Protecting Patient Data, Credit Cards, and Healthcare Organizations

12 › 23 › 2020

CARSON&SAINT

Cybersecurity and risk-management services you can trust.

Protecting Patient Data, Credit Cards, and Healthcare Organizations

Agenda

- About Carson & SAINT
- Healthcare Solutions
- Cybersecurity Products

12 › 23 › 2020

Cybersecurity and risk-management

Cybersecurity Services and Software Experts

Trusted Partner to our Customers

- Award-Winning Security
  - Customers: Public and Private

Deep Experience

- Cybersecurity technology
- Industry-specific solutions
- Healthcare security services

Your Trusted Partner

What does Trusted Partner mean?

- Dedicated, committed team
- Decades of experience
- Full stack of essential technology, operations, and procedures
- SAINT vulnerability scanning suite
- PCI Qualified Security Assessor
- PCI Approved Scanning Vendor
- Experts in HIPAA and healthcare risk

Types of Customers

Industries That Trust Carson & SAINT

- Medical Centers
- Hospitals
- Assisted Living Facilities
- Educational Institutions (Local Colleges, Major Universities)
- Financial Organizations
- Payment Card Service Providers
- Retailers and Product Vendors
- Small and Medium Businesses
- Large-Scale Enterprises
- Local, State, and Federal Government
- Utilities
- Compliance Organizations
- Managed Services Providers
- Managed Security Service Providers

HIPAA Expertise

Some of the Healthcare Organizations That Trust Carson & SAINT

Lutheran Social Ministries of Maryland (CCRC)

Department of Health and Human Services

Hanover Hospital

Harvard Medical School

Integrated Health Management Solutions

National Institutes of Health

Southern Tier Pediatrics

UMPC - University of Pittsburgh Medical Center

Veterans Administration

Other Organizations That Trust Carson & SAINT

Federal Trade Commission

Nuclear Regulatory Commission

Department of Homeland Security

Defense Information Systems Agency

General Services Administration

Cyber Tactics without Cyber Strategy is the breeding-ground of breaches

Management Services

Get **answers.**
Reduce **risk.**

Industry Solutions

Find your answer.
Trust our experience.

Cybersecurity Products

Take **control.**
Manage **risk.**

Partners

Maximize service.
Build **success.**

HIPAA Expertise

HIPAA: We Make it work *for* you

- Risk & Gap Analysis
- Risk management, Remediation Roadmaps
- HIPAA Security Officer, HIPAA Policies & Procedures
- Security Awareness Training Materials
- Improve organizational wellbeing
- Full spectrum of services and technologies
- Experience with both large and small organizations
- Decades of experience

How We're Different

Administrative Safeguards

Physical Safeguards

Technical Safeguards

Organizational Safeguards

Policies and Procedures

PRODUCE COMPLETE RISK ANALYSIS

FOR ALL HIPAA REQUIREMENTS

Our Experts

Information Assurance

- Advanced degrees
- Technical certifications:
  - PCI ASV/QSA
  - CEH
  - CISA
  - CISSP
  - CRISC
  - GPEN
  - GWAPT
  - ISO 27001
  - LPT

Subject Matter Experts

- Compliance certifications:
  - HIPAA
  - PCI ASV/QSA
  - FedRAMP
  - FERPA
  - FFIEC
  - FINRA
  - FISMA
  - ISO 27001
  - SEC
  - SOX

HIPAA and PCI – Build a more secure Community

Credit card use in Healthcare

- Medical services
- Gift shops
- Hospital café

Standards synergy: HIPAA + PCI

- strong standards of HIPAA
- strong technical requirements of PCI

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council™
APPROVED SCANNING VENDOR

Integration Points

SAINT®

Any cybersecurity report that never leaves IT is ineffectual

Our goal is to show corporate risk teams that by joining their standards, methodologies and desires to make their organization safe with more than just the output of SAINT, but the meanings, implications and application of the SAINT responses and risk vectors, they have the ability to create a single, seamless, solution to their cyber risks.

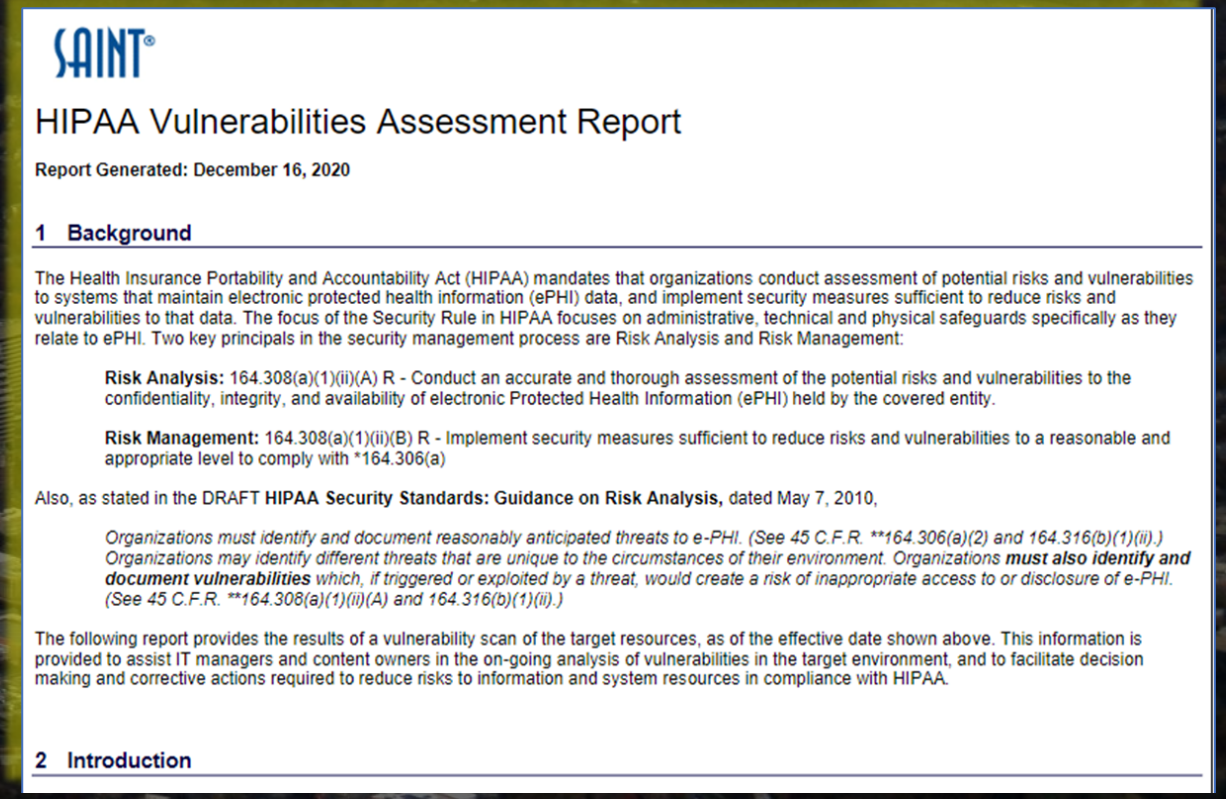
How We're Different

Start where you are weakest

SAINT Discovery

SAINT Content

SAINT Scans



SAINT®

HIPAA Vulnerabilities Assessment Report

Report Generated: December 16, 2020

1 Background

The Health Insurance Portability and Accountability Act (HIPAA) mandates that organizations conduct assessment of potential risks and vulnerabilities to systems that maintain electronic protected health information (ePHI) data, and implement security measures sufficient to reduce risks and vulnerabilities to that data. The focus of the Security Rule in HIPAA focuses on administrative, technical and physical safeguards specifically as they relate to ePHI. Two key principals in the security management process are Risk Analysis and Risk Management:

Risk Analysis: 164.308(a)(1)(ii)(A) R - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) held by the covered entity.

Risk Management: 164.308(a)(1)(ii)(B) R - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with *164.306(a)

Also, as stated in the DRAFT **HIPAA Security Standards: Guidance on Risk Analysis,** dated May 7, 2010,

*Organizations must identify and document reasonably anticipated threats to e-PHI. (See 45 C.F.R. **164.306(a)(2) and 164.316(b)(1)(ii).) Organizations may identify different threats that are unique to the circumstances of their environment. Organizations **must also identify and document vulnerabilities** which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI. (See 45 C.F.R. **164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)*

The following report provides the results of a vulnerability scan of the target resources, as of the effective date shown above. This information is provided to assist IT managers and content owners in the on-going analysis of vulnerabilities in the target environment, and to facilitate decision making and corrective actions required to reduce risks to information and system resources in compliance with HIPAA.

2 Introduction

Know Organizational Risk

SAINT® Security Suite Capabilities

SAINT®

- HIPAA & PCI compliance scanning
- Discovery Scanning
- Vulnerability management
- Configuration assessment
- Social engineering
- Content Search for Credit cards and social security #
- Penetration testing
- Asset management
- Advanced analytics
- Incident response
- Reporting
- Third-party integration

The World Trusts Carson & SAINT

65
Countries

1,876,712+
ASV Attestations

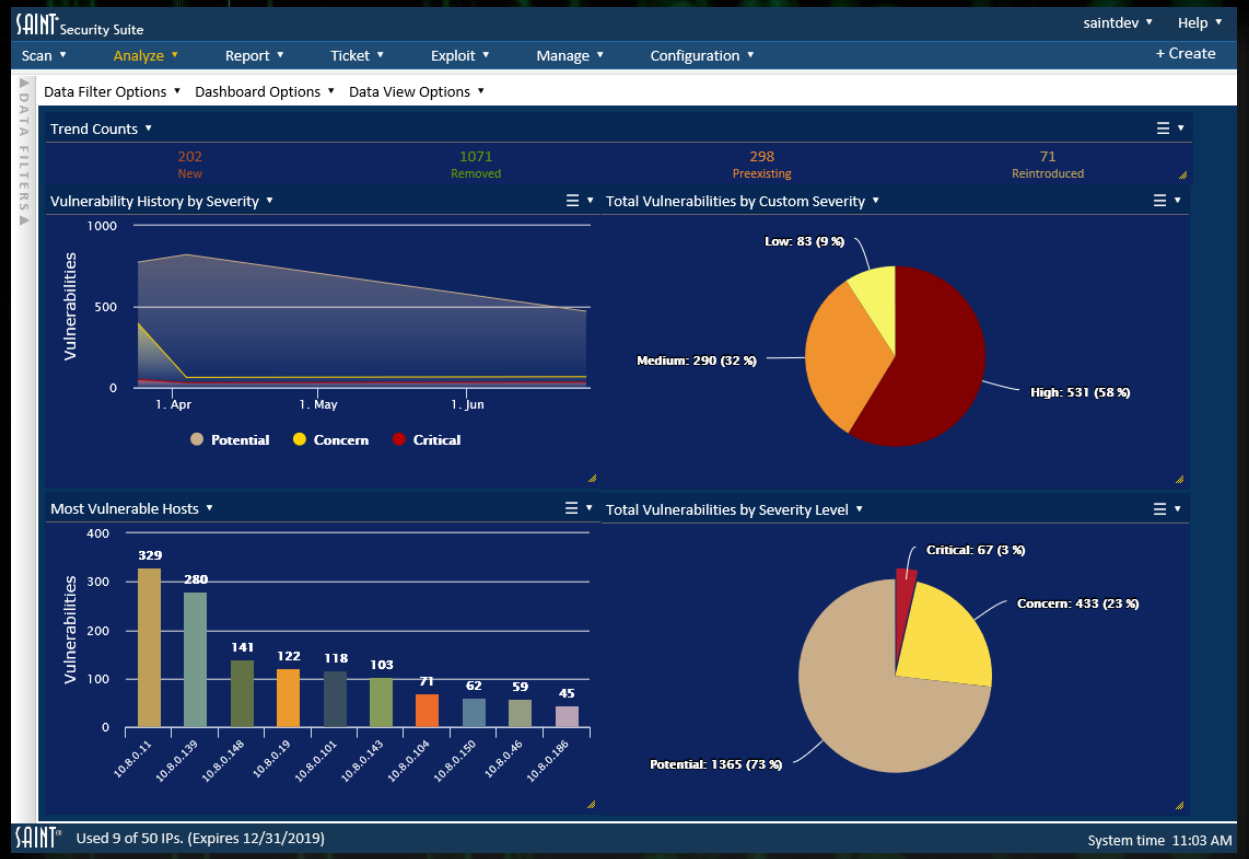
20,845,653+
Customer Assets Scanned Annually

SAINT Features and Offerings

The SAINT Security Suite provides a single, fully-integrated suite of security capabilities that scale from small to large deployments.

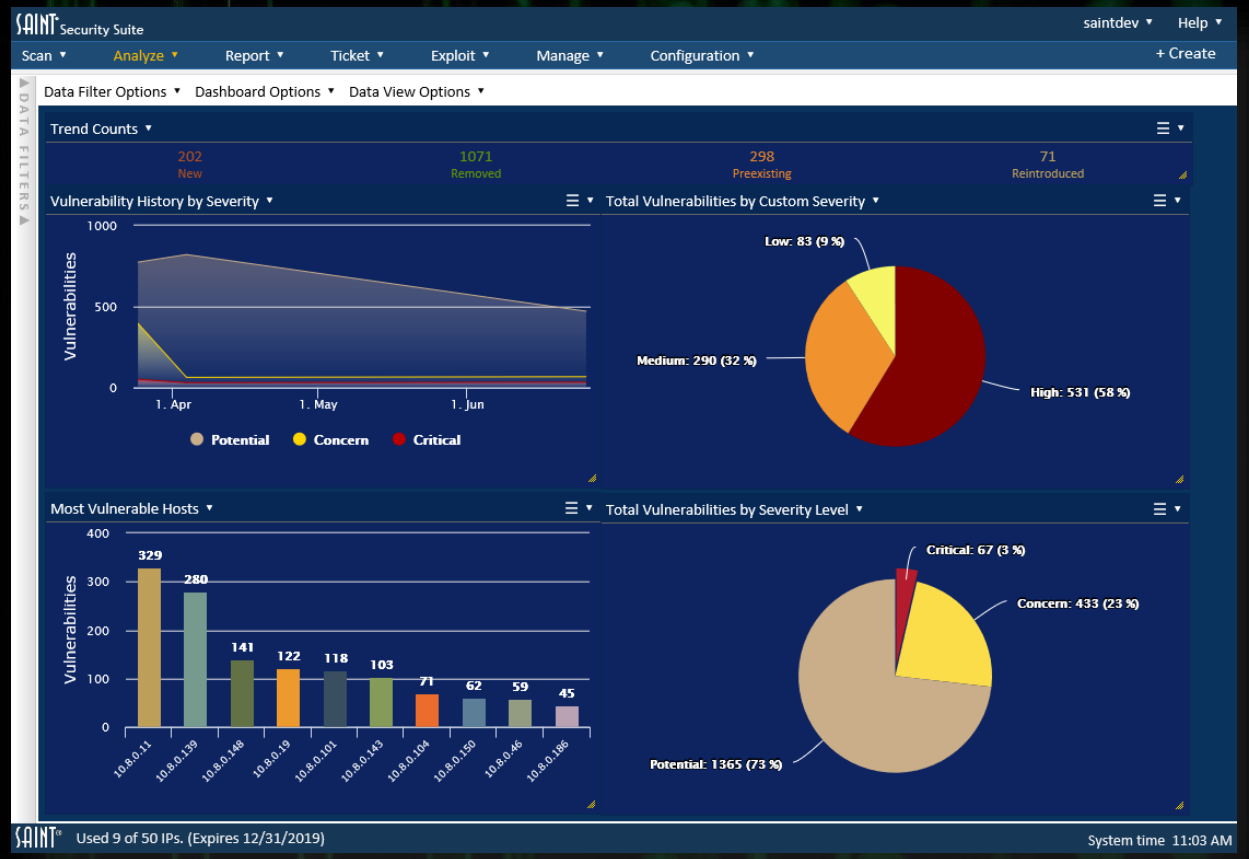
Feature highlights:

- Centralized management console
- Highly scalable (distributed scan architecture)
- Multi-tenancy support
- Agent and agentless scan options
- Asset classification
- VPC and instance mapping for cloud
- Custom severities
- Custom policies



SAINT Features and Offerings

The SAINT Security Suite provides a single, fully-integrated suite of security capabilities that scale from small to large deployments.



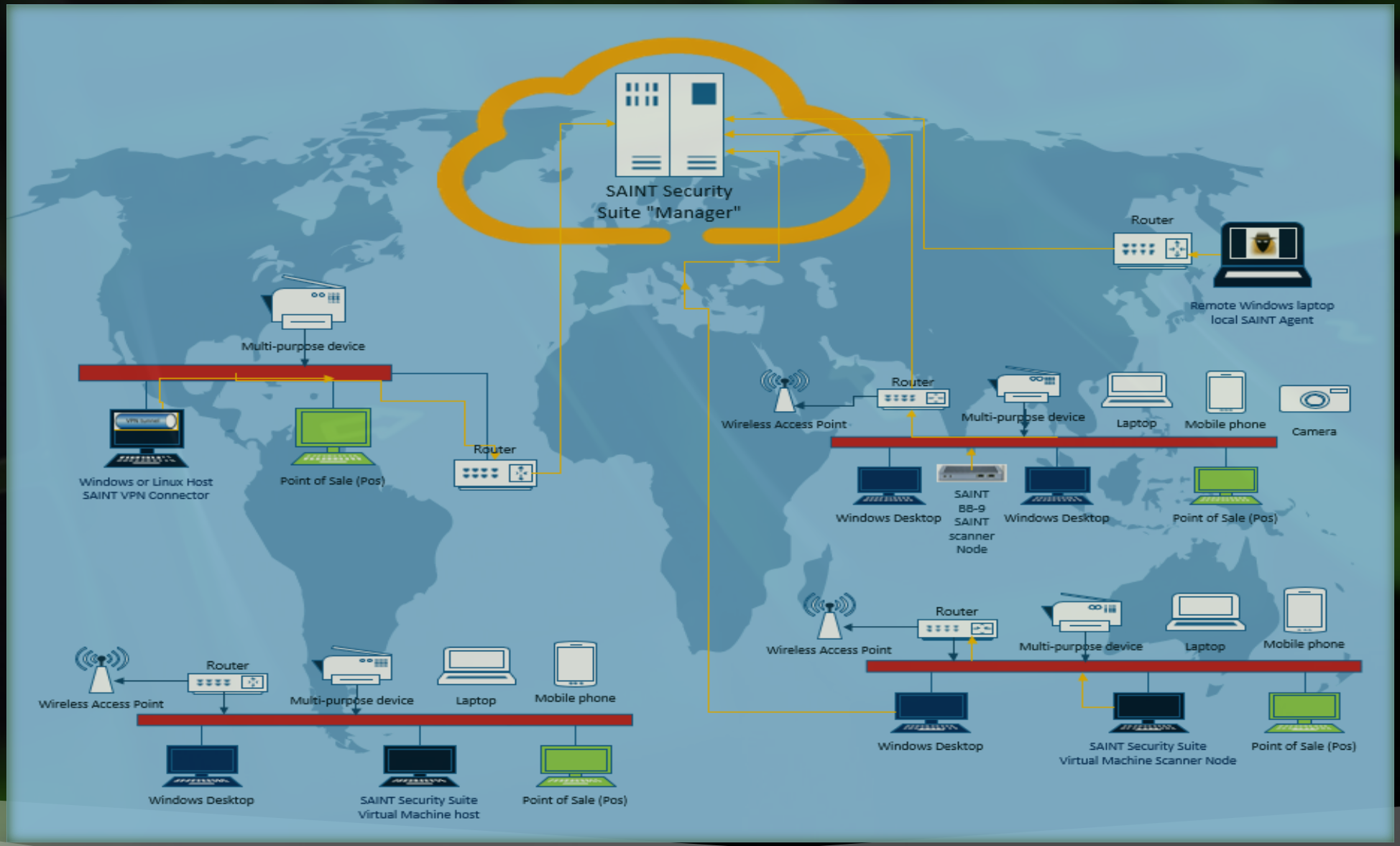
Feature highlights (continued):

- Vulnerability assessments (VA)
- Credentialed and un-credentialed scanning
- Social engineering tools
- Penetration testing
- Configuration auditing (NIST and CIS)
- Remediation ticketing
- Pre-designed and customizable report templates
- Pre-configured compliance scan policies and report templates
- REST API and third-party integration support

SAINT Features and Offerings

SAINT Key Features Matrix															
CAPABILITY	SAINT Security Suite	SAINT Security Suite - Enterprise	SAINT Security Suite - Standard	SAINT scanner	SAINTsmb	SAINT Cloud	SAINT Consultant	SAINT Consultant PRO	SAINT AWS (BYOL)	SAINT AWS (With License) Ubuntu	SAINT AWS (With License) RED HAT	SAINT AWS (Pre-auth) Scanner	Tr-3	SAINTbox and BB-9 Node	BB-9 SAINTsmb Bundle
Number of Hosts included in License		500	300	300	100		1,000	1,000		Unlimited	Unlimited				100
Free Discovery Scan	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔				✔
Vulnerability Scanning	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔		✔
Benchmark Scanning	✔	✔	✔	✔			✔	✔	✔	✔	✔				✔
Passive Scanning	✔	✔	✔					✔							
Penetration Testing	✔	✔				✔		✔	✔	✔	✔				
Social Engineering	✔	✔				✔		✔	✔	✔	✔				
Asset Tagging	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔				✔
Custom Severities	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔				✔
Vulnerability-to-Exploit mapping	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔				✔
Ticketing	✔	✔	✔				✔	✔	✔	✔	✔				
Multi-user and Group management	✔	✔	✔	✔		✔		✔	✔	✔	✔				
Multi-scanner Node (distributed scanning)	✔	✔				✔		✔	✔	✔	✔				
Custom Policies	✔	✔	✔			✔		✔	✔	✔	✔				
Internal scanning	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔				✔
External Scanning	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔		✔
Pre-defined Report templates	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔		✔
Custom Reporting	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔				✔
Conmpliance Report templates	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔		✔
Scan Engine-only												✔		✔	
Hardware appliance														✔	✔
Cloud hosted offering						✔			✔	✔	✔	✔	✔		

Install Topologies

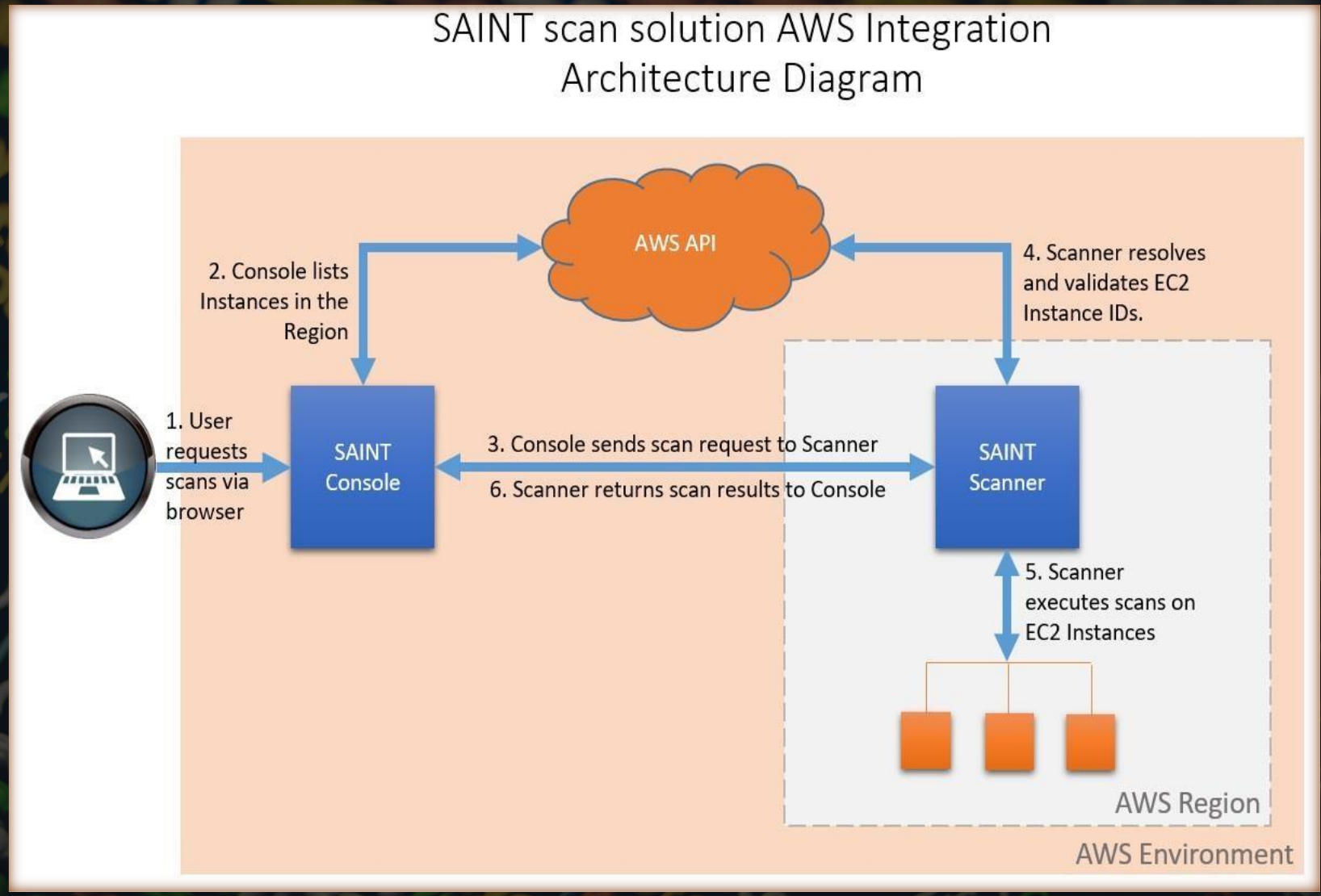


AWS - Three AMI Offerings

I. SAINT (BYOL) AMI - This AMI provides the fully integrated capabilities of SAINT Security Suite.

II. SAINT Pre-authorized AMI - This offering provides users with a vulnerability scanning engine that has been pre-approved by the AWS architecture team to scan into the EC2 instance.

III. SAINT (With License) AMI - Like the SAINT (BYOL) AMI, this AMI provides preconfigured license to support on-demand scanning, with use automatically applied to customer's AWS account.



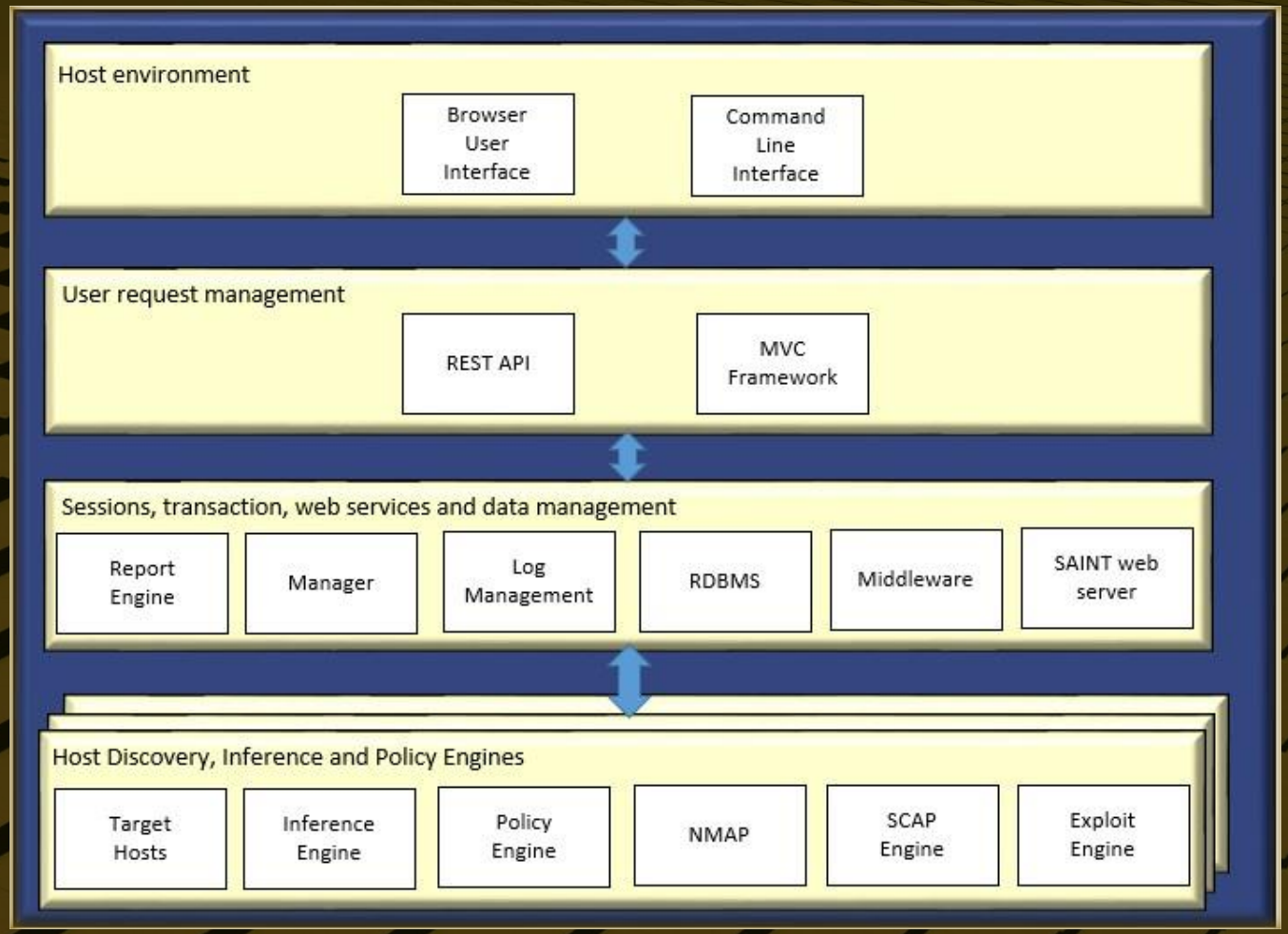
SAINT Architecture

Application is delivered via a desktop browser interface or Command-Line Interface.

Host requests and application handling are executed from the REST API - delivery is executed through Model, View, Controller framework.

Middleware functions perform transaction handling and session management.

Scan engines execute host discovery, manage policies, deliver scan probes, perform data acquisition, and perform fact and vulnerability correlation.

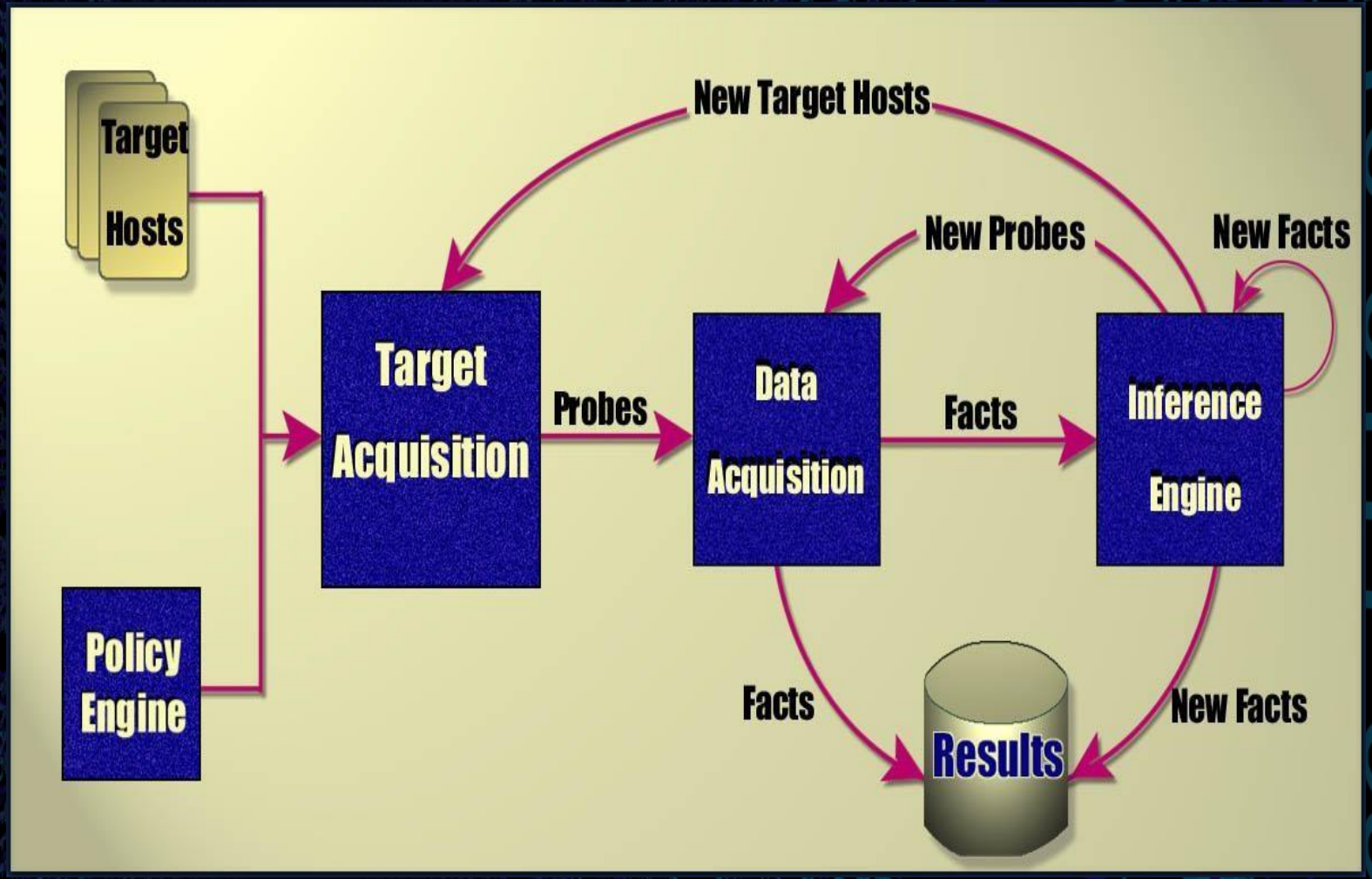


Scan Engine Architecture

The target hosts specified in the scan job together with the policy engine set the parameters for the target acquisition component to discover the targets to scan.

This results in the execution of probes and data acquisition.

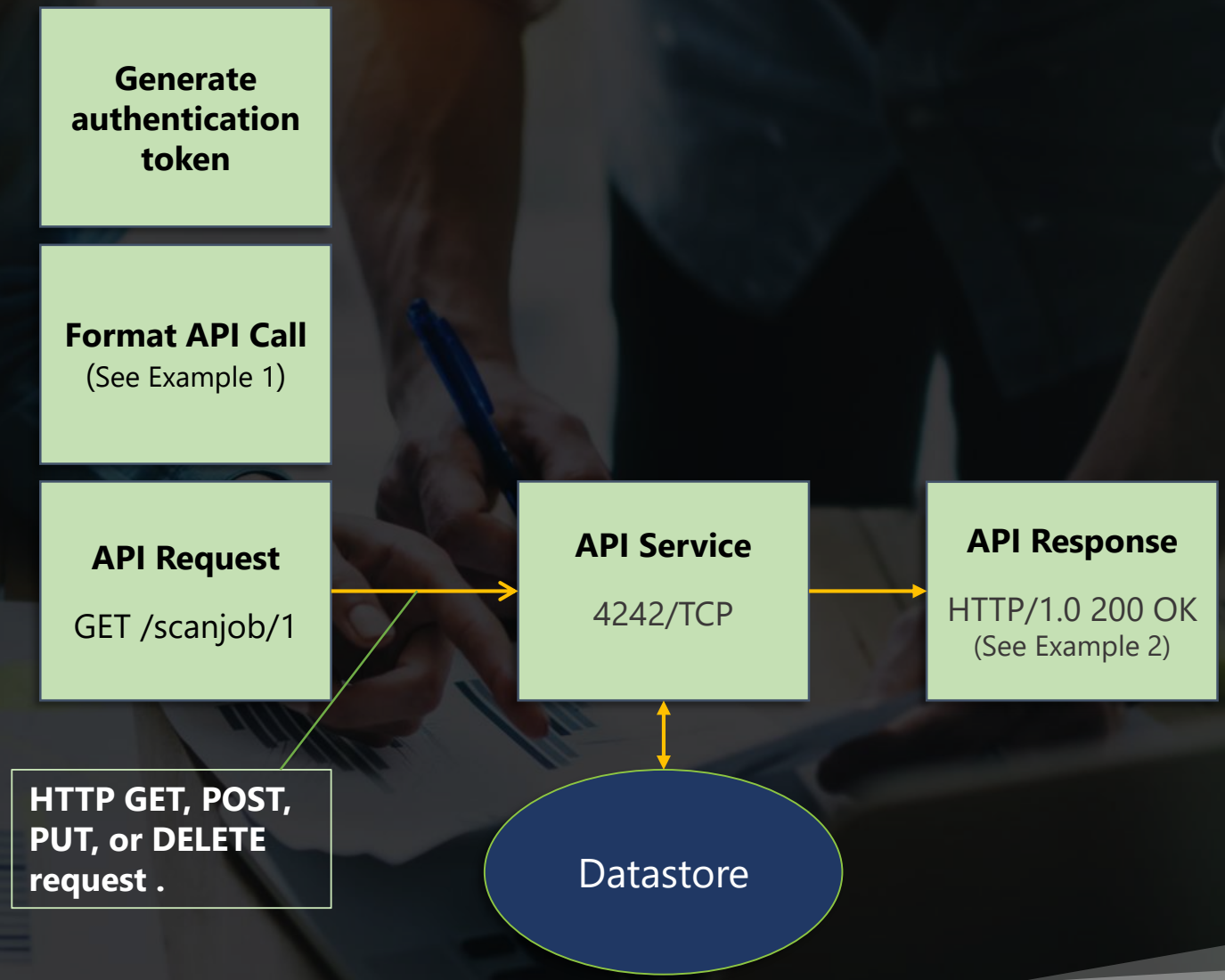
The resulting facts are stored, in addition to being used by the inference engine to discover additional hosts, schedule additional probes, and infer additional facts.



Interfacing With SAINT API

The SAINT API is designed for maximum flexibility and depth of operation.

This well-defined interface allows the customer to wrap SAINT capabilities into virtually any environment and perform all of the essential functions required for a robust vulnerability management program.



How We're Different

Services | Full-Stack Tech | Standards | Knowledge | Experience

PRODUCE COMPLETE RESULTS THAT

- Show
- Guide
- Solve

YOUR ORGANIZATIONAL RISK

Thank You









CARSON&SAINT

carson-saint.com

sales@carsoninc.com

301.656.0521