CYBER SECURITY SOLUTION

SAFE | SECURE | CERTIFIED

Product Overview

PSG's Cyber Security Solution (CSS) is critical for addressing the rapidly evolving Cyber threats. Designed with an integrated suite of tools for managing cyber compliance on all DOD and DOE networks. Information Security is a dynamic process and requires a thorough approach using continuous auditing, monitoring, and updates via centralized and automated management toolsets.

The system is designed for high-reliability and minimal downtime applications. Options include full redundancy and regionalized hardware configurations for mission critical applications. Once implemented, the Cyber Security Solution saves time, reduces system down time, and provides continuous monitoring and centralized client updates for any network.
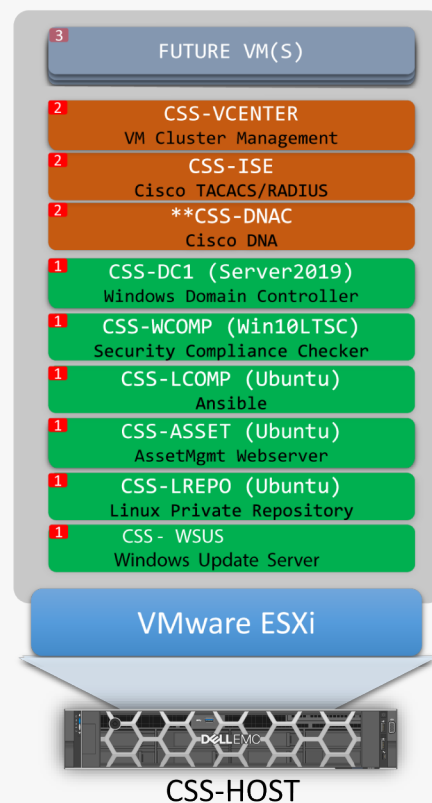
PSG's Cyber Security Solution benefits:

- Continuous auditing, monitoring and updates
- Compatible with any DOD, DOE, and Critical Infrastructure networks
- Reducing downtime through centralized automation and logging
- Saves time and increases productivity by automating the security compliance/STIG auditing process; Including vulnerability items that are overlooked by standard Security Content Automation Protocol (SCAP) scanning tools. PSG's Cyber Security toolbox is designed to run as Virtual Machines, on COTS or GOTS hardware, designed to meet the stringent DISA STIG security compliance baseline for both DoD and DOE applications.

Features	Benefits
Domain Controller (CSS - DC)	The CSS-DC is responsible for controlling the network by pushing out Group Policy (GP) to all machines; these Group Policies enforce STIG compliance on the domain. This is done for the purposes of Protection and Implementation from the NIST Five Functions Framework as well as NIST RMF. CSS-DC does this by utilizing Group Policy Management and Active Directory.
Asset Management (CSS - ASSET)	The purpose of CSS-ASSET is to track assets and edge devices such as cameras, server boxes, workstations, and monitors.
Windows Compliance (CSS - WCOMP)	The purpose of the CSS-WCOMP is to ensure that all Windows machines on the domain are in compliance with applicable STIG's. This is accomplished by using a DISA certified Security Compliance Checker (SCAP compliance tool) as well as PSG's Cyber Audit tool.
Windows System Update Server (CSS - WSUS)	The purpose of CSS-WSUS is to allow administrators to automate the deployment of windows updates to all windows machines within the domain.
Linux Compliance (CSS - LCOMP)	The purpose of the CSS-LCOMP is to ensure that all Linux machines on the domain are in compliance with the applicable STIG's. This is accomplished by the use of Ansible Playbook toolsets defined by PSG.
Linux Repository (CSS - LREPO)	The purpose of CSS-LREPO is to allow administrators to automate the deployment of Linux updates to all Linux machines within the domain.
Toolset Expansion/Configurable Slots	Allows for the addition of ANY Cyber Security toolset to be applied, including network monitoring via WhatsUp Gold or SolarWinds.

3 FUTURE VM(S)

2 **CSS-VCENTER**
VM Cluster Management

2 **CSS-ISE**
Cisco TACACS/RADIUS

2 ****CSS-DNAC**
Cisco DNA

1 **CSS-DC1 (Server2019)**
Windows Domain Controller

1 **CSS-WCOMP (Win10LTSC)**
Security Compliance Checker

1 **CSS-LCOMP (Ubuntu)**
Ansible

1 **CSS-ASSET (Ubuntu)**
AssetMgmt Webserver

1 **CSS-LREPO (Ubuntu)**
Linux Private Repository

1 **CSS- WSUS**
Windows Update Server

VMware ESXi

CSS-HOST

1. CSS Base Virtual Machine included
2. CSS Guest Virtual Machine (optional or customer provided)
3. Virtual Machine Expansion

Note: Dell servers depicted. HP server option is available

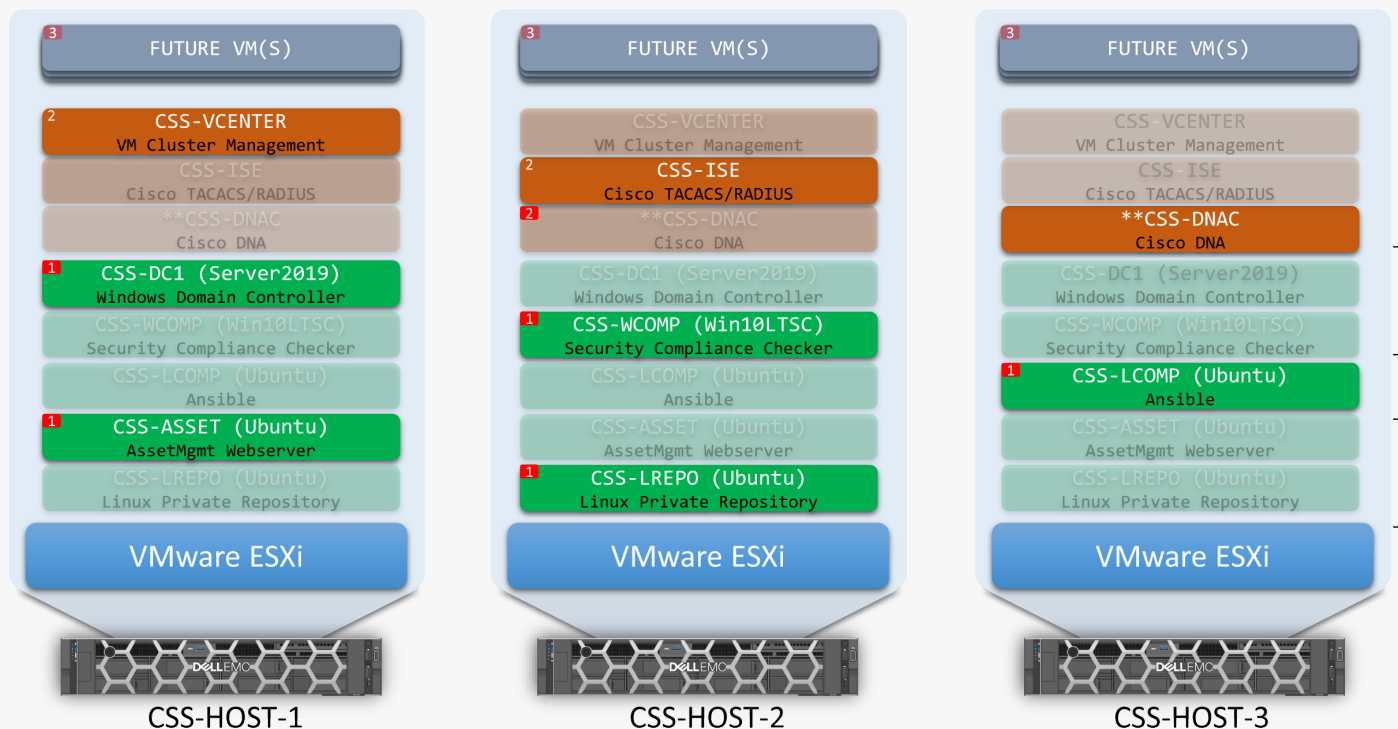CSS-HOST-01
CPU = 16 X 2.10 Ghz
*Mem = 96 GB
**Storage = 8TB

* Base model RAM is 96GB. Expandable to 1536GB
** Base model storage = 8TB Raid10. Expandable

PSG Cyber Security Solution - Cluster Model

FUTURE VM(S)

CSS-VCENTER
VM Cluster Management

CSS-ISE
Cisco TACACS/RADIUS

**CSS-DNAC
Cisco DNA

CSS-DC1 (Server2019)
Windows Domain Controller

CSS-WCOMP (Win10LTSC)
Security Compliance Checker

CSS-LCOMP (Ubuntu)
Ansible

CSS-ASSET (Ubuntu)
AssetMgmt Webserver

CSS-LREPO (Ubuntu)
Linux Private Repository

VMware ESXi

CSS-HOST-1

FUTURE VM(S)

CSS-VCENTER
VM Cluster Management

CSS-ISE
Cisco TACACS/RADIUS

**CSS-DNAC
Cisco DNA

CSS-DC1 (Server2019)
Windows Domain Controller

CSS-WCOMP (Win10LTSC)
Security Compliance Checker

CSS-LCOMP (Ubuntu)
Ansible

CSS-ASSET (Ubuntu)
AssetMgmt Webserver

CSS-LREPO (Ubuntu)
Linux Private Repository

VMware ESXi

CSS-HOST-2

FUTURE VM(S)

CSS-VCENTER
VM Cluster Management

CSS-ISE
Cisco TACACS/RADIUS

****CSS-DNAC**
Cisco DNA

CSS-DC1 (Server2019)
Windows Domain Controller

CSS-WCOMP (Win10LTSC)
Security Compliance Checker

CSS-LCOMP (Ubuntu)
Ansible

CSS-ASSET (Ubuntu)
AssetMgmt Webserver

CSS-LREPO (Ubuntu)
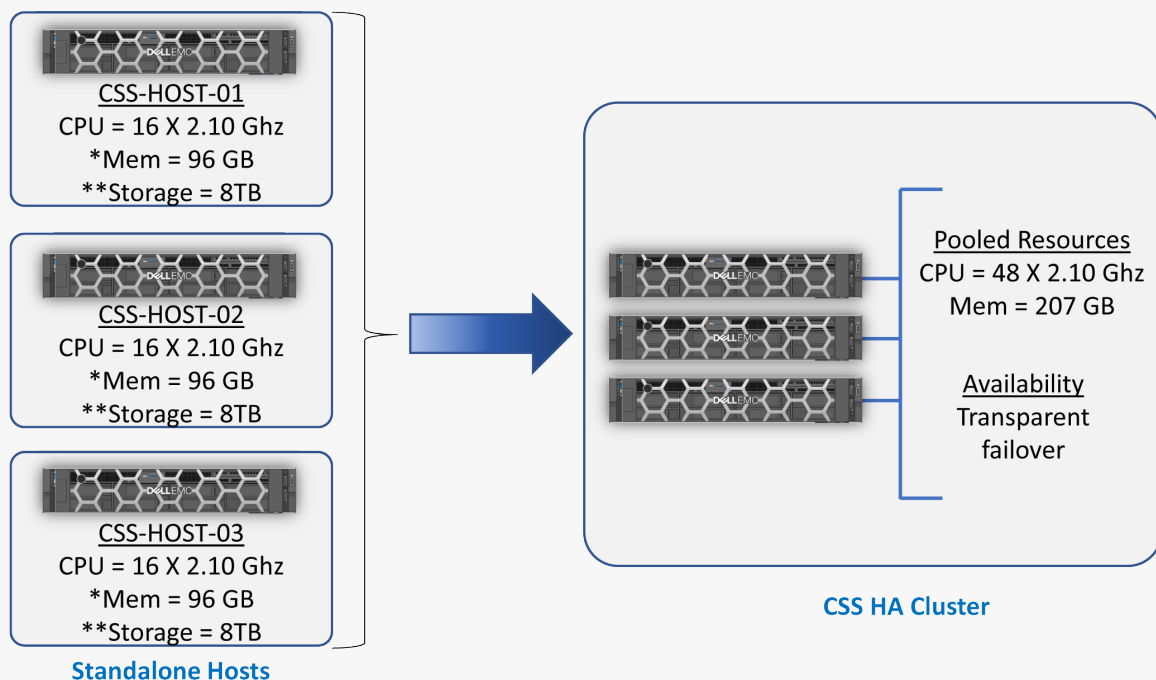Linux Private Repository

VMware ESXi

CSS-HOST-3

---

* Virtual Machines depicted as load balanced. Cluster designed to handle (n-1) host failure.
** If available in Virtual Machine packaged from Cisco
1. CSS Base Virtual Machine included
2. CSS Guest Virtual Machine (optional or customer provided)
3. Virtual Machine Expansion
Note: Dell servers depicted. HP server option is available

PSG Cyber Security Solution - High Availability

CSS-HOST-01
CPU = 16 X 2.10 Ghz
*Mem = 96 GB
**Storage = 8TB

CSS-HOST-02
CPU = 16 X 2.10 Ghz
*Mem = 96 GB
**Storage = 8TB

CSS-HOST-03
CPU = 16 X 2.10 Ghz
*Mem = 96 GB
**Storage = 8TB

Standalone Hosts

Pooled Resources
CPU = 48 X 2.10 Ghz
Mem = 207 GB

Availability
Transparent
failover

CSS HA Cluster

* Base model RAM is 96GB. Expandable to 1536GB
** Base model storage = 8TB Raid10. Expandable