Booz | Allen | Hamilton®

SOFTWARE DEFINED CYBERSECURITY

AFCEA Cyber Symposium

JUNE 2019

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

CYBERSECURITY & RISK MANAGEMENT TODAY

TECHNOLOGY IS EVER-EVOLVING, CAN ENTERPRISE SECURITY KEEP PACE?

- **Compliance driven exercise for most organizations**
  - Minimum standards vs Improving enterprise posture
  - Compliance failure(s) and difficulties
- **Toolsets lack strategic integration and security fidelity**
  - Misconfigured or misaligned purposes
  - Lack of flexibility
- **Generic deployments lead to improper implementation**
  - Increases cost
  - Reactive vs proactive operations hinders forward learning strategy
- **Dynamic nature** of threats requires constant compliance monitoring in near real-time
- Critical Questions
  - *What's broken or non-compliant right now?*
  - *Is this the most recent snapshot of my systems?*
  - *What do I have to worry about first?*
  - *What resources are needed to resolve the problem?*
  - ***Can I execute my mission?***

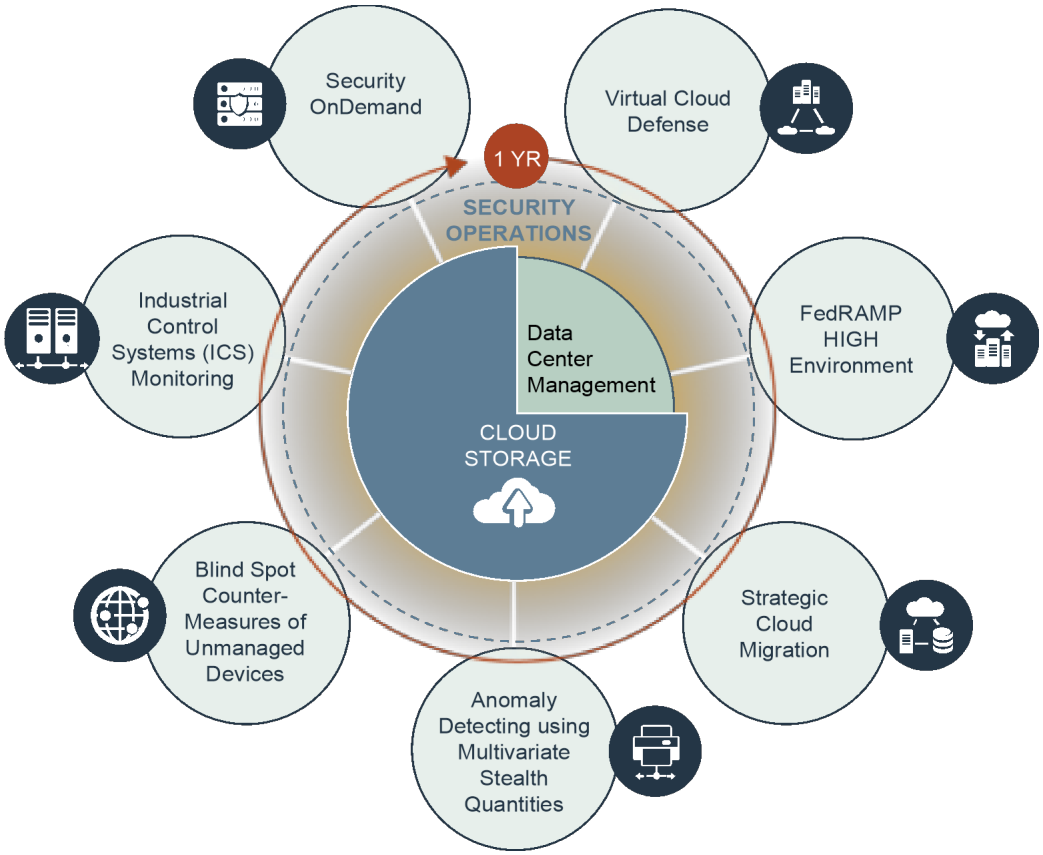
SOFTWARE DEFINED CYBERSECURITY

THE "HYBRID-CLOUD" MOBILIZES SOLUTIONS FOR ASSET STORAGE, WHY NOT SECURITY OF ASSETS?

In addition to protecting assets and data, increasing modularity of security practices can help reduce cost, increase performance, and enhance protection from cyber security measures.

- **Software Defined Cybersecurity**
  - Mobility, adaptability, and modularity
  - Real time: Prevention, detection, analysis, response
- **Software Defined Solutions**
  - Holistic approach to security
  - Hybrid solutions to include threat hunting and solution implementation
  - Reduced threat surface(s)
- **On Demand Security as a Service (SaaS)**
  - Entirely scalable
  - Optimized responses to threats
  - Minimization / Modification of Attack Surface

INTEGRATED MODULAR SECURITY DEFENSE



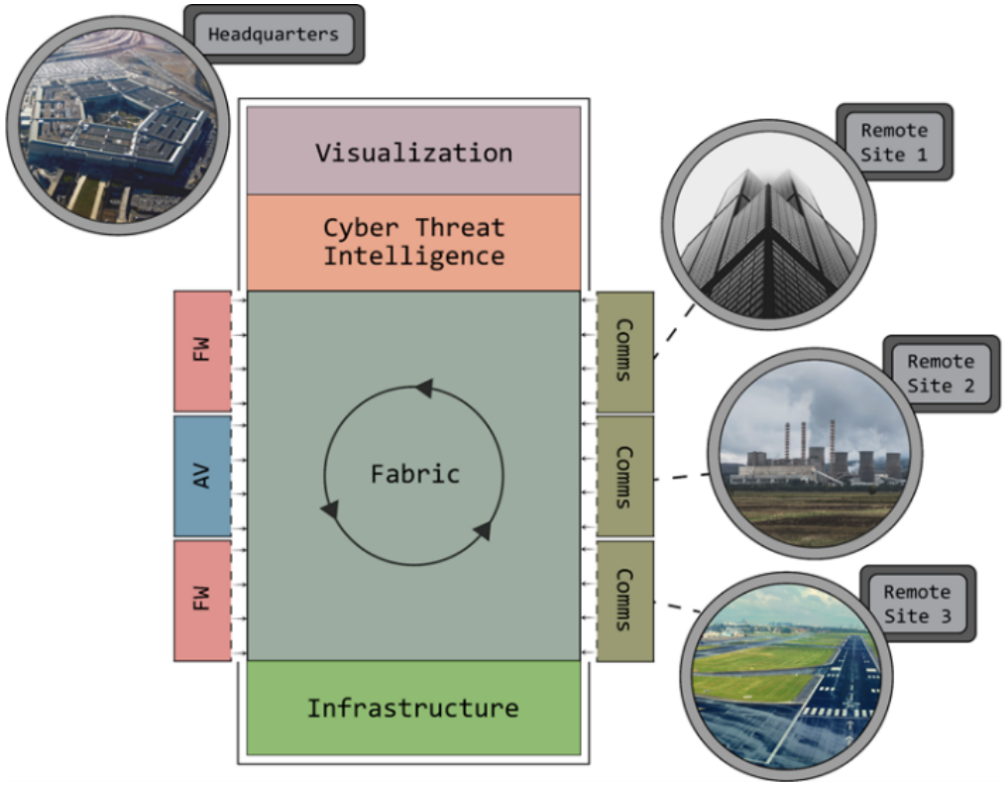
Integrated Security

Lower Total Cost

Scalability

SECURITY ONDEMAND

- Back bone consists of virtualization, microservices, cloud computing infrastructure
- Layering through modular services
- FIPS compliant encryption for communication
- Efficiently scalable design
- ***Smart Data Center***
  - Network enumeration by threat actors
  - User determines accuracy
  - Alter footprint of security devices
  - Preconfigured exploits will fail once changed

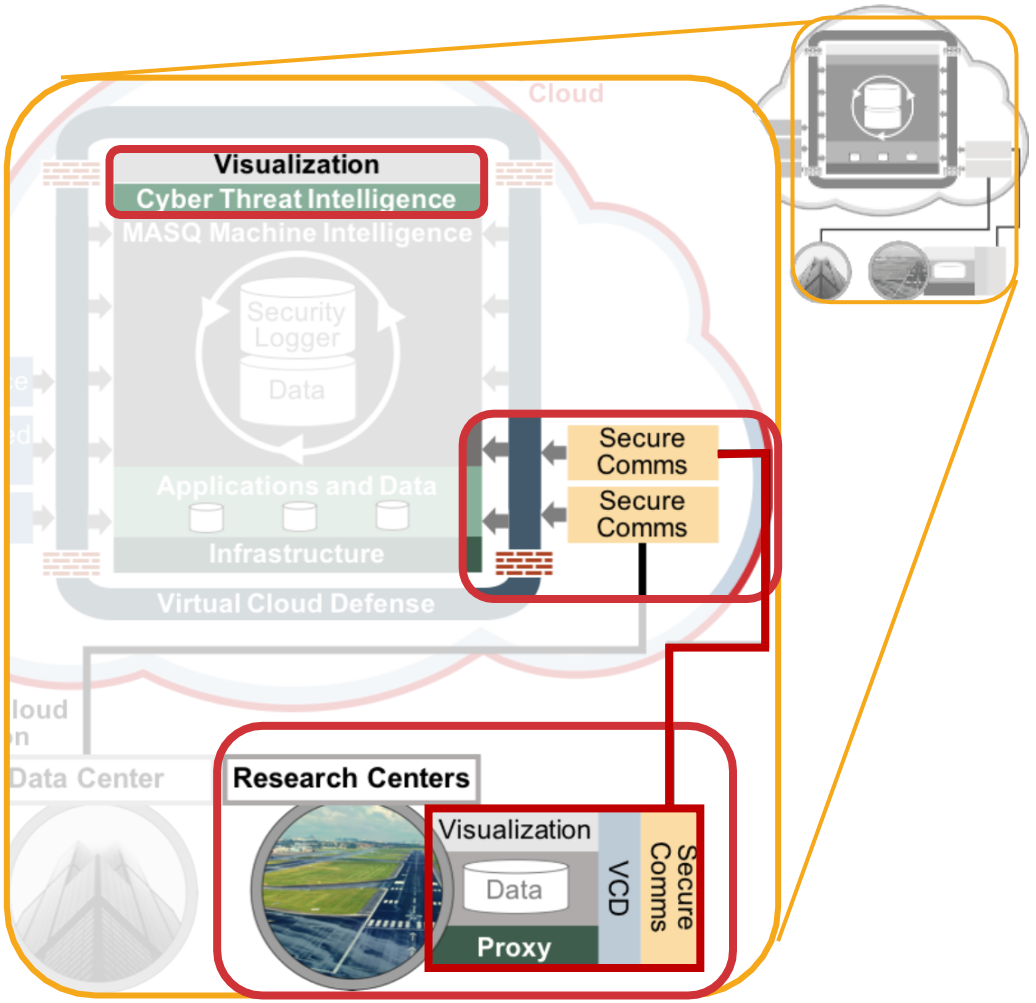


A LOOK INTO INTELLIGENT ARCHITECTURE

APPROACH

1. ***Smart Data Center*** incorporates real time threat analysis
2. Security through cloud
3. Deploy remote interface
4. Incorporates near real-time threat intelligence
5. Modify security stack, adjusts to client mission(s)
6. Continually monitor and update cloud security stack

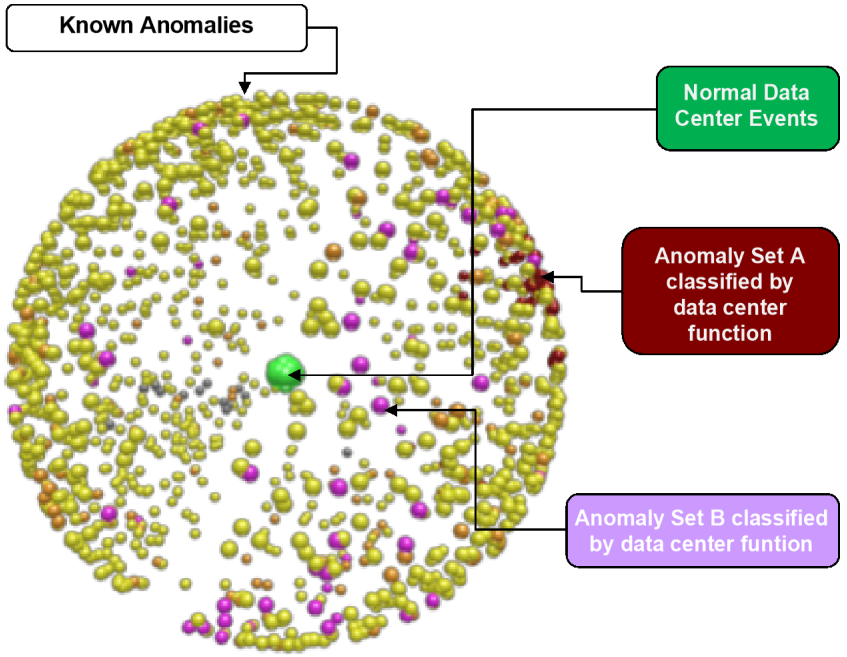
On-Demand Security allows the organization to modify its attack surface per real-time mission needs.

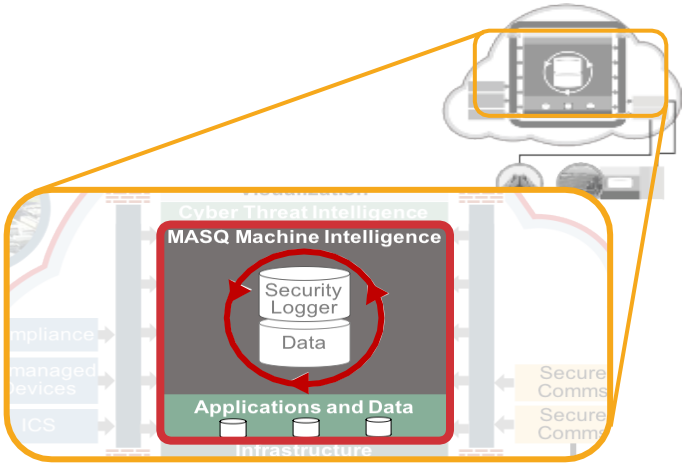


PROACTIVE DEFENSE USING MACHINE LEARNING

Steps to enhance defense & where machine intelligence fits in:

1. Identify data sets
2. Ingest selected data into MASQ algorithm
3. MASQ classifies and identifies known/unknown anomalies
4. Investigate anomalies
5. Human inspection for a fraction of anomalies (QA)

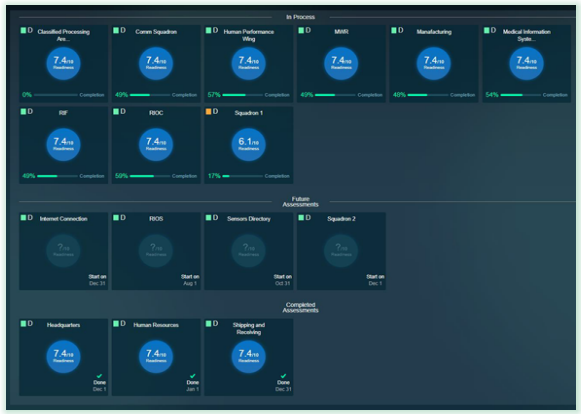


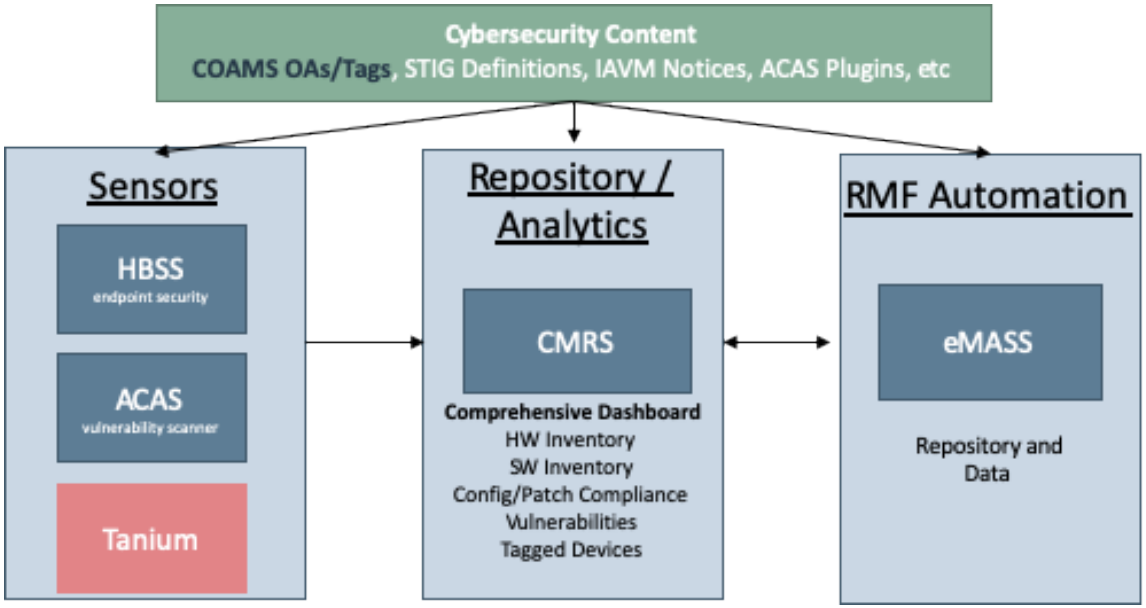


MASQ analysis will group IT functions into categories and correlate with operational outcomes, creating a ***Smart Data Center***.

ENTERPRISE RISK MANAGEMENT SOLUTION

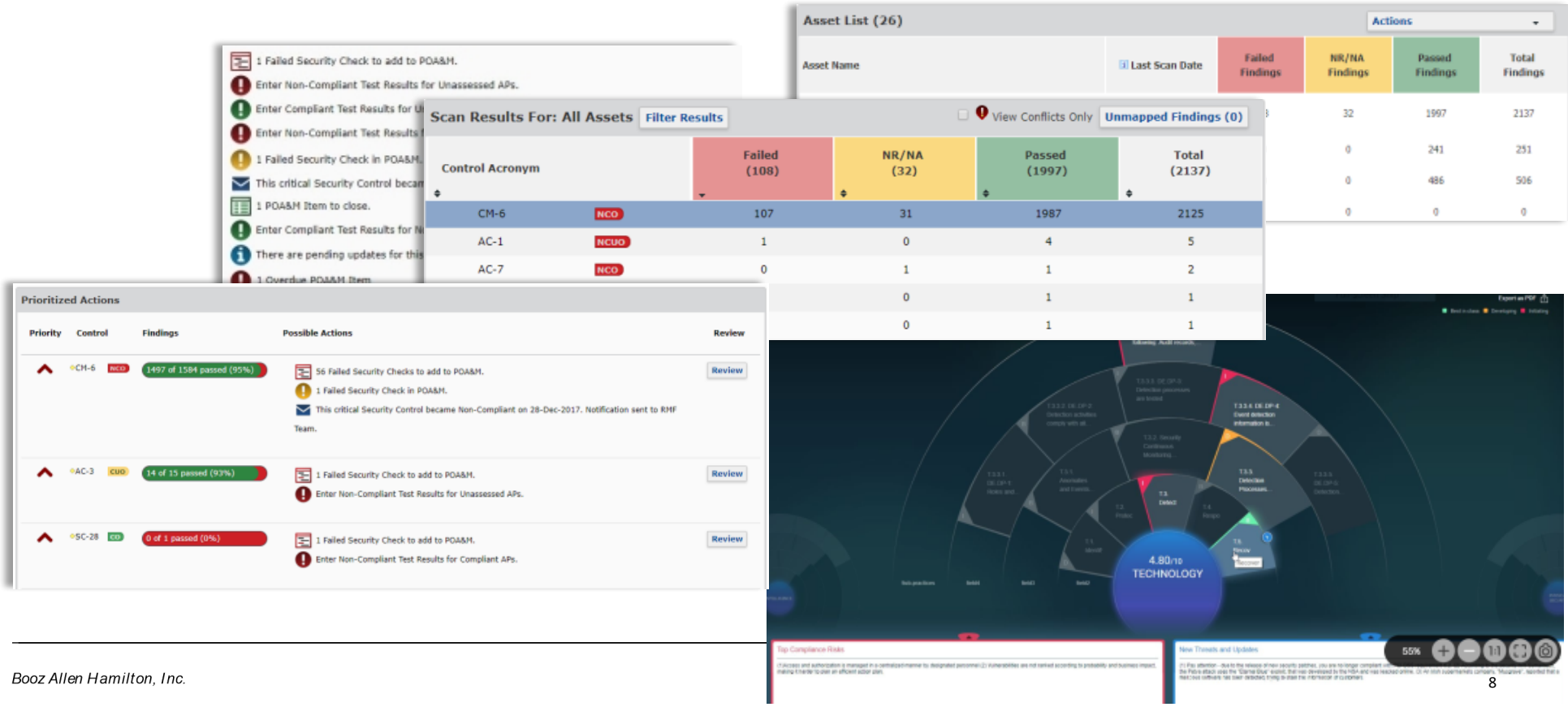
- Virtualized, modular architecture for transparency, simplicity
- Streamlined assessments of infrastructure
  - Reduce Risk Management Framework (RMF) timeline
- Enhanced baseline monitoring
- Near real-time updates
  - Security posture
  - Threat / potential impact alerts
- Reduced risk of cyber incidents
  - Less time spent on Incident Response





MOBILIZED & HOLISTIC ENTERPRISE SECURITY

- Comprehensive Dashboard
- Prioritized To-Do List
- Vulnerability Remediation
- Near Real-Time Attack Surface Modification per Intelligence Feed



THE JOURNEY TO OPTIMIZED SECURITY

CHALLENGE

Compliance Focused Security

Disintegrated Deployment of Tools

Lack of Proactive Strategy Towards Enterprise Security

OUR SOLUTION

Software Defined Security

Next generation security operations center introduces a virtualized attack surface, changing attack surface as necessary to incoming threat intelligence feeds.

1. **Reduced and Adaptive Attack Surface**

Modify attack surface through Virtual Machines (as needed); based on threat intelligence updates

2. **Secure + Scalable Architecture**

Network architecture built with security from the beginning.

3. **Lower Overall Security Costs**

Pay for security services as needed.

OUTCOME

Mobilized & Holistic Enterprise Security

Strategic Deployment of Value-Driven Tools

Active Continuous Monitoring & Progressive Security and Strategy