

**Adria Forum 2025**

# Security for Private Cloud with VCF

Mladen Krivokuća

Senior Solution Engineer, MBCOM Technologies, Broadcom Representative

[m.krivokuca@mbcom.com](mailto:m.krivokuca@mbcom.com)



# Security in Cloud Foundation



## Be Secure, Faster

All the capabilities you need to succeed, turned on and ready to use, flexible to meet any workload or environment's needs.



## Inherent Trust

Visibility into, and control of, the entire infrastructure stack is very important. Replace trust with continuous verification.



## Recover Quickly

Resilience has always been the primary feature of VMware infrastructure, whether you face a failed application upgrade or a natural disaster.

# CIA Triad: **Core Tenets** of Information Security



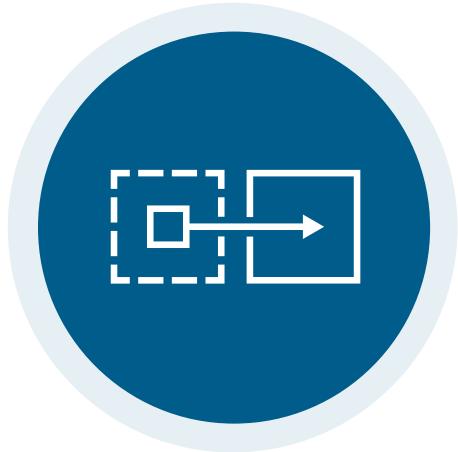
## Confidentiality

Protecting systems & data from unauthorized people & groups



## Integrity

Preventing modification of data by unauthorized groups & systems



## Availability

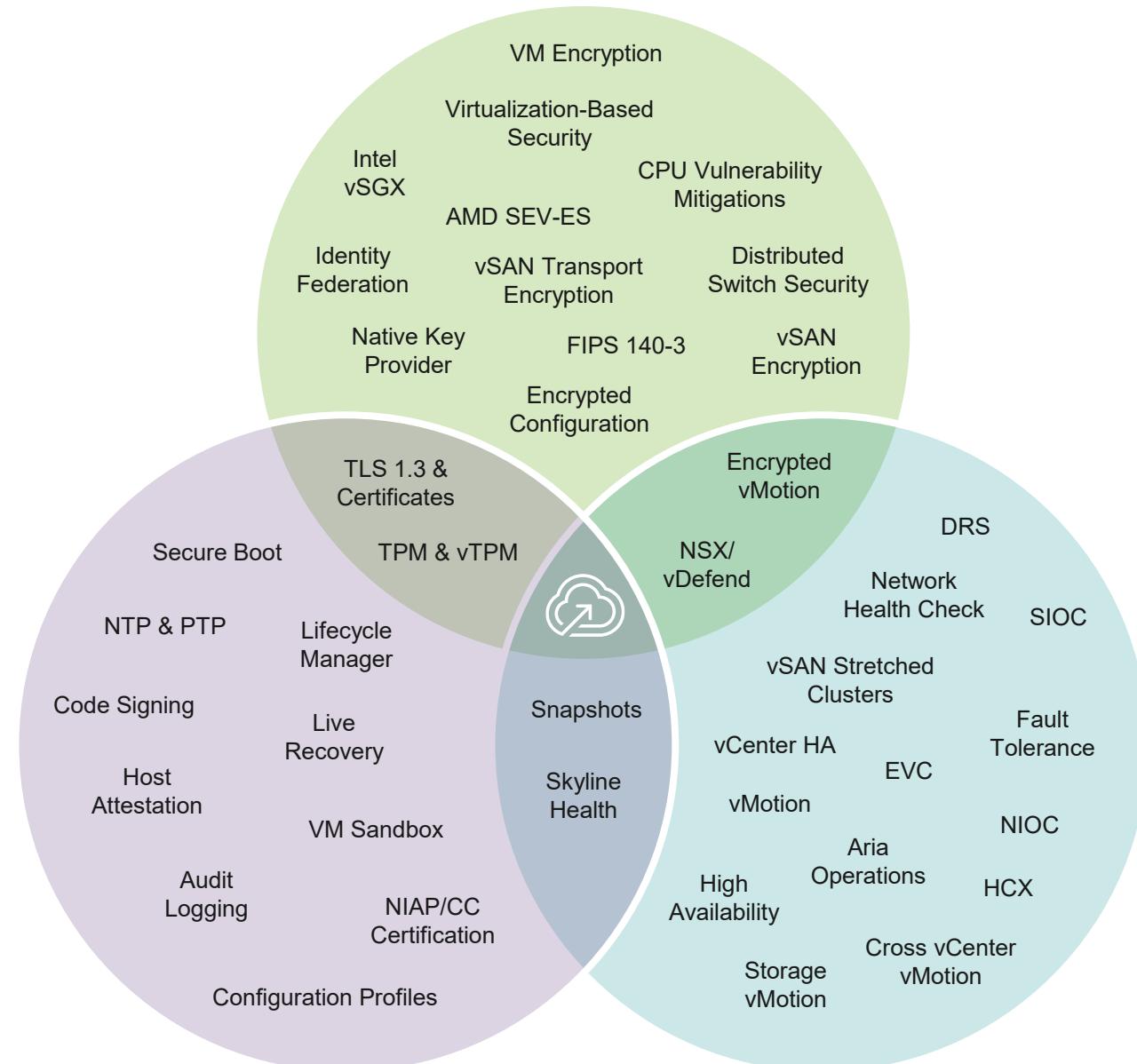
Ensuring that data is available to authorized parties when needed

# Every Feature is a Security Feature

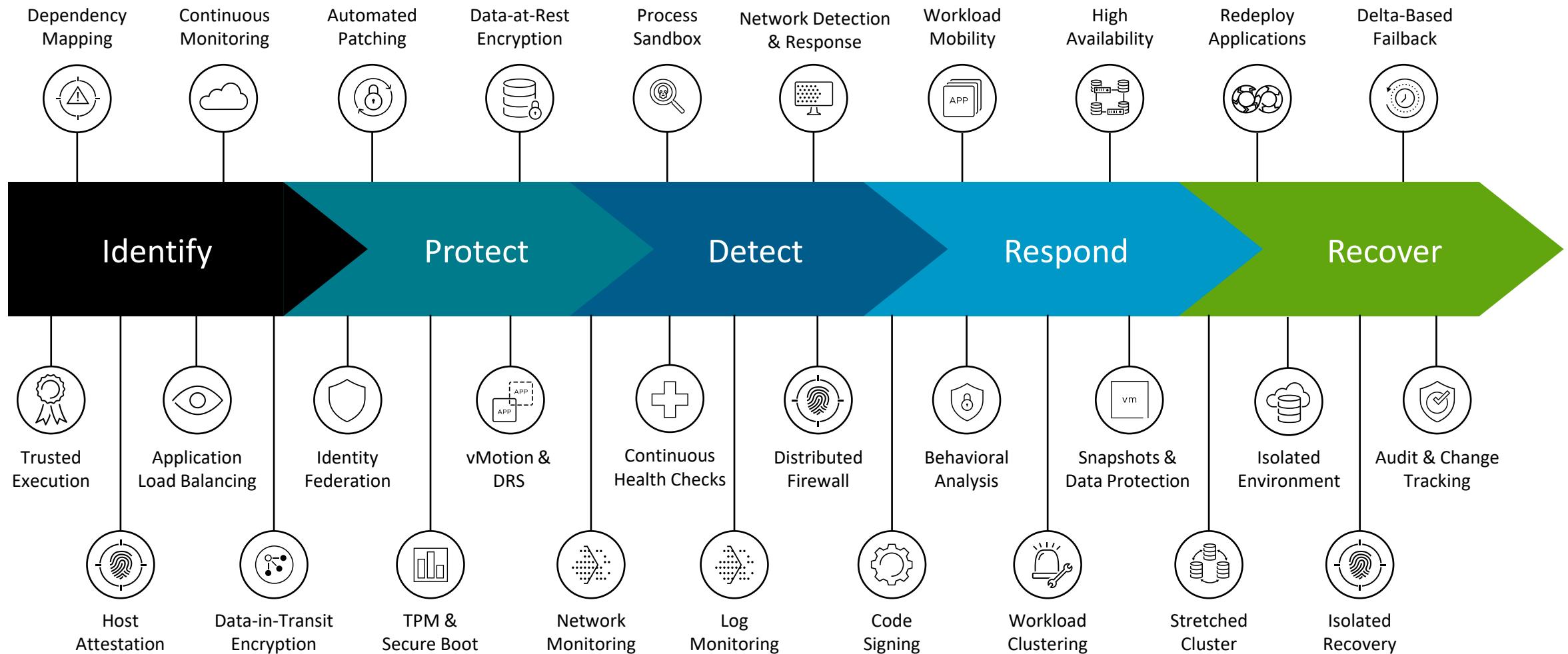
## Integrity

## Confidentiality

## Availability



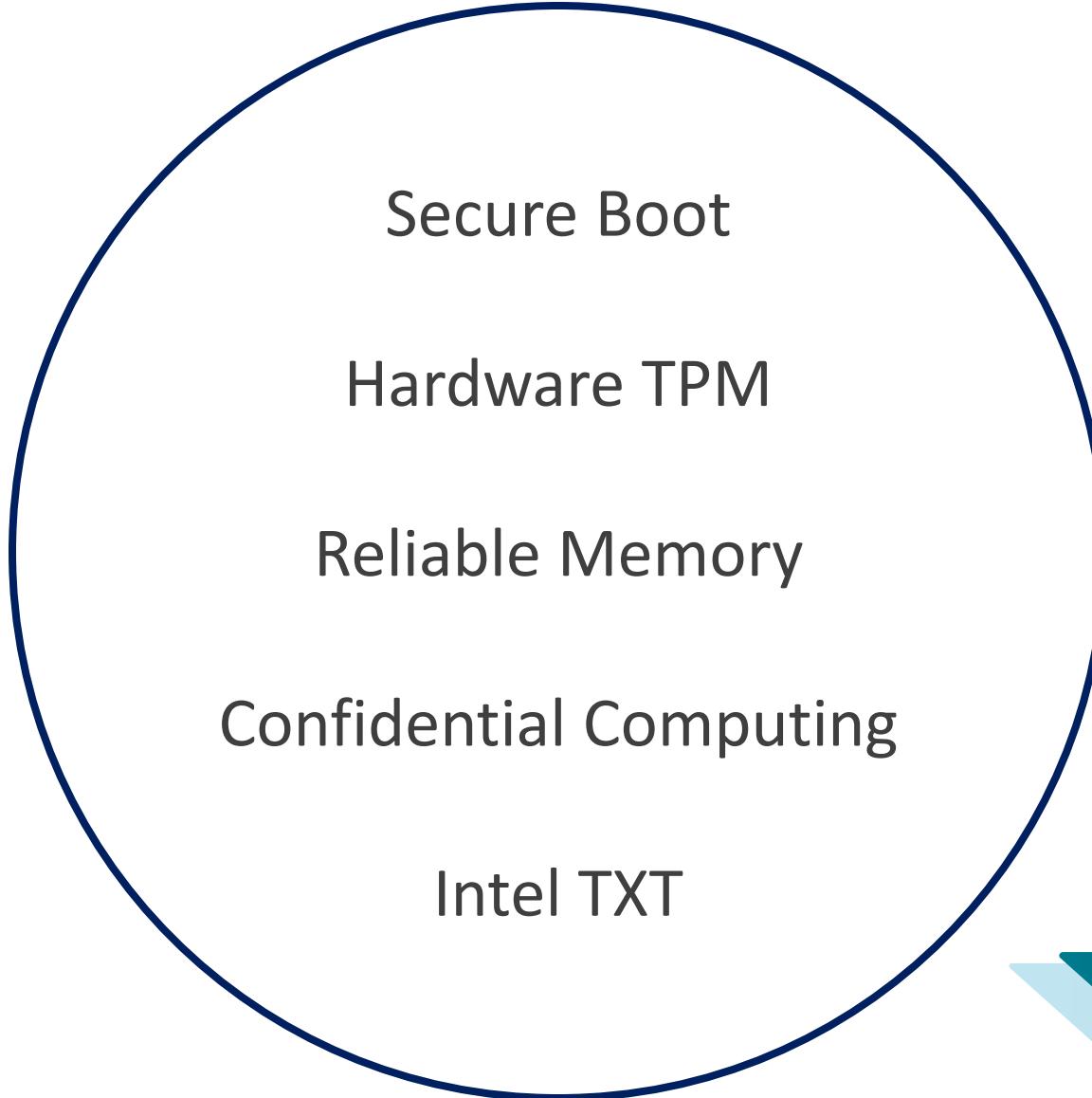
# Resilience Woven Throughout VMware Cloud Foundation



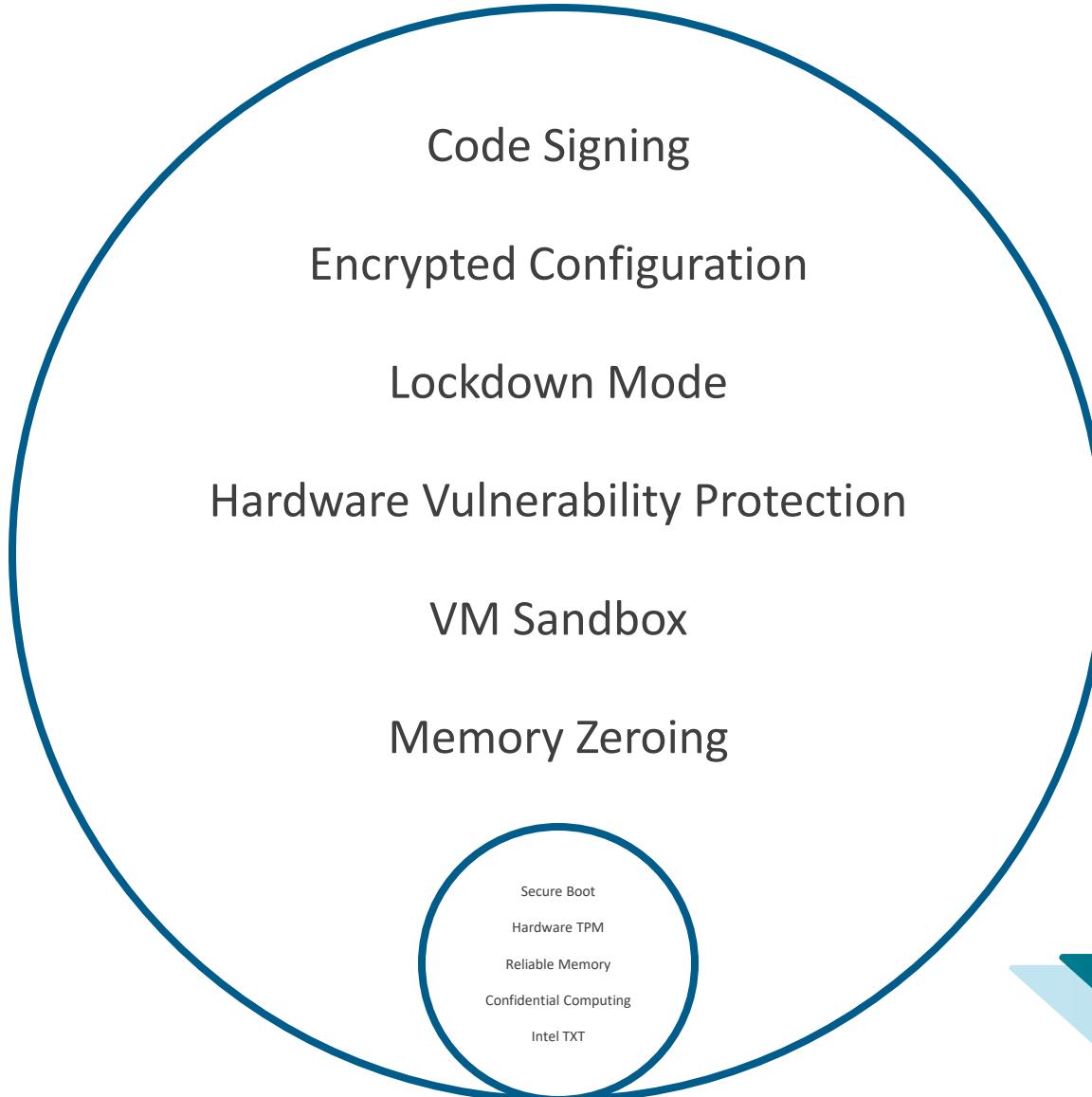
# Layered Defenses

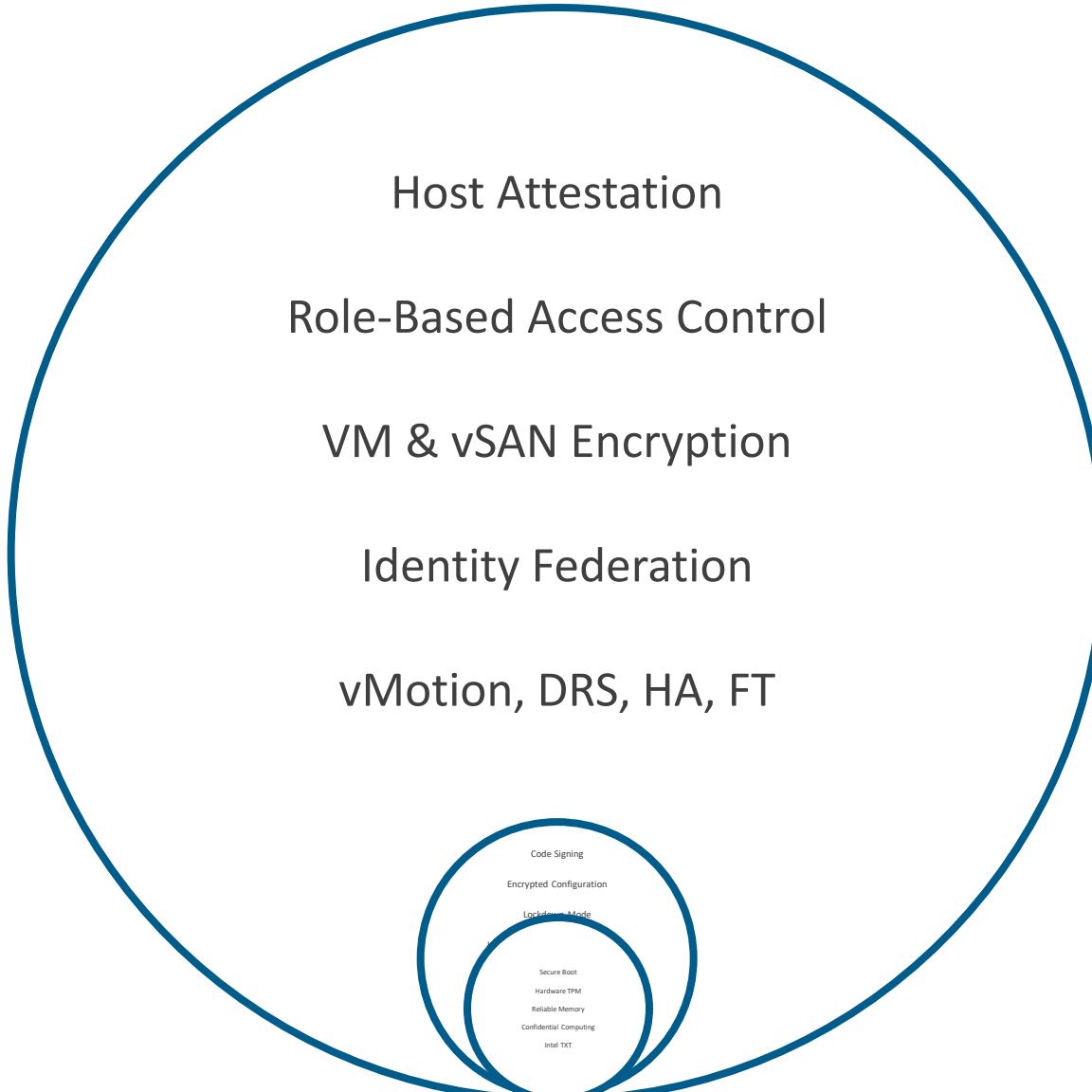
## VMware Cloud Foundation 9.0





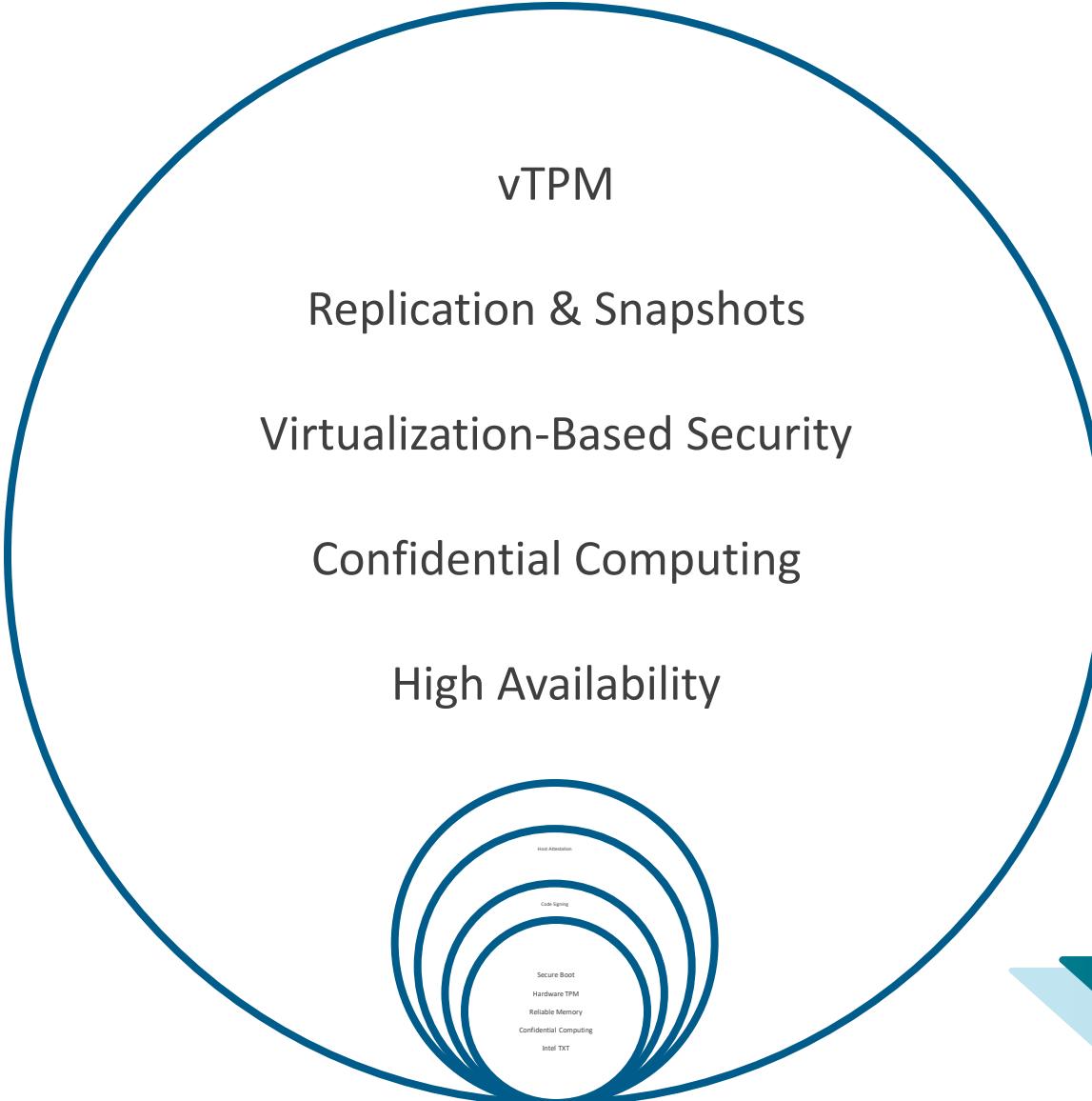
Hardware

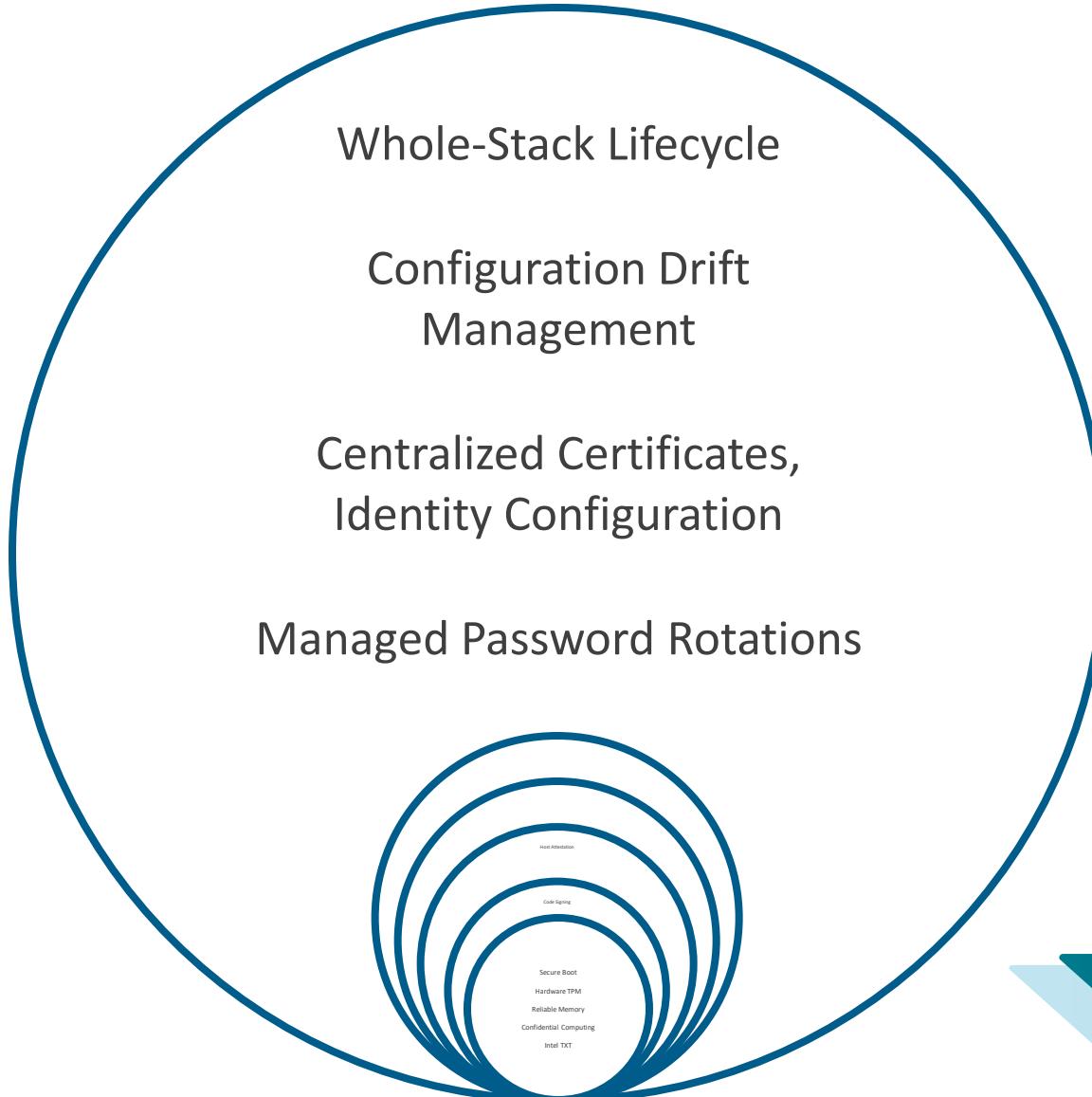




vCenter







Operations



VCF



VMware Cloud  
Foundation® Operations



VMware Cloud  
Foundation® Automation



VMware  
Live Recovery™



VMware  
vDefend™



VMware Cloud Foundation® Operations



VMware Cloud Foundation® Automation



VMware Live Recovery™



VMware vDefend™



VMware Cloud Foundation® Operations



VMware Cloud Foundation® Automation



VMware Live Recovery™



VMware vDefend™



VMware Cloud Foundation® Operations



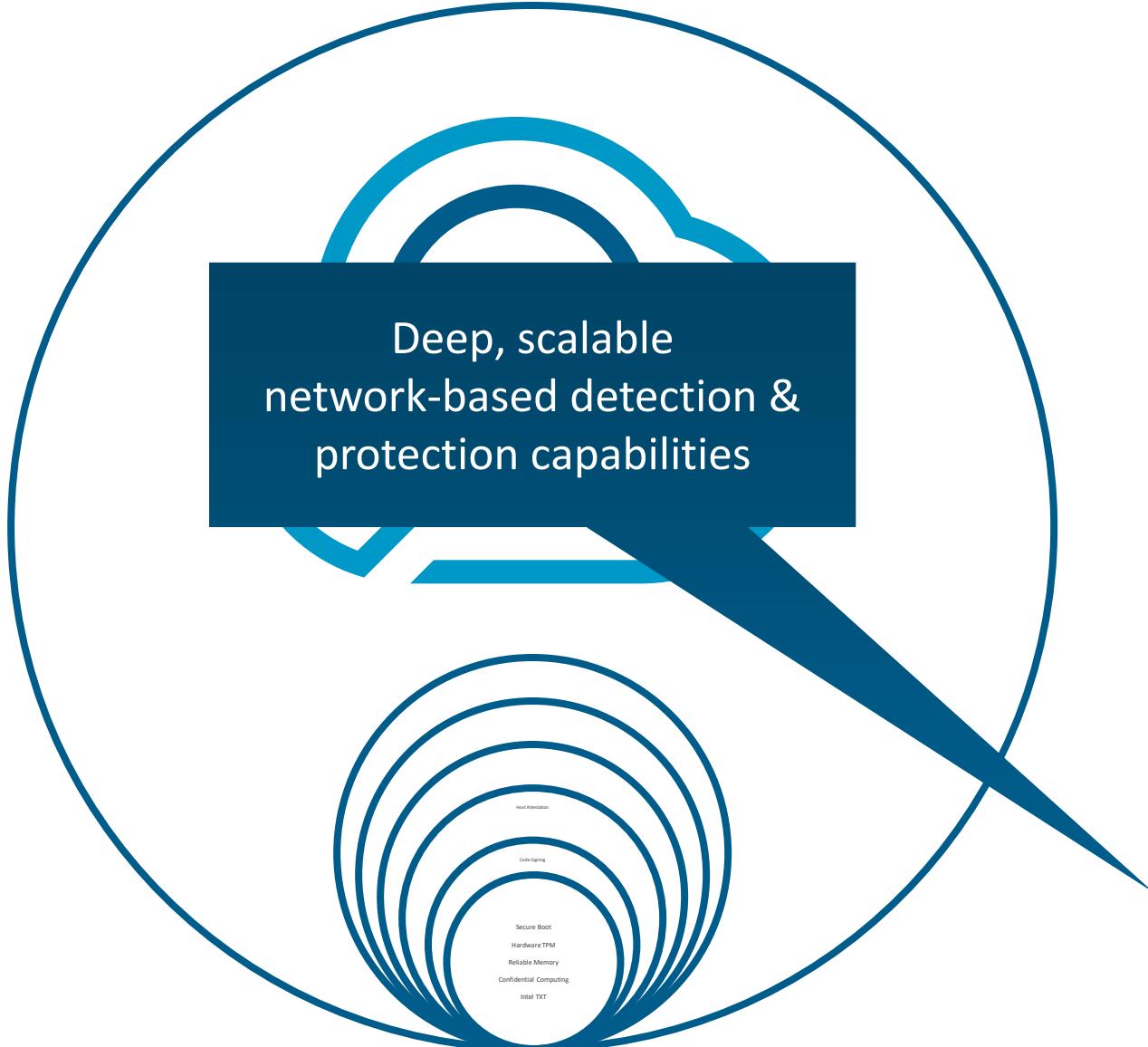
VMware Cloud Foundation® Automation



VMware Live Recovery™



VMware vDefend™



VMware Cloud Foundation® Operations



VMware Cloud Foundation® Automation



VMware Live Recovery™

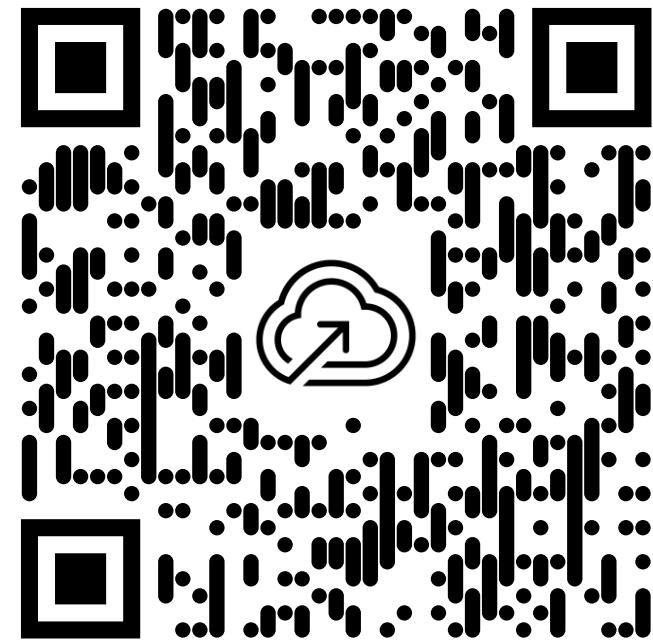


VMware vDefend™

# Security Hardening & Compliance Resources

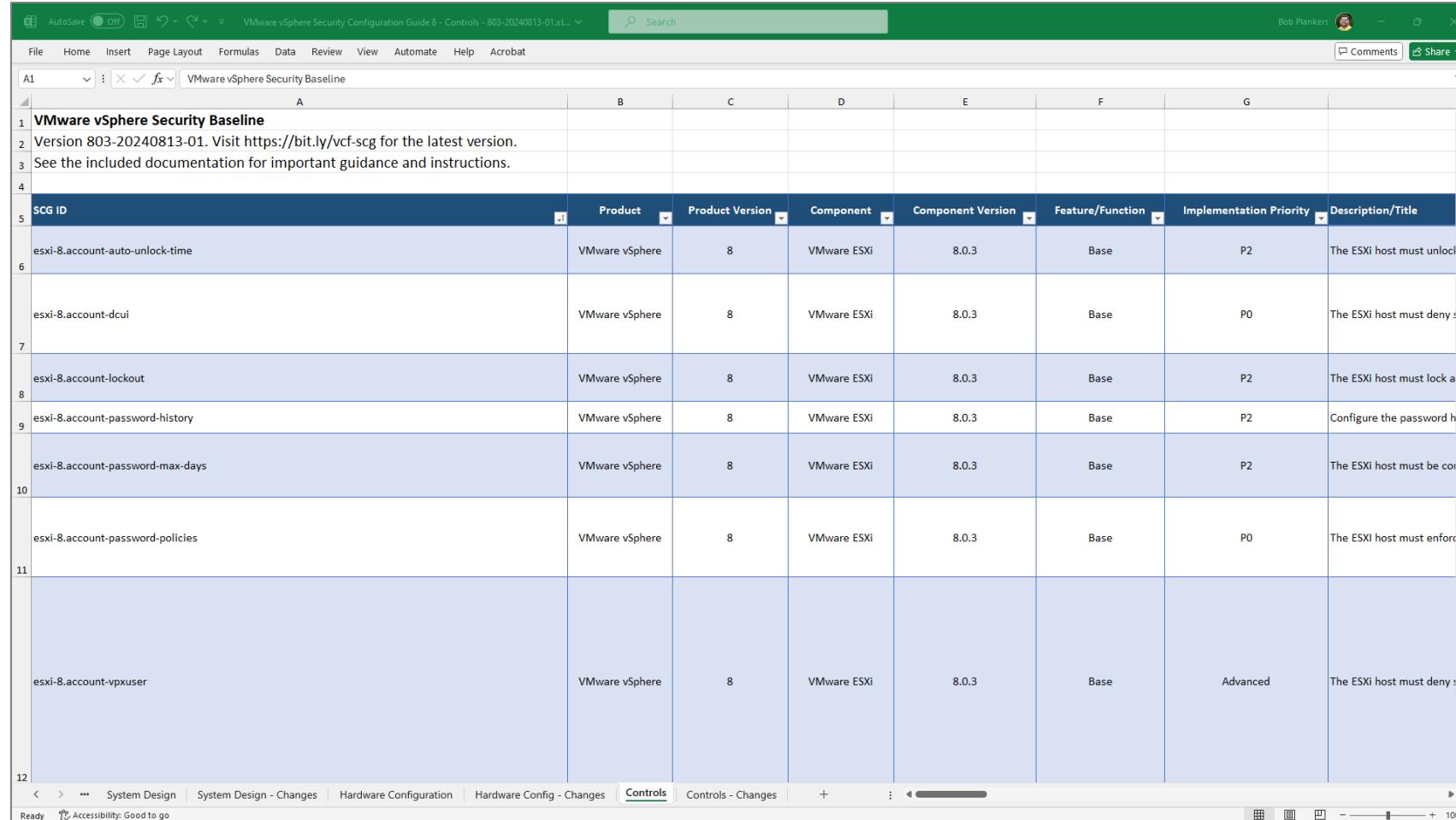
<https://brcm.tech/vcf-security>

<https://github.com/vmware/vcf-security-and-compliance-guidelines/>



# Baseline Security Hardening Guidance

## Security Configuration Guides



SCG ID	Product	Product Version	Component	Component Version	Feature/Function	Implementation Priority	Description/Title
esxi-8.account-auto-unlock-time	VMware vSphere	8	VMware ESXi	8.0.3	Base	P2	The ESXi host must unlock accounts after a specified time period.
esxi-8.account-dcui	VMware vSphere	8	VMware ESXi	8.0.3	Base	P0	The ESXi host must deny direct console user interface (DCUI) access.
esxi-8.account-lockout	VMware vSphere	8	VMware ESXi	8.0.3	Base	P2	The ESXi host must lock accounts after a specified number of failed login attempts.
esxi-8.account-password-history	VMware vSphere	8	VMware ESXi	8.0.3	Base	P2	Configure the password history requirement for accounts.
esxi-8.account-password-max-days	VMware vSphere	8	VMware ESXi	8.0.3	Base	P2	The ESXi host must be configured to enforce password maximum age.
esxi-8.account-password-policies	VMware vSphere	8	VMware ESXi	8.0.3	Base	P0	The ESXi host must enforce password complexity policies.
esxi-8.account-vpxuser	VMware vSphere	8	VMware ESXi	8.0.3	Base	Advanced	The ESXi host must deny direct console user interface (DCUI) access for vpxuser accounts.

Guidance that is easy to use and understand for VCF components

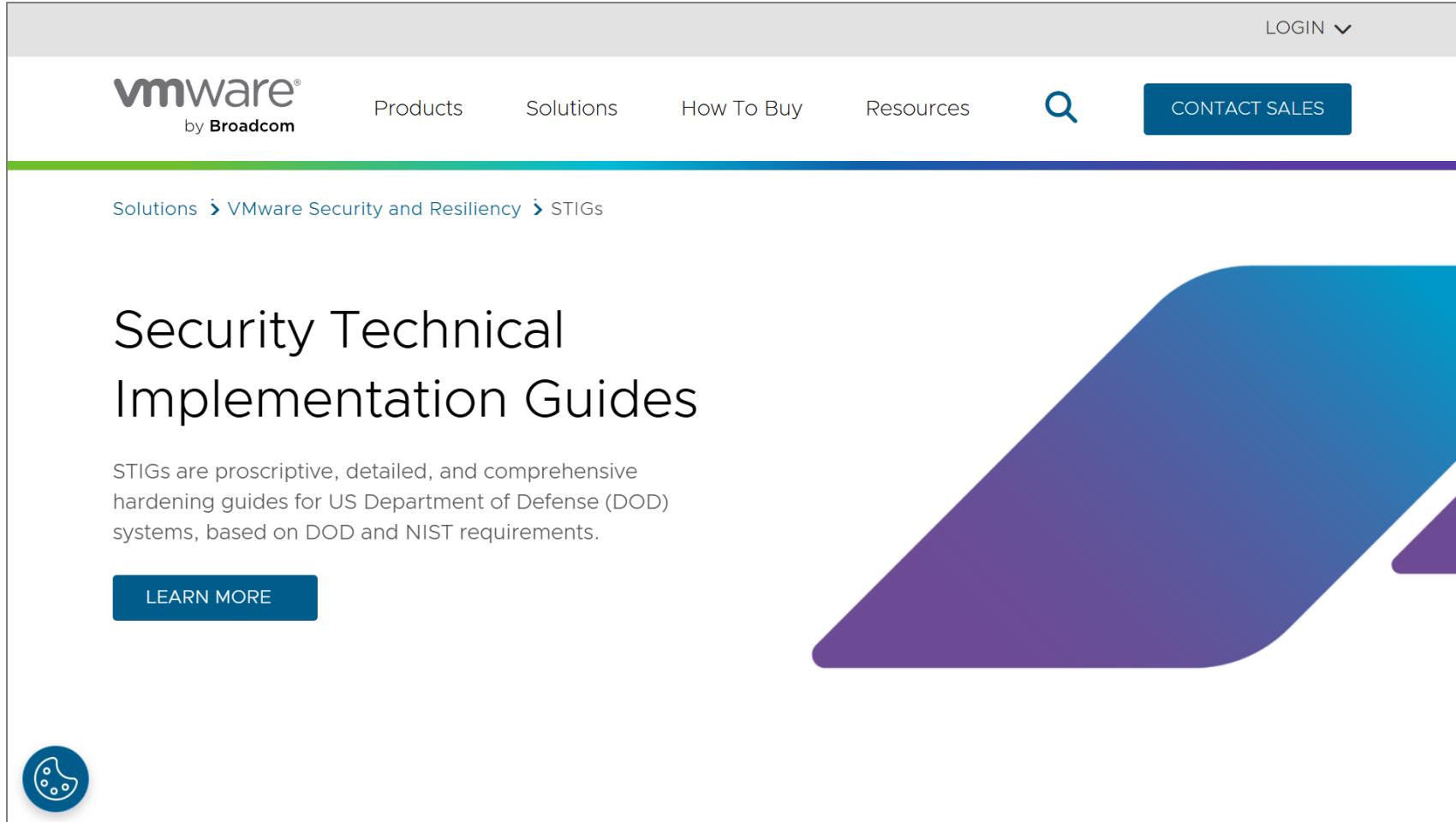
Filterable based on component, feature, version, and risk

Standardizes checks across components

Maps additional regulations and differences

# US Department of Defense Guidance (DISA STIG)

## Security Configuration Guides



The screenshot shows the VMware website with a navigation bar at the top. The navigation bar includes the VMware logo, a search icon, and buttons for 'LOGIN', 'CONTACT SALES', 'Products', 'Solutions', 'How To Buy', and 'Resources'. Below the navigation bar, a breadcrumb trail shows 'Solutions > VMware Security and Resiliency > STIGs'. The main content area features a large blue and purple abstract graphic on the right. The text 'Security Technical Implementation Guides' is prominently displayed. A subtext explains that STIGs are proscriptive, detailed, and comprehensive hardening guides for US Department of Defense (DOD) systems, based on DOD and NIST requirements. A 'LEARN MORE' button is visible. In the bottom left corner, there is a small circular icon with a blue and white design.

DISA-published  
STIGs for direct US  
DOD compliance

STIG Readiness  
Guides: what has  
been submitted to  
DISA for approval

**Automation  
capabilities via  
Powershell &  
InSpec to make it  
easy to pass audits**

# Understand Specifically How VCF Features Help

## Product Applicability Guides & Kits for Regulatory Compliance



**EU Digital Operational Resilience Act**  
Product Applicability Guide for  
VMware Cloud Foundation 5.2  
December 12, 2024

vmware®  
by Broadcom

**Key Functional Categories**

**Access Control**  
VMware Cloud Foundation (VCF) integrates with third-party Privileged Access Management (PAM) solutions and identity providers through APIs, supporting both on-premises and cloud-based authentication for user and programmatic access. The platform enforces granular permissions through role-based access control (RBAC) while VMware vDefend Firewall capabilities manage network access controls.

**Relevant Framework & Article:**

- DORA: Article 9.4(c), 9.4(d)

**Key Components:**

- VMware Cloud Foundation (Core)
- VMware vDefend Distributed Firewall
- VMware vDefend Gateway Firewall

**Cross Reference:**

- NIST 800-53R5: AC-1, IA-1
- SCF 2024.3: IAC-01

**API, Ecosystem, and Integration**  
VMware Cloud Foundation (VCF) provides extensive API integration support for third-party tools such as IT asset management (ITAM), configuration management databases (CMDB), and security assessment tools. The VMware Aria and VMware vDefend product suites deliver security assessment and continuous monitoring functionality. Security teams can generate custom reports, export data, and automate tasks using product interfaces, PowerCLI, and APIs to maintain security and compliance requirements.

**Relevant Framework & Article:**

- DORA: Article 4.1, 4.2, 4.3, 5.4, 8.4, 8.5, 8.6, 9.1, 9.2, 23, 25.1, 25.2, 25.3

**Key Components:**

- VMware Cloud Foundation (Core)
- VMware Aria Operations
- VMware Aria Operations for Logs
- VMware Aria Operations for Networks
- VMware vDefend Distributed Firewall
- VMware vDefend Gateway Firewall

**Cross Reference:**

- NIST 800-53R5: CM-8, CM-8(1), PL-1, RA-5
- SCF 2024.3: AST-01.1, AST-02, AST-02.1, CPL-01, CPL-01.2, OPS-01, VPM-06

vmware®  
by Broadcom

Know which features of VCF apply to a specific regulatory requirement.

Aids auditor understanding of VCF features.

**Speeds design work and audits, making everyone happier.**

# Multiple Compliance Standards? No Problem.

## Secure Controls Framework Mappings

	A	B	C	D	E	F	G	H	I	J	K	Related Work
	SCF Domain	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Evidence Request List (ERL) #	Possible Solutions & Considerations Micro-Small Business (<10 staff) BLS Firm Size Classes 1-2	Possible Solutions & Considerations Small Business (10-49 staff) BLS Firm Size Classes 3-4	Possible Solutions & Considerations Medium Business (50-249 staff) BLS Firm Size Classes 5-6	Possible Solutions & Considerations Large Business (250-999 staff) BLS Firm Size Class 7-8	Possible Solutions & Considerations Enterprise (>1,000 staff) BLS Firm Size Class 9	SCF Control Question	Related Work
1	Cybersecurity & Data Protection Governance	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	E-GOV-01 E-GOV-02	- ComplianceForge - Cybersecurity & Data Protection Program (CDPP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> )	- ComplianceForge - Cybersecurity & Data Protection Program (CDPP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> )	- Steering committee - ComplianceForge - Digital Security Program (DSP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> ) - ComplianceForge - Cybersecurity & Data Protection Program (CDPP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> )	- Steering committee - ComplianceForge - Digital Security Program (DSP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> ) - ComplianceForge - Cybersecurity & Data Protection Program (CDPP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> )	- Steering committee - ComplianceForge - Digital Security Program (DSP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> ) - ComplianceForge - Cybersecurity & Data Protection Program (CDPP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> )	Does the organization facilitate the implementation of cybersecurity & data protection governance controls?	
2	Cybersecurity & Data Protection Governance	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	E-GOV-03	- Third-party advisors (subject matter experts)	- Third-party advisors (subject matter experts)	- Steering committee / advisory board	- Steering committee / advisory board	- Steering committee / advisory board	Does the organization coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis?	
3	Cybersecurity & Data Protection Governance	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	E-CPL-05 E-CPL-09 E-GOV-03 E-GOV-04 E-GOV-05 E-GOV-06	- Quarterly Business Review (QBR)	- Quarterly Business Review (QBR)	- Quarterly Business Review (QBR)	- Quarterly Business Review (QBR)	- Quarterly Business Review (QBR)	Does the organization provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to its cybersecurity & data protection program?	
4	Cybersecurity & Data Protection Governance	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	E-GOV-08 E-GOV-09 E-GOV-11	- ComplianceForge - Cybersecurity & Data Protection Program (CDPP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> ) - SCFConnect ( <a href="https://scfconnect.com">https://scfconnect.com</a> )	- ComplianceForge - Cybersecurity & Data Protection Program (CDPP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> ) - SCFConnect ( <a href="https://scfconnect.com">https://scfconnect.com</a> )	- ComplianceForge - Digital Security Program (DSP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> ) - SCFConnect ( <a href="https://scfconnect.com">https://scfconnect.com</a> )	- ComplianceForge - Cybersecurity & Data Protection Program (CDPP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> ) - SCFConnect ( <a href="https://scfconnect.com">https://scfconnect.com</a> )	- ComplianceForge - Digital Security Program (DSP) ( <a href="https://complianceforge.com">https://complianceforge.com</a> ) - SCFConnect ( <a href="https://scfconnect.com">https://scfconnect.com</a> )	Does the organization establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures?	
5	Cybersecurity & Data Protection Governance	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	E-GOV-18	- Manual exception management process - SCFConnect ( <a href="https://scfconnect.com">https://scfconnect.com</a> )	- Manual exception management process - Governance, Risk & Compliance (GRC) solution - SCFConnect ( <a href="https://scfconnect.com">https://scfconnect.com</a> )	- Manual exception management process - Governance, Risk & Compliance (GRC) solution - SCFConnect ( <a href="https://scfconnect.com">https://scfconnect.com</a> )	- Manual exception management process - Governance, Risk & Compliance (GRC) solution - SCFConnect ( <a href="https://scfconnect.com">https://scfconnect.com</a> )	- Governance, Risk & Compliance (GRC) solution - SCFConnect ( <a href="https://scfconnect.com">https://scfconnect.com</a> )	Does the organization prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded?	
6	Cybersecurity & Data Protection Governance	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	E-GOV-12	- Human reviews - Documentation change control	- Human reviews - Documentation change control	- Human reviews - Documentation change control	- Human reviews - Documentation change control	- Human reviews - Documentation change control	Does the organization review the cybersecurity & data privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness?	
7	Cybersecurity & Data Protection Governance	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	E-HRS-01 E-HRS-05 E-HRS-06 E-HRS-07 E-HRS-08 E-HRS-09	- Third-party advisors (e.g., virtual CISO, Managed Security Services Provider (MSSP), etc.)	- Third-party advisors (e.g., virtual CISO, Managed Security Services Provider (MSSP), etc.)	- Chief Information Security Officer (CISO)	- Chief Information Security Officer (CISO)	- Chief Information Security Officer (CISO)	Does the organization assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program?	
8	Cybersecurity & Data Protection Governance	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	E-HRS-15	- Documented roles and responsibilities	- Documented roles and responsibilities	- Documented roles and responsibilities	- Documented roles and responsibilities	- Documented roles and responsibilities	Does the organization enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks?	
9	Cybersecurity & Data Protection Governance	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	E-HRS-15	- Organization chart	- Organization chart	- Organization chart	- Organization chart	- Organization chart	Does the organization establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks?	
10	Cybersecurity & Data Protection Governance	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	E-GOV-13	- Manually-generated metrics - Governance, Risk & Compliance (GRC) solution	- Manually-generated metrics - Governance, Risk & Compliance (GRC) solution	- Manually-generated metrics - Governance, Risk & Compliance (GRC) solution	- Manually-generated metrics - Governance, Risk & Compliance (GRC) solution	- Manually-generated metrics - Governance, Risk & Compliance (GRC) solution	Does the organization develop, report and monitor cybersecurity & data privacy program measures of performance?	
11				Mechanisms exist to develop, report and monitor Key		- Manually-generated metrics	- Manually-generated metrics	- Manually-generated metrics	- Manually-generated metrics	- Manually-generated metrics	Does the organization develop, report and monitor Key	

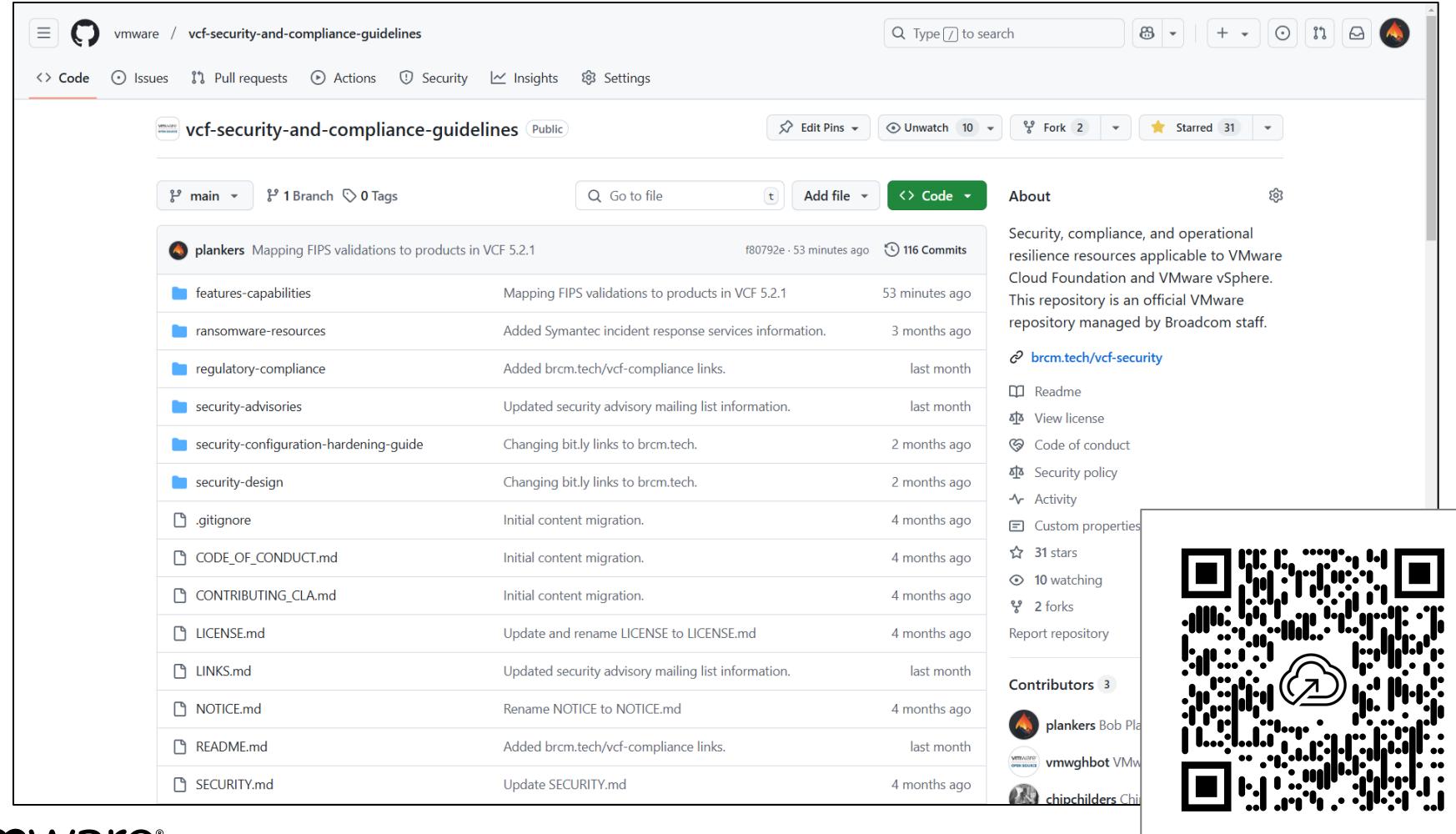
SCF is a terrific open-source meta-framework for regulatory compliance

Crosswalk between 100+ compliance standards

We've mapped VCF capabilities & baseline guidance to security controls

# Lots of Other Security & Compliance Information

<https://github.com/vmware/vcf-security-and-compliance-guidelines>



The screenshot shows the GitHub repository page for `vcf-security-and-compliance-guidelines`. The repository is public and has 116 commits. The 'About' section describes the repository as a collection of security, compliance, and operational resilience resources for VMware Cloud Foundation and vSphere. It is managed by Broadcom staff. The page includes links to the README, license, code of conduct, security policy, and activity. A QR code is displayed on the right side of the page.

**Commits:**

- plankers Mapping FIPS validations to products in VCF 5.2.1 (f80792e - 53 minutes ago)
- features-capabilities Mapping FIPS validations to products in VCF 5.2.1 (53 minutes ago)
- ransomware-resources Added Symantec incident response services information. (3 months ago)
- regulatory-compliance Added brcm.tech/vcf-compliance links. (last month)
- security-advisories Updated security advisory mailing list information. (last month)
- security-configuration-hardening-guide Changing bit.ly links to brcm.tech. (2 months ago)
- security-design Changing bit.ly links to brcm.tech. (2 months ago)
- .gitignore Initial content migration. (4 months ago)
- CODE\_OF\_CONDUCT.md Initial content migration. (4 months ago)
- CONTRIBUTING\_CLA.md Initial content migration. (4 months ago)
- LICENSE.md Update and rename LICENSE to LICENSE.md (4 months ago)
- LINKS.md Updated security advisory mailing list information. (last month)
- NOTICE.md Rename NOTICE to NOTICE.md (4 months ago)
- README.md Added brcm.tech/vcf-compliance links. (last month)
- SECURITY.md Update SECURITY.md (4 months ago)

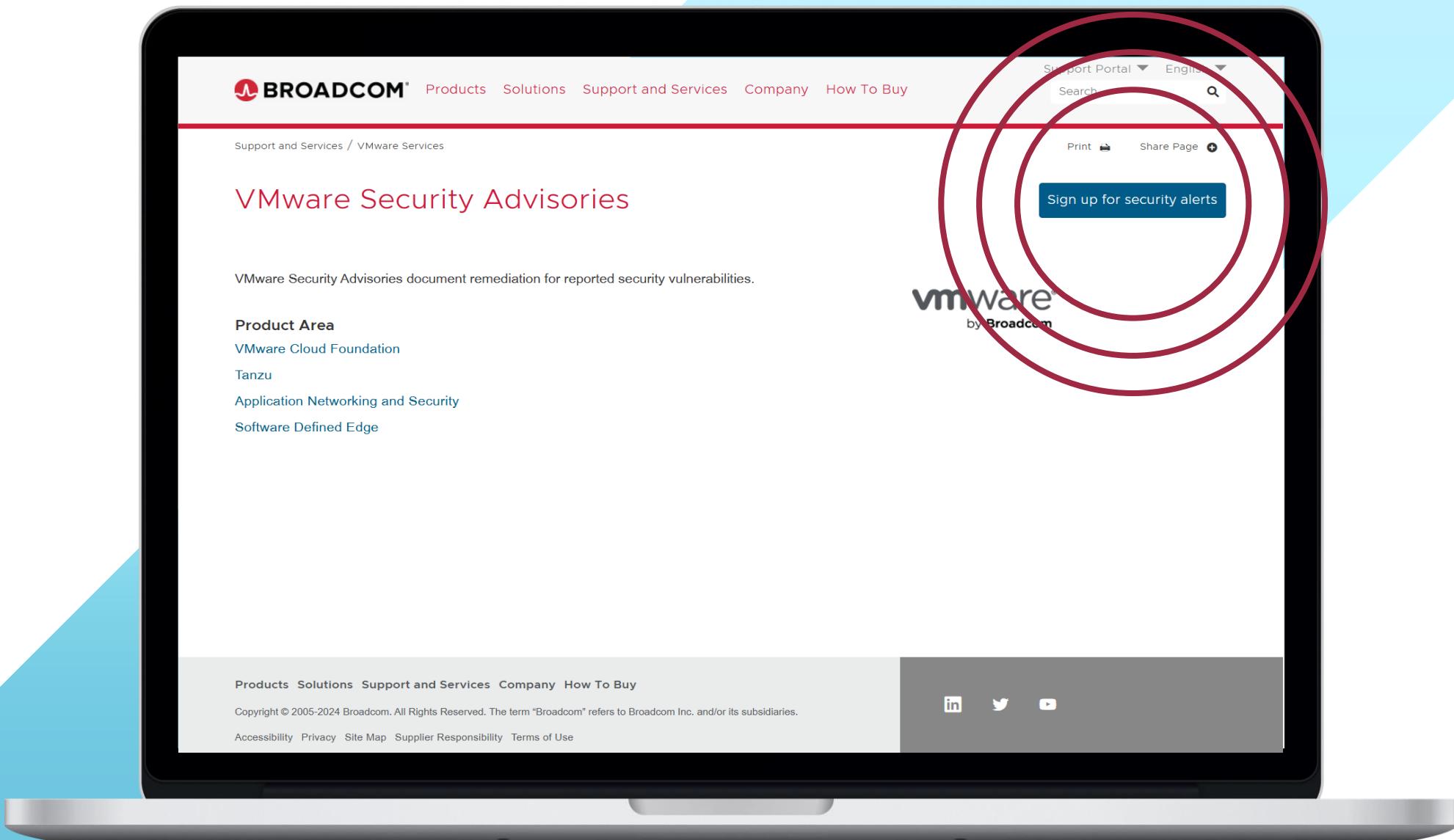
Vast Q&A for product capabilities

Regulatory compliance information

SCG & sample code for automation

Advisory Q&A

A growing “one-stop shop” for all things VMware security



**Adria Forum 2025**

# Thank You!