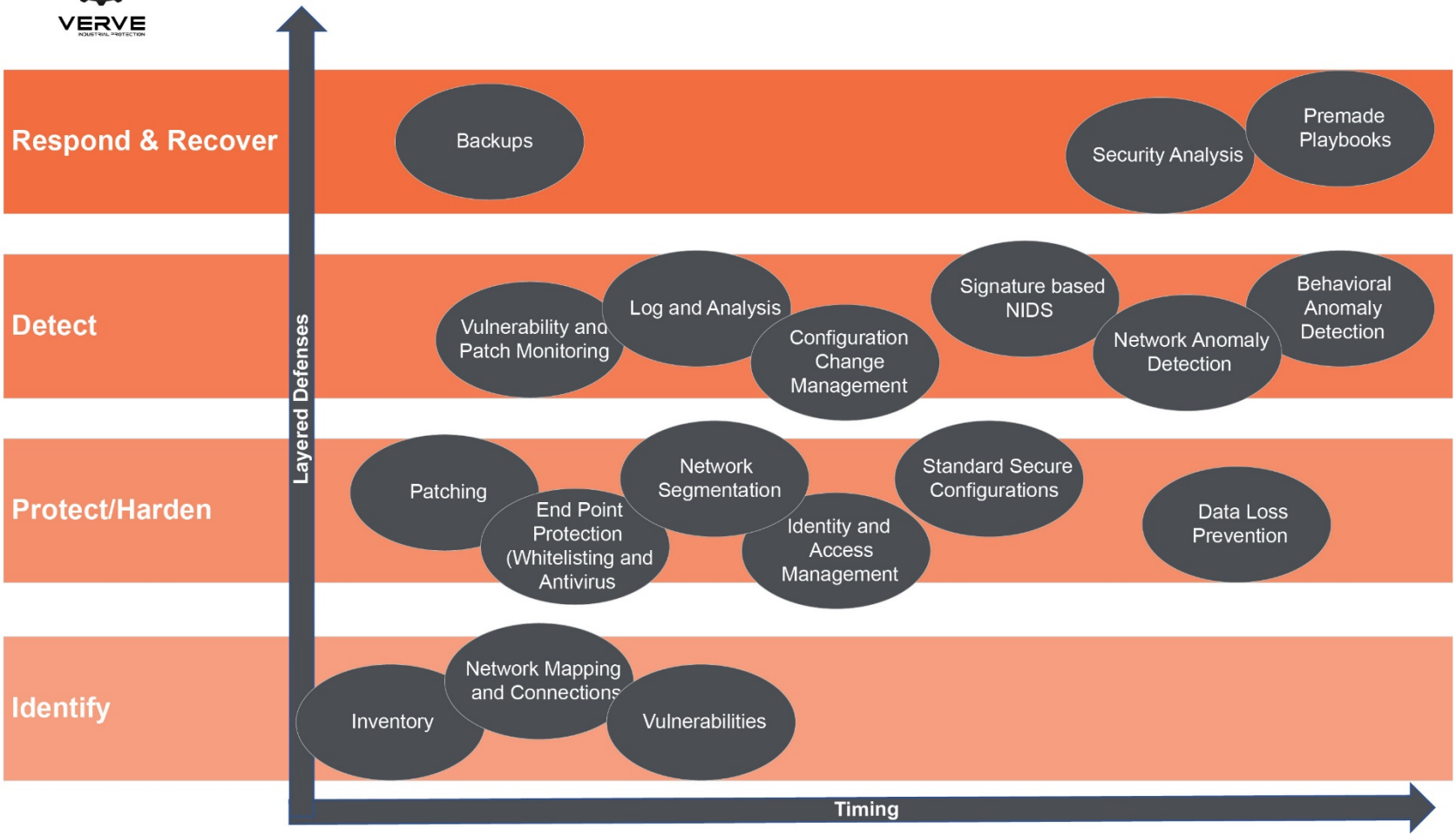


High-Level Summary

- End-point protection, detection & response is a key management concern
- Focus to solve it currently is network solutions (segmentation & monitoring)
  - Technical challenge
  - ICS vendor pushback on endpoint protection (or sale of their own solutions which don't work with other vendor systems)
  - Quality/compliance often a barrier to security
  - Ownership of OT devices often in engineering teams that are not experienced in ITSM
  - Little awareness of safe end-point solutions
  - History (or common stories) of end-point security functions impacting operations
- Result is a focus on network protection and monitoring as only reasonable solution
- EPDR is real and possible in OT/ICS/IIOT networks: safe, secure, and simple



Portfolio of Initiatives – Building a Robust Security Program



Specific Security Controls Applied Over Time as Compared to the NIST CSF Categories

Top Ten Requirements of End-point protection, detection & response

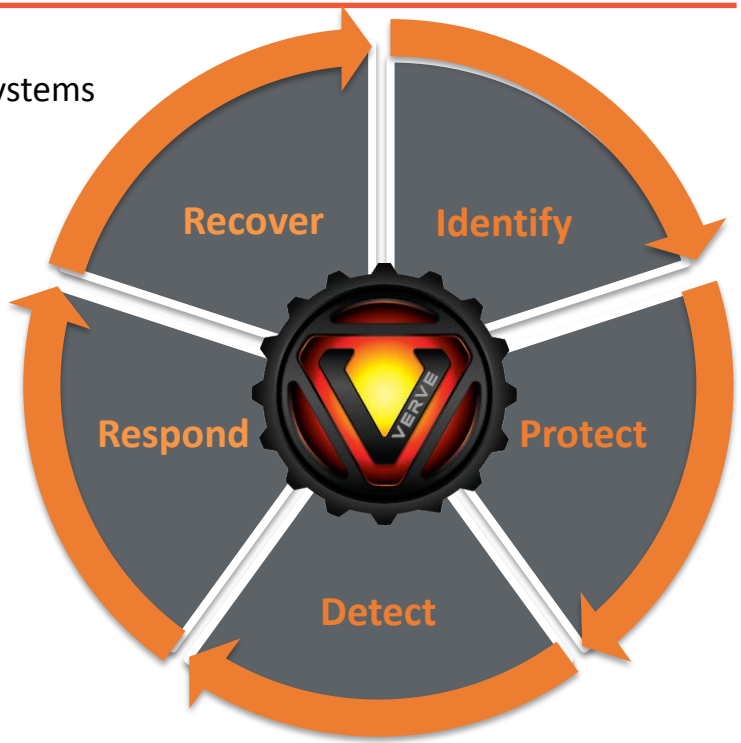
VERVE INDUSTRIAL PROTECTION

10. Vendor-agnostic
9. Hybrid “edge” and “central” architecture
8. Protect/manage all ICS OT & IT Assets
7. Provide full suite of NIST requirements
6. Send pre-packaged OT info to corporate SOC
5. Open to integrate with current tools
4. Integrate static & time-series (log) data
3. Understand process context to prioritize
2.Cost Efficient
1. Proven no impact on ICS systems (cross vendors)



Verve Security Center: A Comprehensive Solution

- Backup & restore of all systems
- Recovery procedures & Processes



- 100% Hardware & Software Asset inventory
- Configuration baselines
- Network connectivity & rules
- Vulnerability assessment

- Incident response across all endpoint and network info
- Software management
- Configuration management

- End-to-End Patch Management
- Secure configuration analysis
- Antivirus
- Application & device whitelisting
- Network segmentation
- Identity management & authentication controls

- Host Intrusion Detection/Log Management
  - Configuration change Management
- Network traffic (flows & packets) anomalies
- Integrated endpoint, network, performance Anomaly Detection