HARVARD UNIVERSITY

Enterprise Architecture
Harvard University Information Technology
Security Operations

HUIT Standard

Security Minimal Viable Product Requirements for HUIT Hosted/Managed Server Instances

Authors: • Sevier, Raoul	**Audience Level:** • IT Director / Manager • Solution Architect and Project Manager • Application Developer and Designer • DevOps Staff
Version: 1.2 **Last Revised:** 4/15/2020 2:11:00 PM **Status:** Published **Document Type:** Single Topic Standard	**Distribution Scope:** • HUIT
Workgroup Members: Bombalicki, Mark; Burson, Jefferson; DeSilva, Indika; Drief, Malik ; Fanton, Joel; Hall, Nathan; Hoffman, Harry; LaPorte, David; Larsen, Tamara; Mazer, Matthew; Moran, Keith; Vaverchak, Tim	**Reviewers:** • Burson, Jefferson – EA • Larsen, Tamara- DevOps • Moran, Keith – S-MVP Team • Vaverchak, Tim – Shared Services

Document Change Log

Date	Editor	Changes
28-Jan-2020	Raoul Sevier	Initial Draft
5-Feb-2020	Raoul Sevier	RFC edition closing EOD on 2/24
24-Feb-2020	Raoul Sevier	Content discussions, HUIT and NIST compliance table
27-Feb-2020	Raoul Sevier	Content updates to compliance table; HUIT/TPS alignment
16-Mar-2020	Raoul Sevier	Content updates from review meetings and SMEs
23-Mar-2020	Raoul Sevier	Incorporated second round RFC comments; published v1.0
15-Apr-2020	Raoul Sevier	Incorporated Monitoring Services and published v1.2

1. Problem Statement

We live in a world where IT resources such as server instances are aggressively targeted by individuals, organizations, and national actors. This results in passive damage such as exfiltration of intellectual property, or active damage such as data ransoming or destruction.

2. Requirement

Harvard's HUIT organization has made a deliberate effort to align with recommendations from multiple organizations such as NIST, OWASP, SANS, and other universities. As a result, HUIT believes there are six characteristics of a well-managed server environment, which taken together represent the minimum standard for HUIT server security:

Compliance Objectives	**Software Function**	**Standard Product**
Server inventories are comprehensive	Inventory Collection	CloudAware
Intrusions are detected	Endpoint Detection and Response	CrowdStrike – Falcon Host
Known viruses for Windows detected and blocked	Windows Anti-Virus	Broadcom Symantec AV
Activities are tracked	Logging	Splunk
Vulnerabilities are assessed	Vulnerability Scanning	Nessus - Tenable
Health is Checked	Monitoring	LogicMonitor with SNMP
Configuration management is automated	Manage Configurations Automatically	Ansible for Linux or SCCM for Windows

Table 1 – Security Capabilities and Products

HUIT is committed to managing IT resources, on behalf of its customers, in a secure way. These standards are intended to provide simple guidance and effective server security. The discussions that follow will elaborate on the current standard definitions, future roadmap activities, and any known concerns about implementation.

Key Recommendations:

- All Harvard server instances MUST deploy CrowdStrike to detect intrusions.
- All HUIT-hosted/managed server instances MUST conform to the Server Security specifications in this document.
- Other Harvard organizations SHOULD follow HUIT's lead by conforming to at least some of these specifications.

3. Compliance

HUIT requires that all HUIT-hosted/managed server instances conform to these specifications beginning July, 2020. The scope of this standard extends to all server instances that are within the HUIT domains on a fully-managed basis, or are hosted within HUIT on behalf of customers that administer the server instances. The overarching goal of this work is to satisfy Harvard's HUIT Information Security Policy Objectives and NIST Cyber-Security Framework (CSF) Objectives.

Security Component	Security Product	HUIT Information Security Policy Objective	NIST Cyber-Security Framework (CSF) Objective
Inventory Collection	CloudAware	SA1	ID.AM
Endpoint Detection and Response	CrowdStrike	SC3, SA10	DE.AE, DE.CM
Windows Anti-Virus	Symantec AV	SC3, SA10	PR.PT
Logging	Splunk	SB7, SB8, SC6	PR.PT, DE.AE, DE-CM
Vulnerability Scanning	Nessus	SA9, SA10, SC3	DE.CM
Monitoring	LogicMonitor		
Manage Configurations Automatically	Ansible Tower with SSH or SCCM	SA9, SB7, SB8, SC3, SC6	PR.MA

Table 2 – Security components with HUIT and NIST Compliance

IT environments undergo continuous change. As a practical matter, it is important to manage those changes with as much automation as possible to maximize both effectiveness and efficiency of IT operations. This means updating the standards as the mix of resources change. Just as important as knowing what minimum security resources are needed, is a sense of where exceptions are important, and an inventory of waivers to the standards with the reasons the waivers were given.

3.1. Updates to these Standards

TPS and InfoSec management will update the standards when and as required. They will assign this task to the appropriate resources for editing. Should the scope of change be large enough, an additional round of peer and management review may be required. This material and updates will be cross-published on TPS sites and the InfoSec sites.

3.2. Waivers from these Standards

There may be some circumstances where standards have not yet been defined for a class of security requirement. Under these circumstances an exception can be allowed, as long as there is TPS and InfoSec management concurrence. This becomes the basis for updating the standards document, as well as allowing work to keep moving forward. A log of exceptions must be kept.

3.3. Exceptions to these Standards

In the event there is an applicable standard for a particular security issue, but there are compelling reasons to deviate from them, waivers may be granted. Under these circumstances, TPS and InfoSec management must grant the waiver in writing. A log of waivers must be kept.

4. Discussion

Implementation of measures to better manage server security sometimes requires deployment of code ('Agents') inside the server, sometimes services outside the server, but most often both. This general model illustrates these relationships.

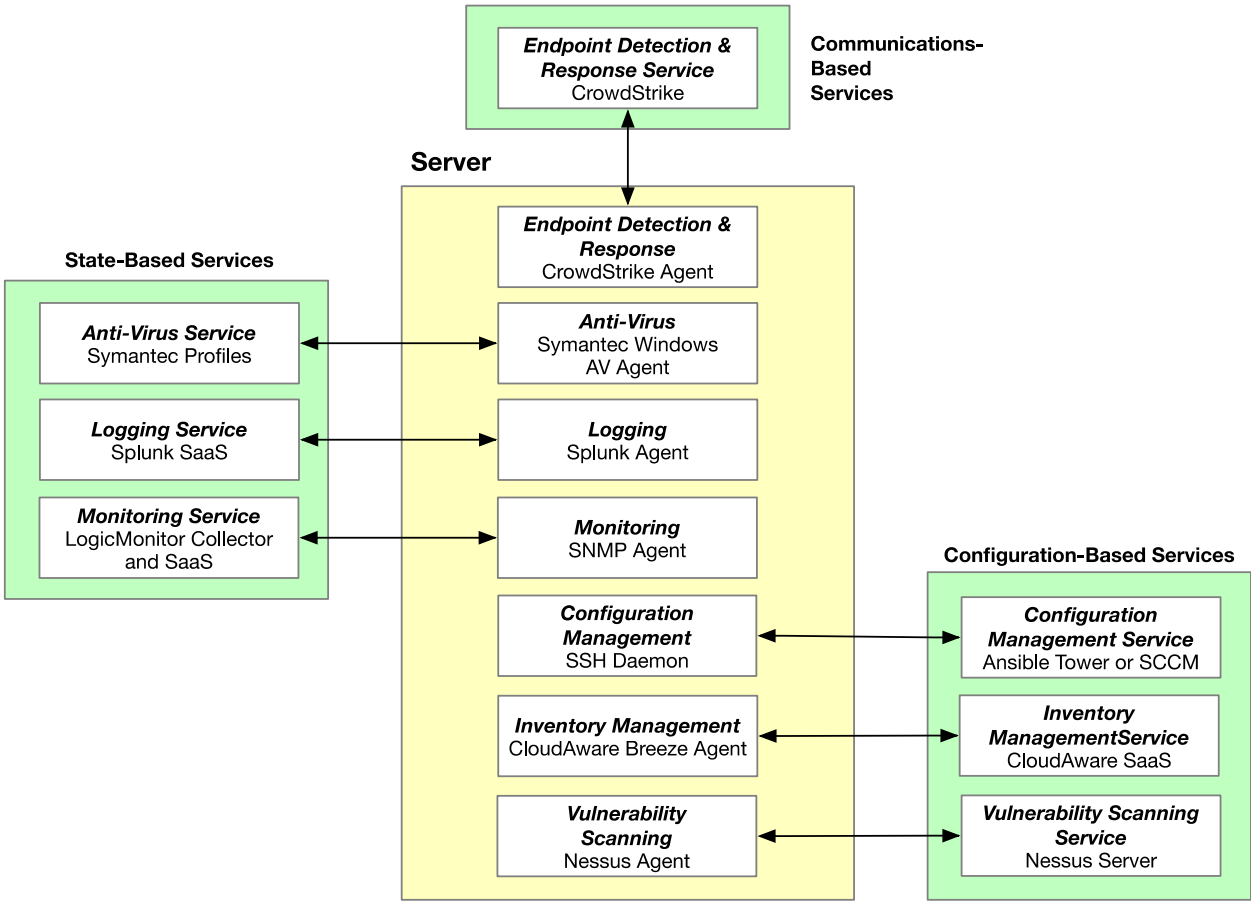


Figure 1 – General Model of Minimum Server Security Requirements

4.1. The role of Agents and Services

Security capabilities, such as vulnerability scanning and anti-virus, are generally implemented using two components. Services organize the capability for many server instances in an organization and collect the outcomes for consolidated assessment by administrators. Agents are deployed on a per-server basis which generally do the finite work of the security capability. For example, Symantic's Anti-Virus Agent, in its position within a server and assigned appropriate privileges, determines the existence of viruses. The agent then sends the results to the AV Service which reports its findings to the administrators, with additional notifications if virus risks are found.

With the complexity of modern server environments, regardless of whether deployed on-premise, in clouds, or in containers, no one server security service is able to all the risks. HUIT has determined that seven services are needed to provide adequate protection for most server instances. Additional security services could be needed for exceptional cases in server instances where very sensitive data is managed, or financial transactions occur.

HUIT has deployed and operates these services on behalf of its customers' server instances as well as its own. Schools and other organizations that intend to secure their own server instances to the same standards will need to deploy their own security services and agents, or collaborate with HUIT to ensure their server instances are protected.

4.2. Take Inventory - Inventory Collection Services

In the context of server instances, Inventory collection has two aspects: Inventory of server instances, and inventory of the contents of each server. Essential to protection the computing environment as a whole is a comprehensive list of active server instances. This ensures that there are no unaccounted server instances that could act as an entry point for bad actors. Additionally, within each server it is essential to know what server-based capabilities are active in order to ensure they are properly configured and versioned to avoid vulnerabilities.

Current State

HUIT currently uses CloudAware to gather inventory information which is then stored in the ServiceNow CMDB. CloudAware is deployed as a SaaS vendor-managed capability. Secure communications allow CloudAware to query registered server instances for their internal capabilities and configurations.
More information at: https://www.cloudaware.com

Future State Roadmap

Inventory discovery is limited to cloud-based assets at this time. In the future we will add an on-premise based inventory discovery capability as well. There are no current plans to move beyond CloudAware as the inventory collection service provider.

Known Concerns

HUIT is continuing to identify server instances that are part of the total HUIT-hosted/managed server portfolio, and ensuring the CloudAware agent is deployed within them.

4.3. Detect Intrusions – Endpoint Detection and Response (EDR) Services

Endpoint Detection and Response (EDR) continuously records system activities and events taking place on endpoints to provide security teams with the visibility needed to uncover incidents that would otherwise remain undetected. Continuous monitoring and analysis of server activity allows Harvard to more rapidly detect and even prevent malicious activity. The remote collection of system activity logs enables improved post-incident forensics.

Current State

Harvard's University CIO has set CrowdStrike as the standard for all servers belonging to all schools and internal organizations, including HUIT. CrowdStrike provides assessment of activity on servers, immediate notification of detected anomalies, and historical information that aids forensic analysis of attacks on servers.
More information at: https://www.crowdstrike.com

Future State Roadmap

There are no current plans to move beyond CrowdStrike as the Endpoint Detection and Response Services provider.

Known Concerns

After installation the agent must be able to communicate with CrowdStrike's servers to function. Servers that access the internet through proxies, firewalls, and/or NATs must be configured to allow this access.

4.4. Prevent Corruption – Anti-Virus Services

Anti-virus software scans for, detects, and blocks/removes known malicious software. This activity happens in real-time and does not require a connection to another server or service to function (a key difference from EDR). Malware detection (ie. anti-virus) is required by Harvard University's Information Security Policy as well as many compliance regimes (e.g. 201 CMR 17).

Current State

HUIT currently uses Symantec AV fulfil this role. It uses the traditional approach of scanning a server for matches against an inventory of known viruses.
More information at: https://www.symantec.com/products/atp-content-malware-analysis

Future State Roadmap

The state-of-the-art in this area is enabling two additional approaches to managing server corruption.

The first borrows learning from the PCI – Credit Card industry which has required that the contents of a server 'as a whole' be measured and then regularly tested. This avoids the repetitive scanning and managing a current virus inventory, but eliminates the flexibility of making incremental changes of any kind to a server.

The second approach is 'Application Whitelisting' which allows only approved and trusted files, applications, and processes to be installed and run on a server. TPS is actively considering using CarbonBlack in 'high-enforcement mode' to perform Application Whitelisting.

The feasibility of these approaches is improved dramatically when combined with automated configuration management, which allows a server to be built from the ground-up according to a script. This ensures a 'known-good' baseline definition of a server which supports server-level state change measurements, and finite lists of whitelisted applications and processes.

Known Concerns

Pre-requisite to deploying CarbonBlack's application whitelisting capability, is the need to re-engineer the design of server application architectures, and to increase the use of automated configuration management. This will limit the rate at which these new techniques can be deployed.

4.5. Track Activities - Logging Services

The usual means of tracking activities on a server is to keep a log of the activities. The reality is more complex, in that there are many components on a server that individually keep logs, resulting in fragmentation of activity tracking by both type and by time. Logging Services provide a means of centralizing the individual logs kept by server components and applications, and delivering this data to a centralized service where it can be assessed and stored for forensic purposes.

Current State

HUIT currently uses Splunk as the central service for log aggregation and assessment. This service provides administrators the means to search logs in many ways in order to find expected and unexpected events during server operations.
More information at: https://www.splunk.com

Future State Roadmap

There are no current plans to move beyond Splunk as the Logging Services provider.

Known Concerns

Data generated by individual server component logging activity is voluminous. When all component logs are combined, it is more voluminous. When logs across all HUIT servers is combined it is greatly voluminous. HUIT is currently assessing strategies for managing the volume of data without losing visibility for analysis and forensic needs, and assessing different cost models to manage budgetary impact.

4.6. Assess Vulnerabilities – Vulnerability Scanning Services

Server capabilities that are exposed beyond the bounds of a server represent entry points ('vectors') for attack by bad actors. Many of these vectors are well understood and protected by the design of the exposed capability. Historically some of these vectors accessed poorly designed capabilities which were routinely exploited by bad actors to insert viruses and other malware into server instances. Other vectors used general-purpose capabilities such as HTTP on port 80 to reach insufficiently protected web sites that were vulnerable to attacks such as SQL Injection, Cross-site Scripting, or Man-in-the-Middle. Vulnerability Scanning Services represents a proactive approach to security by testing a server for known vulnerabilities drawn from a library of exploits that is kept up-to-date.

Current State

HUIT currently uses Nessus to perform automated, proactive vulnerability testing of server instances. Nessus provides the ability to test a server for vulnerabilities that allow unauthorized control or access to sensitive data, identify misconfigurations, and other situations that jeopardize the security of a server.
More information at: https://www.tenable.com/products/nessus/nessus-professional

Future State Roadmap

There are no current plans to move beyond Nessus as the Vulnerability Scanning Services provider.

Known Concerns

There are many tools that proactively test server instances for vulnerabilities, in different ways. In addition to automated vulnerability scanning by tools such as Nessus, penetration testing tools such as Metasploit are exhaustive, live examinations for exploits in a server. This kind of testing is typically done at time of an initial application deployment.

4.7. Check Health – Monitoring Services

While some security services assess how internal components are configured (CloudAware), or track the activities of those components (Splunk), Monitoring services measure the operational pulse of the

components. This includes seeing if the component is active, and the health of the processes that operate the component as measured by CPU usage, memory usage, network bandwidth consumption, and disk activity.

Current State

TPS currently uses LogicMonitor in conjunction with locally deployed Collectors and SNMP daemons on servers to perform automated determinations of the state of server components. SNMP is an industry-wide standard service that provides state information, and is routinely deployed in servers as part of the operating system. This pair of tools provide routine, automated state information about the server as a whole, as well as individual components.

Future State Roadmap

There are no current plans to move beyond LogicMonitor as the Monitoring Services provider.

Known Concerns

LogicMonitor was recently selected by TPS as the standard tool for server monitoring, and is undergoing a deployment roll-out.

4.8. Manage Configurations Automatically – Configuration Management Services

Software provisioning and configuration tools uses scripts to create a fully-functional server instances, including all components that are needed at the correct version levels. They can configure both Linux and Windows server instances. The principle of use is that manual crafting of components and configurations is no longer needed. Rather, since a server can be rebuilt automatically, all server instances are created and deployed by the tool. Note that this includes all the server security capabilities discussed in this advisory.

Current State

HUIT currently uses Ansible Tower communicating with Linux-server-based Secure Shell (SSH) daemons to provide server software provisioning and configuration services. This enables the automated deployment of server instances, and also enables their re-deployment when patches and version changes are required. For Windows-based server instances, SCCM provides similar capabilities.

Future State Roadmap

There are no current plans to move beyond Ansible Tower as the Configuration Management Services provider for Linux-based server instances, and SCCM for Windows-based server instances.

Known Concerns

Creation of the configuration scripts is an additional step in the software development life-cycle that not all project teams have undertaken, as yet.

5. Other Considerations

In addition to identifying, deploying, and operating the individual tools identified in this advisory, HUIT recognizes that additional work is required to unify and optimize the use of the tools as a security

platform, and to change the culture of individual software development teams to align with the larger vision.

5.1. Security Groups in AWS Cloud

Harvard and HUIT make extensive use of Amazon's AWS cloud services. HUIT's initial deployments made use of Local Security Groups in server instances. With the upgrade of the cloud security model to Harvard CloudShield 2, emphasis has shifted from Local Security Groups to Global Security Groups.

Current State

HUIT's initial deployments made use of Local Security Groups in server instances.

Future State Roadmap

With the upgrade of the cloud security model to Harvard CloudShield 2, emphasis has shifted from Local Security Groups to Global Security Groups.

Known Concerns

Since Local Security Groups supersede Global Group rules, manual reconfiguration of deployed server instances is needed to align to the Global Groups pattern.

5.2. Reporting Across the Toolchain

In envisioning a secure server platform that has a minimum set of security services, it becomes clear that there are on-going operations and administration requirements that should be optimized.

Current State

Each security tool service that is currently deployed includes its own 'dashboard' or reporting capability, in addition to notification capabilities.

Future State Roadmap

An ideal vision includes the consolidation of at-a-glance dashboards into one pane of glass, consolidated reports across the security platform tools, and fully integrated notification capabilities with appropriate escalations and timers.

Known Concerns

Currently lack of standards and alignment across the vendor communities make this vision difficult to realize.

5.3. Adoption and Compliance

Maximum benefit will be realized once all these tools are deployed across all supported server instances, with mature operational and administrative processes supporting the continuous changes to the larger computing environment.

Current State

Today HUIT is in the process of deploying these tools, but adoption is uneven. Appendix A contains an example of an adoption report. Agent rollout is handled by SCCM (Windows configuration management tool), and Ansible Tower (Linux Configuration management tool) based on operating system. Each agent will require access to the internet, and its

corresponding management system. Each Agent is available in the Common Asset repository and Information Security maintains versions. Adoption requirements include:

- Crowdstrike: Configuration is bundled with playbook/package – Case sensitivity important.
- CloudAware: Configuration is bundled with playbook/package – Internet access required
- Nessus: Configuration is bundled with playbook/package –
- Splunk: Configuration is bundled with playbook/package – deployment server applies base configuration. Additional logging requires revisiting.
- Symantec: Configuration is bundled with package – managed by Sep Management server post rollout

Future State Roadmap

Starting July, 2020, HUIT will treat these requirements as a mandatory standard for all HUIT hosted/managed server instances.

Known Concerns

This vision is a culture shift in the way server instances are designed, provisioned, deployed, and updated. Developers, operations, and administrators will all need to adjust and align to this model.

5.4. Communications and Education

Adoption and compliance to this server security platform vision will rely on the understanding and support of developers, operations teams, administrators, and management.

Current State

This advisory represents an initial attempt to communicate and educate the comprehensive vision of the new Minimum Security Requirements for HUIT-hosted/managed Server instances.

Future State Roadmap

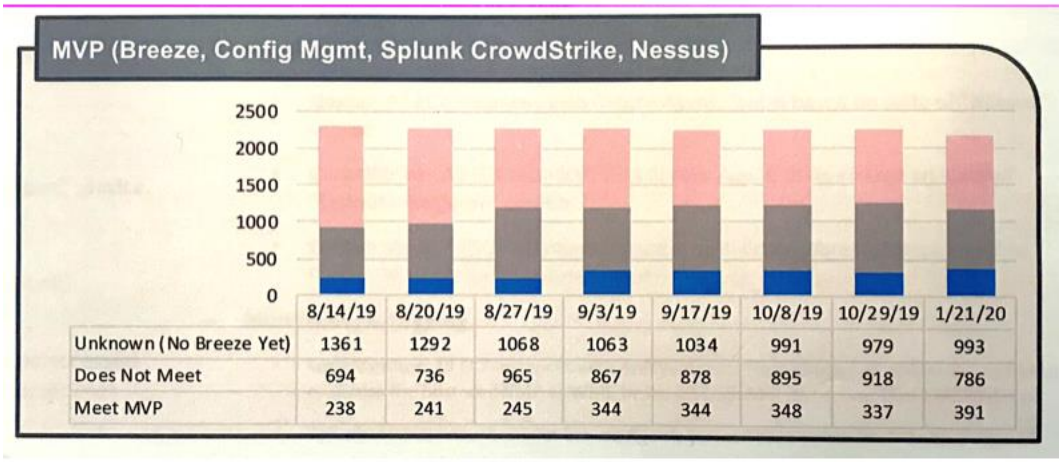
It is envisioned that 1) deeper documentation will be developed to document the design of each component of the server security framework, 2) broader documentation will be developed to document the baseline that application teams must incorporate into their designs, and 3) educational materials will be developed that can be used in venues such as IT Academy and on-line courses to transfer the requisite knowledge to those that need it.

Known Concerns

This vision calls for actions that require interim staffing and funding.

6. Appendix A – Adoption of the Standard Server Security Configuration:

This chart indicates the degree of adoption for HUIT- hosted server instances up to January 2020.



	8/14/19	8/20/19	8/27/19	9/3/19	9/17/19	10/8/19	10/29/19	1/21/20
Unknown (No Breeze Yet)	1361	1292	1068	1063	1034	991	979	993
Does Not Meet	694	736	965	867	878	895	918	786
Meet MVP	238	241	245	344	344	348	337	391

7. References

- Server Protection/Security MVP - Confluence Wiki - https://wiki.harvard.edu/confluence/pages/viewpage.action?pageId=239735382
- Harvard Security Policy website https://policy.security.harvard.edu
- Harvard Security Policy website – Working with Servers https://policy.security.harvard.edu/all-servers
- NIST Special Publication 800-123 - Guide to General Server Security - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf
- Other .edu server security references:
    - Buffalo - Server Security and Hardening Standards - http://www.buffalo.edu/ubit/policies/guidance-documents/server-security-and-hardening/appendix-b.html
    - Colorado - IT Security - Policy & Minimum Security Standards - https://oit.colorado.edu/it-security/policy-minimum-security-standards
    - Northwestern - Server Security Requirements and References - https://www.it.northwestern.edu/policies/serversecurity.html
    - Stanford - Minimum Security Standards - https://technology.umw.edu/it-policies/minimum-security-standard-for-servers/
    - UConn - Server Hardening Standard (Windows) - https://security.uconn.edu/server-hardening-standard-windows/
    - UMW - Minimum Security Standard for Servers - https://technology.umw.edu/it-policies/minimum-security-standard-for-servers/
    - Yale - Minimum Security Standards - https://cybersecurity.yale.edu/minimumsecuritystandards