

# Managing Cyber Threats and Influences on Operational Strategy



SENTARA®

*Dan Bowden, Vice President & CISO  
November, 2019*

# Introduction

- Healthcare since 2007
- CISO, Technology Executive, Business Development

## What Guides Me

- Why am I doing this?
- What is my purpose?
- Who do I serve?

# Handling Cyber Security Threats

Key Technologies and Process are a must for all Organizations



## NETWORK SEGMENTATION

Practice of separating networks to protect and limit exposure to threats.



## SECURITY OPERATIONS CENTER (SOC)

Utilizing IBM Watson to be smarter at detecting and prioritizing Cyber Threats



## 2 FACTOR AUTHENTICATION

Secure Remote Access for all users

81% of hacking-related breaches leveraged either stolen and/or weak passwords



## OPERATIONAL LEADERSHIP

Key operational leaders meet monthly to review discuss and act on Cyber Security Metrics and emerging threats



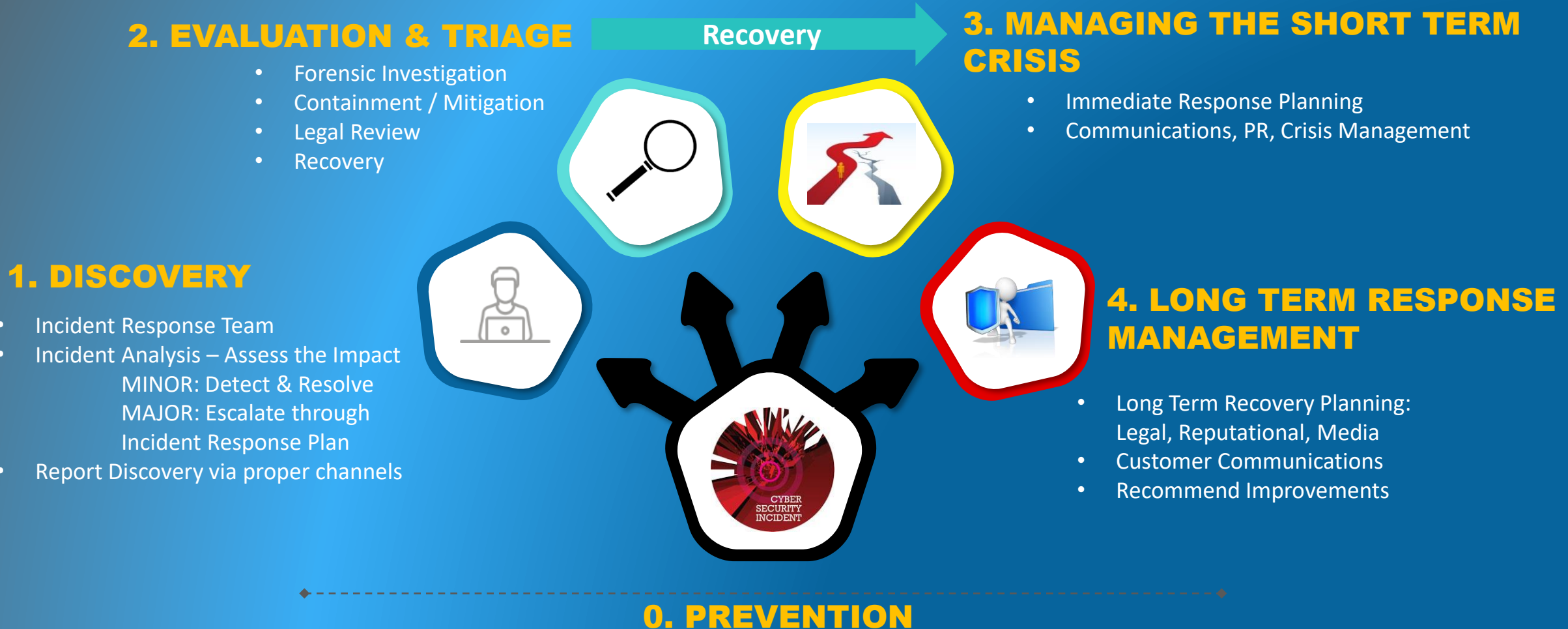
## 3<sup>rd</sup> PARTY RISK

Evaluate and manage risk from:

- Business Associates
- Subcontractors
- Affiliated Providers
- Joint Ventures
- Strategic Partners

**Many of these initiatives are visible by the Board of Directors and are stated annual organizational goals**

# How do we **respond** to a cyber security incident?



## Simplified Incident Response Strategy

# Membership of the **Incident Response Team**

- Incident Response Team leader/coordinator
- Privacy Officer
- Legal
- Risk Management
- Others as appropriate
  - Information security
  - Law Enforcement
  - HR, employee relations, patient relations
  - Public relations / Marketing
  - Fulfillment Vendor
  - Beazley/Broker
  - Outside legal counsel
  - Crisis Management Firm

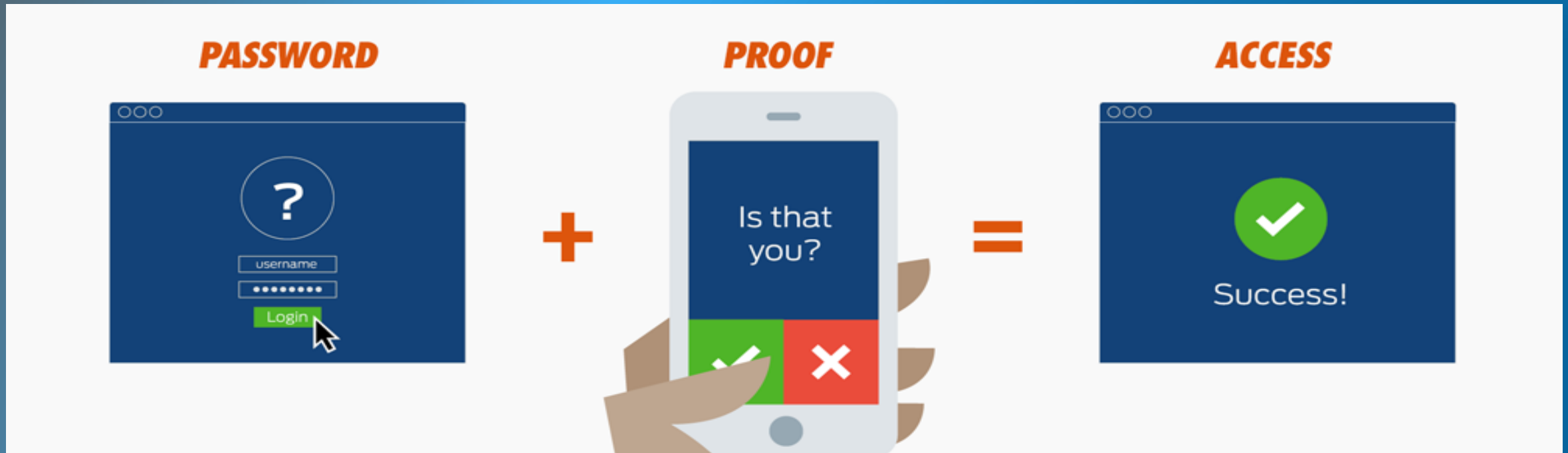


# Cyber Security influences on operational and strategic processes

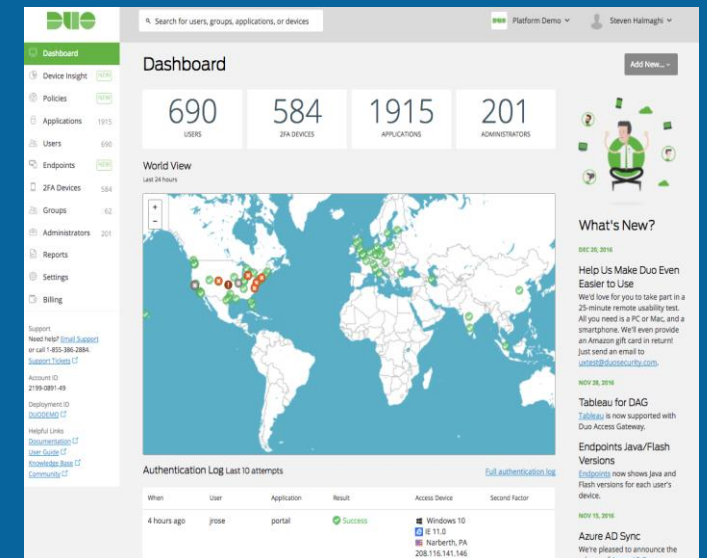
- Proactive Cyber Audits for new partnerships
- Annual Planning for Cyber Investments
- Cyber Security is a Team Sport



# What is 2 Factor Authentication?

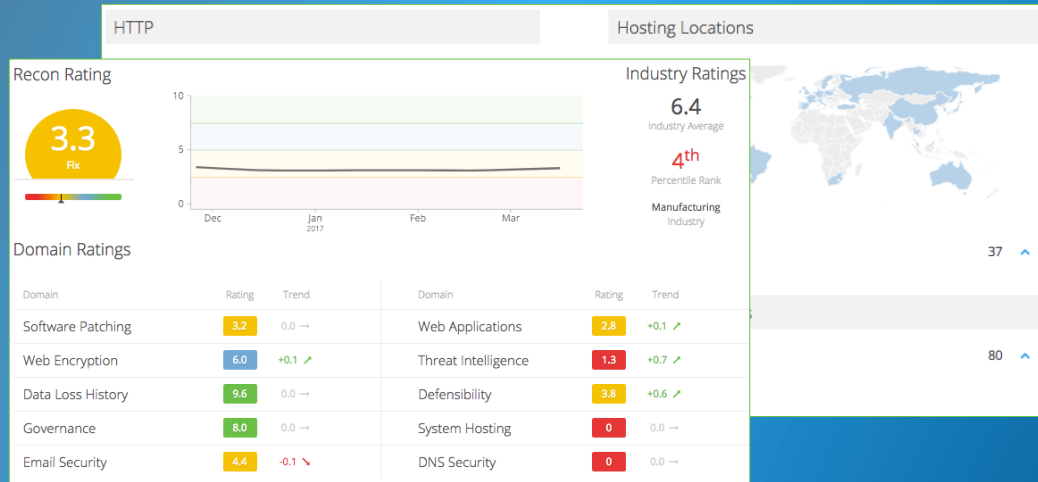


- Successful Rollout for 60,000+ Users
- Secure Remote Access for ALL workforce members
- First Wave Rollout: April 2017 (90% of workforce)
- Second Wave Rollout: June 13 (99%)
- Final Wave: Sept 1 (100%)



# Evaluating partners cyber security risk

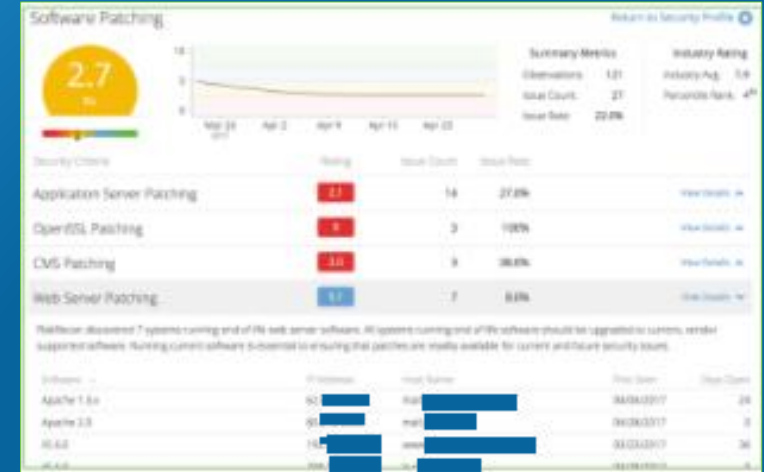
1 Gain objective insight into 3<sup>rd</sup> party cyber security



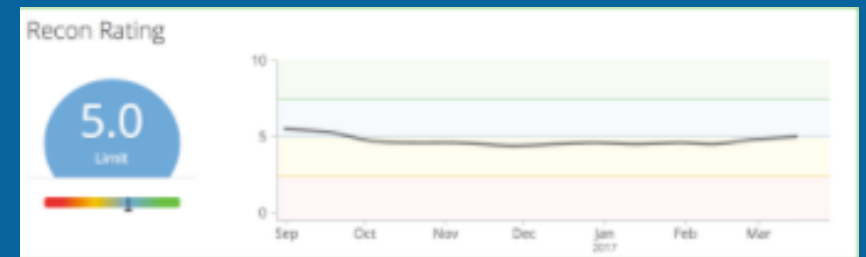
2 Allocate risk resources to where they are most needed



3 Engage partners with accurate, actionable security insights



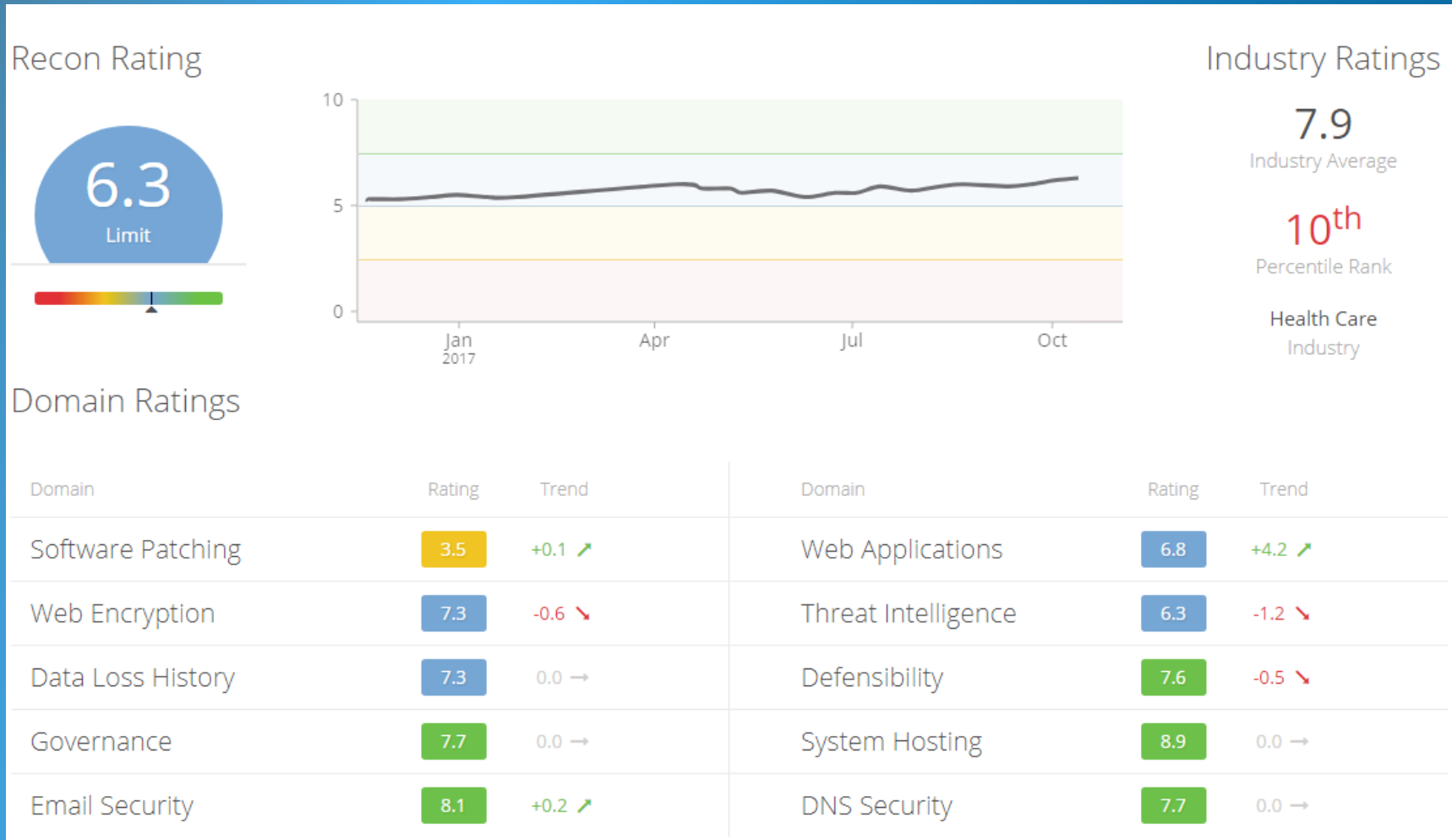
4 Continuously monitor partner performance



5) Collaborate with partners to reduce risks



# Risk Recon -- Sentara's On-line Security Credit Score



\*The CISO's proposed target scores for each area is at least 7.6

# Who are your partners in developing best practice for Cyber Security?

## WHAT IS Information Sharing & Analysis Organization (ISAO)?

*Mission: Improve the Nation's cybersecurity posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices.*



### Sentara's ISAO Partners

The image displays a collection of logos for Sentara's ISAO partners. The logos are arranged in a grid-like fashion. At the top left is the Sentara logo, featuring a yellow 'S' and the word 'SENTARA' in black. To its right is the Intermountain Healthcare logo, which includes a stylized human figure with green and blue arms and the text 'Intermountain Healthcare'. Below Sentara is the University of Utah Health logo, consisting of a red 'U' with a white DNA helix and the text 'HEALTH UNIVERSITY OF UTAH'. To its right is the Mayo Clinic logo, featuring the text 'MAYO CLINIC' above two blue shields. Further right is the Banner Health logo, which includes a blue stylized wave icon and the text 'Banner Health'. At the bottom right is the Presbyterian logo, featuring a red triangle icon and the text 'PRESBYTERIAN'.

# Information Sharing & Analysis Organization (ISAO)

Members with common cybersecurity objectives



**Proposed: Transition from “CanAudit findings”** to ongoing compliance with information security policies (to be aligned with NIST 800-171)



**Map current CAS reporting** from existing dashboard to discreet alignment with NIST 800-171 domains/categories



**CAS to audit control effectiveness** of Sentara’s implementation of NIST 800-171



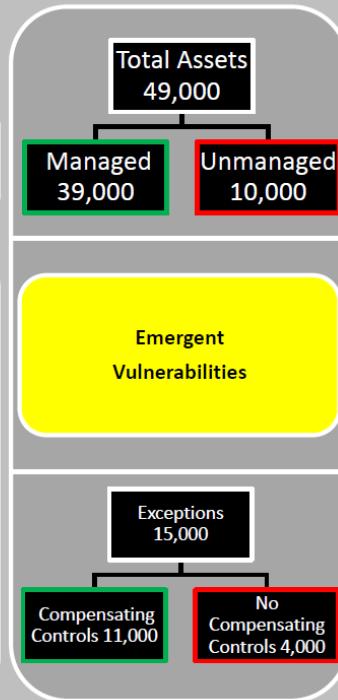
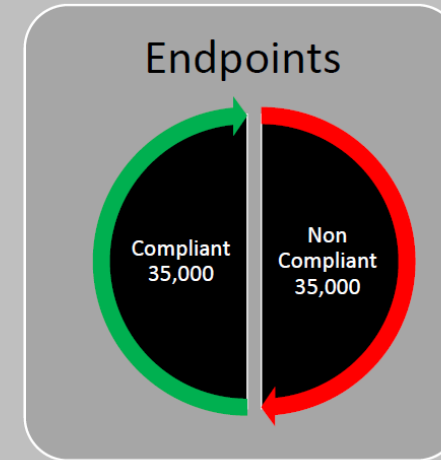
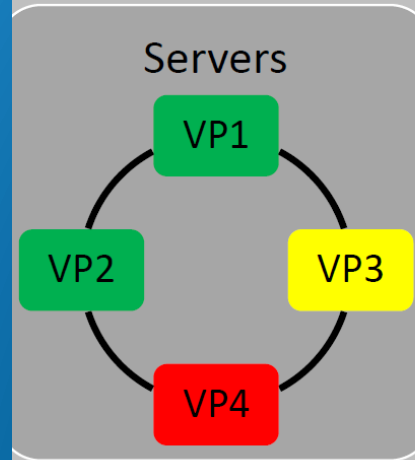
**Manage future executive and board reporting** on cyber security program compliance.



## New Vulnerability Dashboard Weekly Statistics

### Sentara's Compliance Dashboard

#### Enterprise Vulnerability



**Partnership: IT Security & Corporate Audit Services  
Risk Reporting. “Moved from RED to ORANGE to YELLOW”**

WE IMPROVE HEALTH EVERY DAY



### Provider Portal: Optimahealth.com

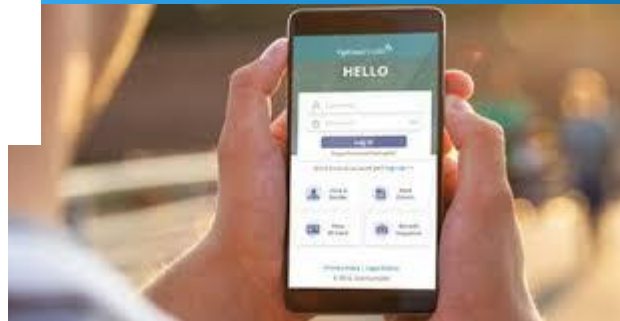
OptimaHealth.com offers providers instant access to resources and tools to optimize doing business with Optima Health. Access what you need, when you need it.

- ✓ Drug formulary and pharmacy authorization forms
- ✓ Medical authorization forms
- ✓ Easy enrollment for Electronic Funds Transfer (EFT)
- ✓ Provider Manuals
- ✓ Provider Newsletter and important updates
- ✓ Clinical guidelines and reference tools
- ✓ Provider Education tools
- ✓ Secure business transactions through Provider Connection



OptimaHealth

Easily manage your healthcare needs anytime, anywhere.



OptimaHealth



# DIGITAL BUILDING BLOCKS



## Customer Engagement

In-depth understanding of our customer through frequent engagement

## Cloud First

Leverage Microsoft, Amazon and Google

## Digital Health

Delivering healthcare in new ways

## APIs, Digital Ledgers

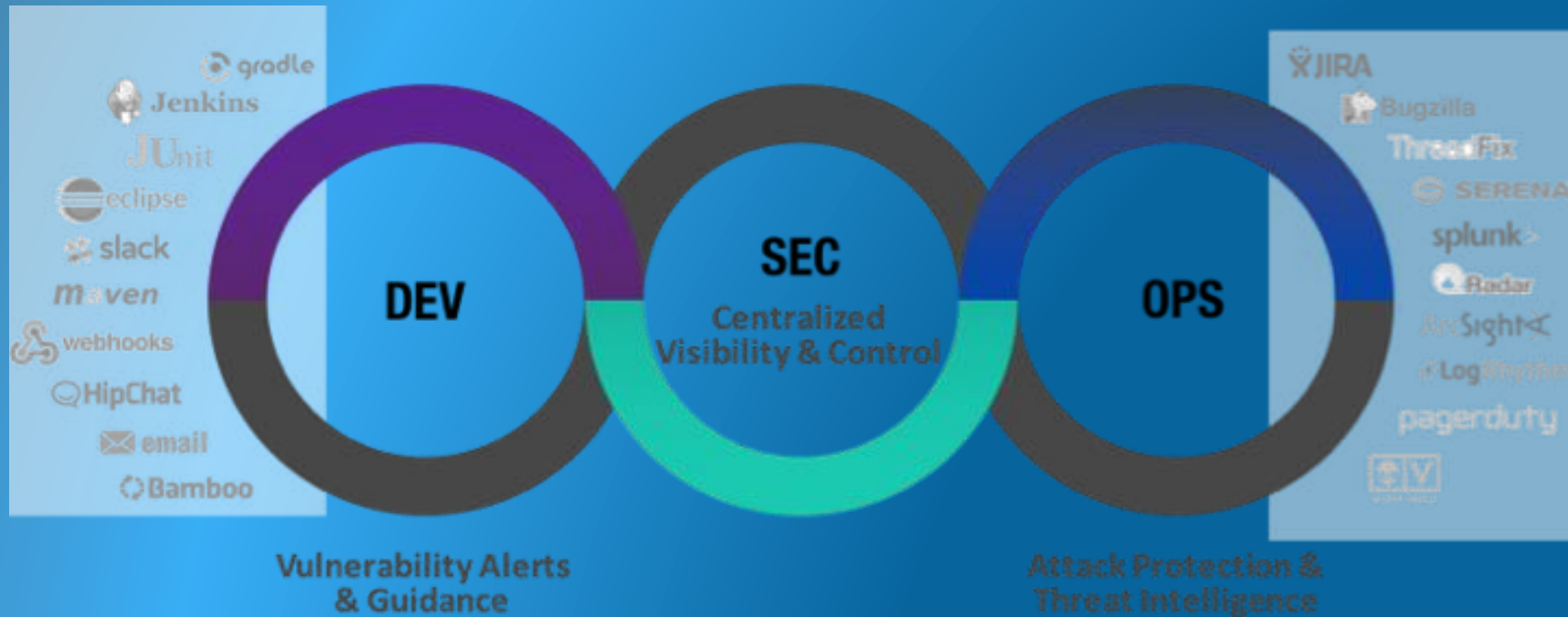
Partner connectivity, disintermediate waste, costs, inefficiency

## Consumer Data

Insights to improve customer experience and reach new customers

# CLOUD SECURITY

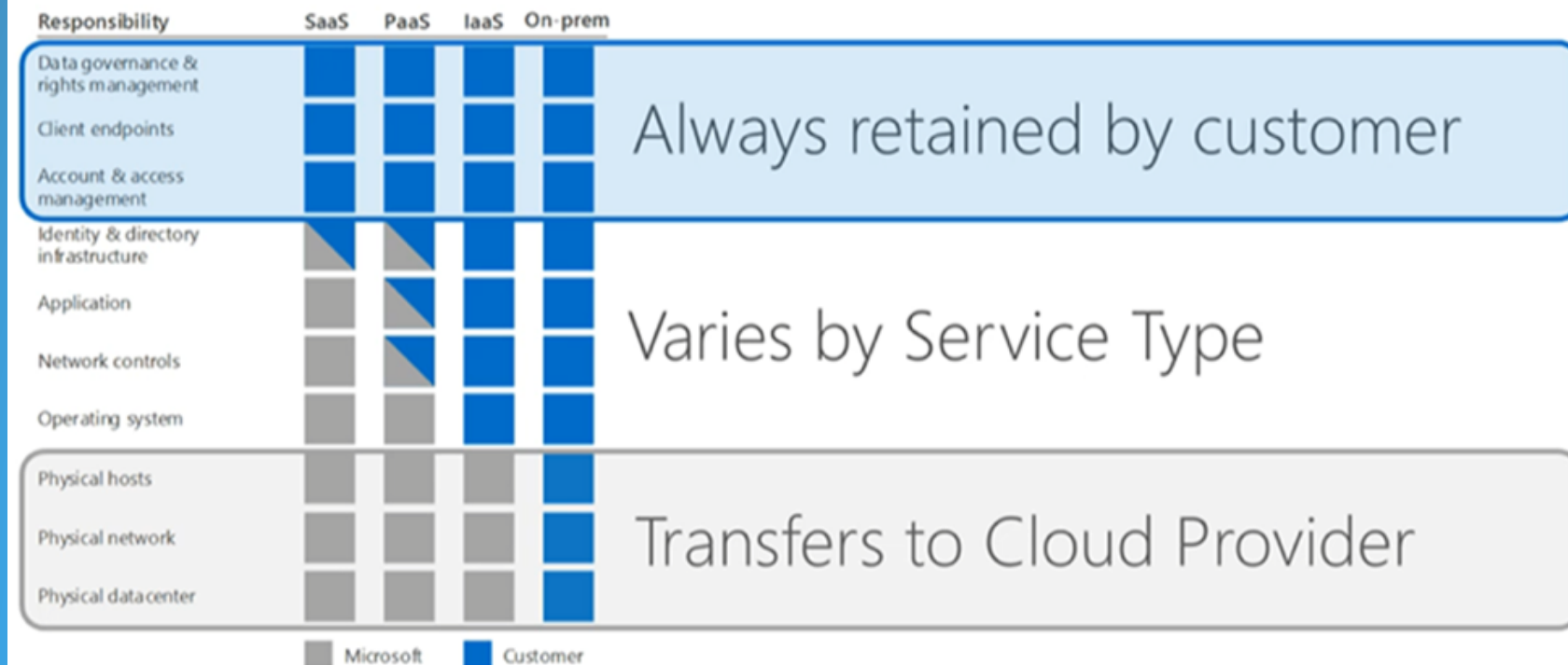
## GET IN LINE



(devsecops.com)

# CLOUD SECURITY TOOLS AND OWNERSHIP

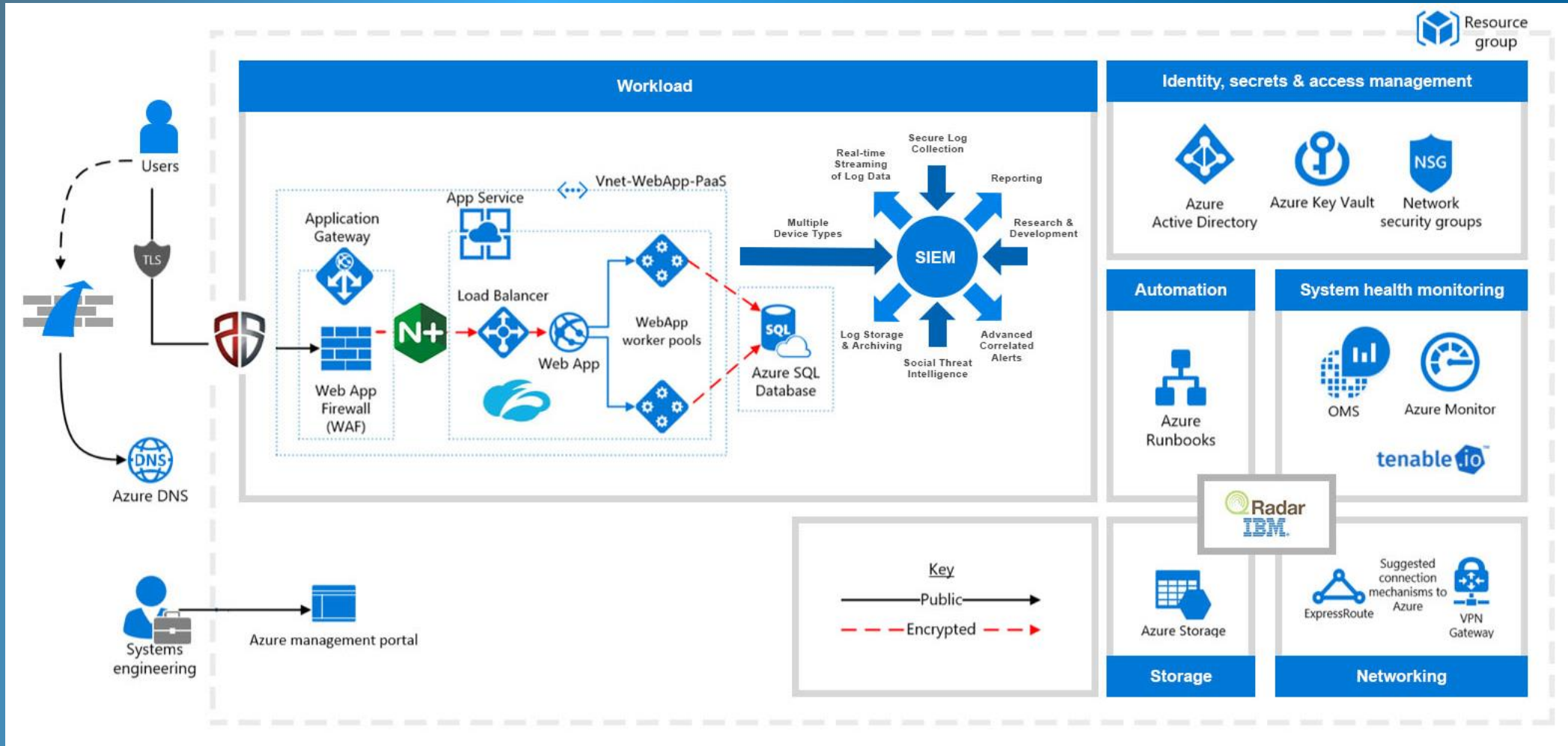
## Responsibility Zones



(Microsoft)

# CLOUD SECURITY

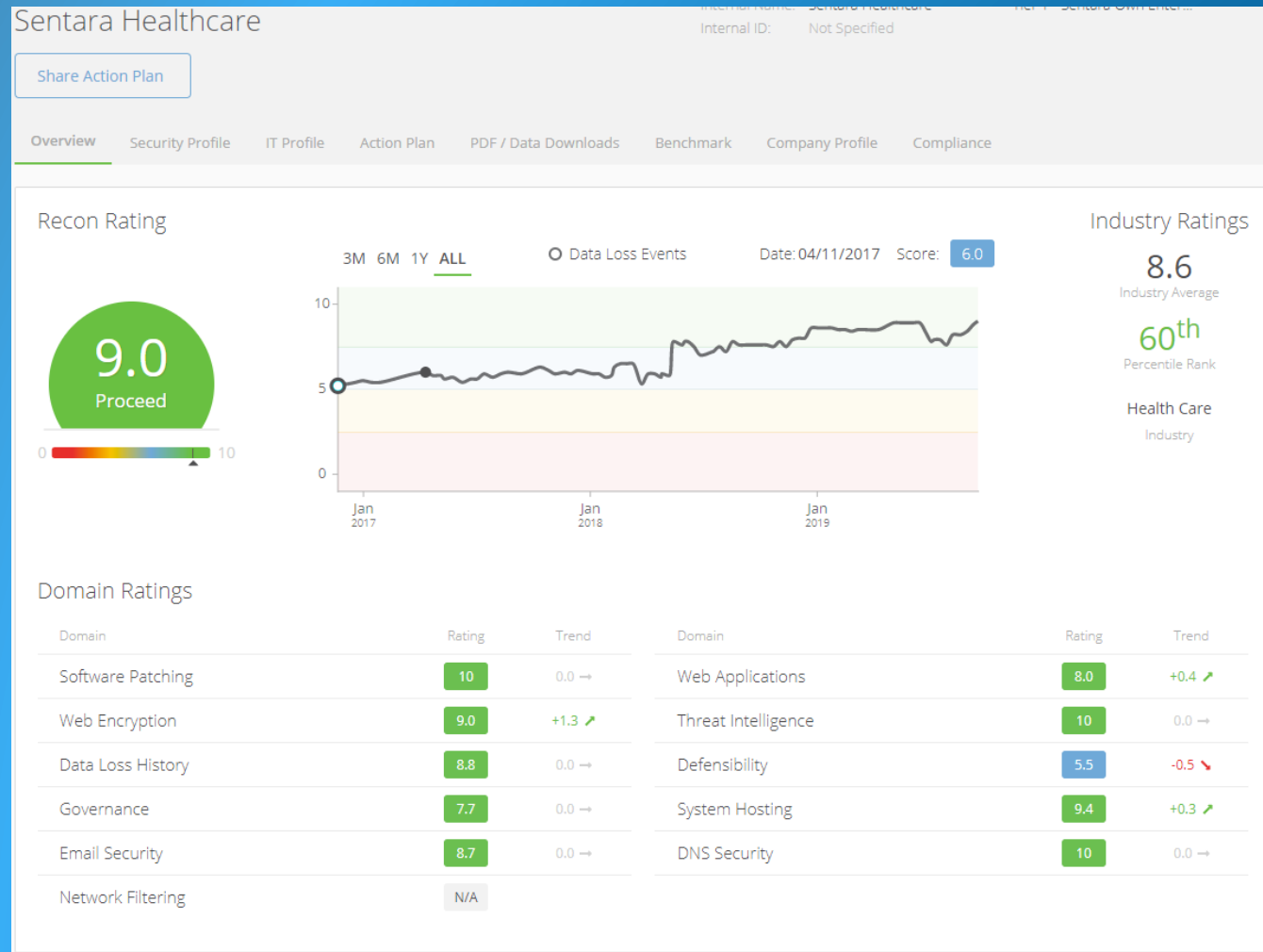
## TOOLS AND OWNERSHIP



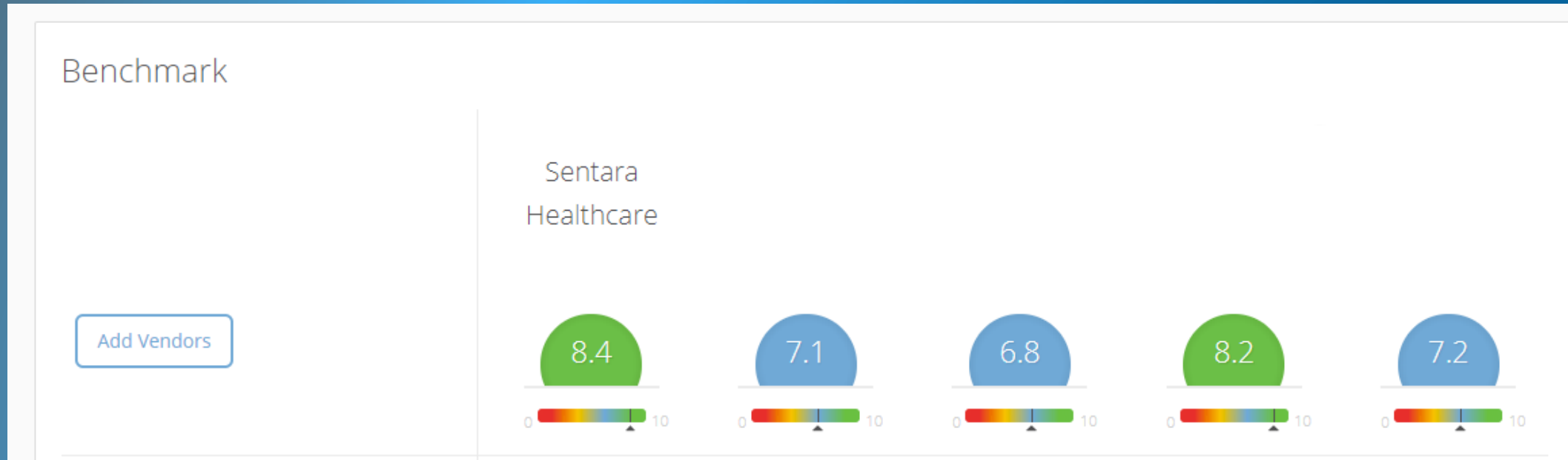
(Microsoft, IBM, Cobalt, others)



# External Vulnerability Management



# Peer Benchmarking



# Cloud Technology

- **By HIMSS20, Sentara will have completed a major partnership and founded a NewCo with the mission of providing an advanced cloud technology service for health provider organizations.**

# Blockchain

- In 2018, developed first-in-class Internet-of-Things Device Identity Management platform.
- In 2019, joined Health Utility Network. HUN is a consortium about to turn NewCo, founded by four major Insurance companies, two significant provider organizations, a large financial institution and a large technology company. HUN will develop new protocols for remediating the data accuracy and financial friction among Insurance and provider organizations.

# Hampton Roads Workforce Development

- **In 2017, the Information Security on-boarded 10 college students as continuous part-time staff.**
- **Students from Old Dominion University, Regent University, University of Virginia, Thomas Nelson Community College, and Tidewater Community College**
- **Students are significant contributors as Security Analysts and Risk Analysts**
- **Through 2019, we have leveraged these academic partnerships, creating internship and training for next generation of Cybersecurity Professionals**

**CSA Section 405(d)'s  
Mandate, Purpose, and  
Desired Goals  
FREE STUFF!**

# Cybersecurity Act of 2015 (CSA): Legislative Basis

## CSA Section 405

Improving Cybersecurity in the Health Care Industry

Section 405(b): Health  
care industry  
preparedness report

Section 405(c): Health  
Care Industry  
Cybersecurity Task Force

**Section 405(d): Aligning  
Health Care Industry  
Security Approaches**

# Industry-Led Activity to Improve Cybersecurity in the Healthcare and Public Health (HPH) Sector

## WHAT IS THE 405(d) EFFORT?



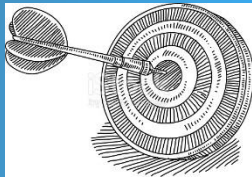
An industry-led process to develop consensus-based guidelines, practices, and methodologies to strengthen the HPH-sector's cybersecurity posture against cyber threats.

## WHO IS PARTICIPATING?



The 405(d) Task Group is convened by HHS and comprised of over 150 information security officers, medical professionals, privacy experts, and industry leaders.

## HOW WILL 405(d) ADDRESS HPH CYBERSECURITY NEEDS?



With a targeted set of applicable & voluntary practices that seeks to cost-effectively reduce the cybersecurity risks of healthcare organizations.

## WHY IS HHS CONVENING THIS EFFORT?



To strengthen the cybersecurity posture of the HPH Sector, Congress mandated the effort in the Cybersecurity Act of 2015 (CSA), Section 405(d).

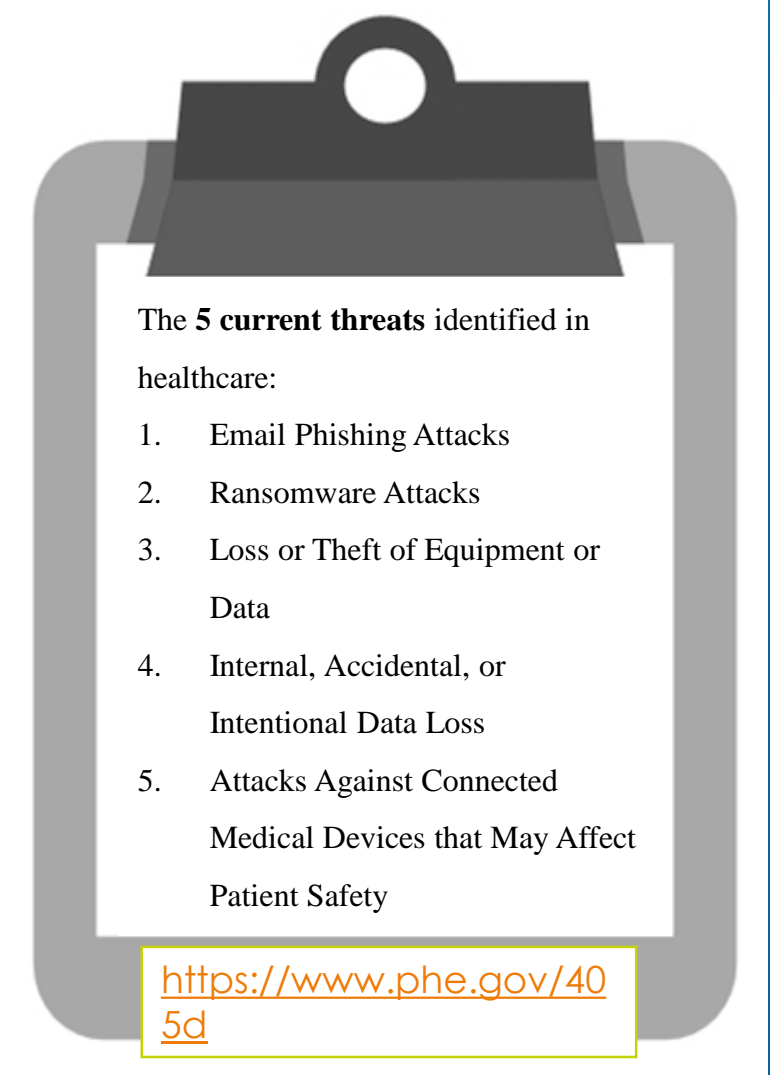


# HICP Publication Overview

# Document - Content Overview (1/2)

After significant analysis of the current cybersecurity issues facing the HPH Sector, the Task Group agreed on the development of three documents—a main document and two technical volumes, and a robust appendix of resources and templates:

- The main document examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.
- *Technical Volume 1* discusses these ten cybersecurity practices for **small** healthcare organizations.
- *Technical Volume 2* discusses these ten cybersecurity practices for **medium and large** healthcare organizations.
- *Resources and Templates* provides mappings to the NIST Cybersecurity Framework, a HICP assessment process, templates and acknowledgements for its development.



The **5 current threats** identified in healthcare:

1. Email Phishing Attacks
2. Ransomware Attacks
3. Loss or Theft of Equipment or Data
4. Internal, Accidental, or Intentional Data Loss
5. Attacks Against Connected Medical Devices that May Affect Patient Safety

<https://www.phe.gov/405d>

# Document - Content Overview (2/2)

The document identifies **ten (10) practices**, which are tailored to small, medium, and large organizations and discussed in further detail in the technical volumes:

- 1 Email Protection Systems
- 2 Endpoint Protection Systems
- 3 Access Management
- 4 Data Protection and Loss Prevention
- 5 Asset Management
- 6 Network Management
- 7 Vulnerability Management
- 8 Incident Response
- 9 Medical Device Security
- 10 Cybersecurity Policies

# Using HICP and Supporting Resources

**[PHE.GOV/405d](https://www.phe.gov/405d)**

# Introduction and Executive Summary

## HICP is...

- A call to action to manage real cyber threats
- Written for multiple audiences (clinicians, executives, and technical)
- Designed to account for organizational size and complexity (small, medium and large)
- A reference to “get you started” while linking to other existing knowledge
- Aligned to the NIST Cybersecurity Framework
- Voluntary

## HICP is **not**...

- ▶ A new regulation
- ▶ An expectation of minimum baseline practices to be implemented in all organizations
- ▶ The definition of “reasonable security measures” in the legal system
- ▶ An exhaustive evaluation of all methods and manners to manage the threats identified
  - You might have other practices in place that are more effective than what was outlined!
- ▶ Your guide to HIPAA, GDPR, State Law, PCI, or any other compliance framework

# A Unique Partnership



## Service Enablement

- Tier-1/2/3 Event Analysis
- Threat Hunting
- Technology Management
- Vulnerability Management

## Healthcare Expertise

- Security Program Leadership
- Healthcare Incident Response
- Compliance Guidance

## Technology Leader

- Gartner SIEM Leader
- Cloud-based technology
- AI Driven Tier-1 Analysis
- Threat Intel Integration

For further information, contact Gene Ridge at (773)-571-0618 or [gridge@medgrup.net](mailto:gridge@medgrup.net)

# Questions?

Dan Bowden

[dsbowden@sentara.com](mailto:dsbowden@sentara.com)

[deltasbravo@yahoo.com](mailto:deltasbravo@yahoo.com)

Office: 757-252-0475

Mobile: 801-518-9087

