MBCOM TECHNOLOGIES | vmware by Broadcom

Adria Forum 2025

Security for Private Cloud with VCF

Mladen Krivokuća

Senior Solution Engineer, MBCOM Technologies, Broadcom Representative

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.

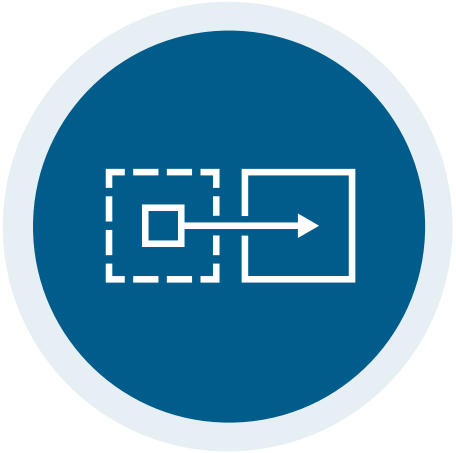
CIA Triad: **Core Tenets** of Information Security

Confidentiality

Protecting systems & data from unauthorized people & groups

Integrity

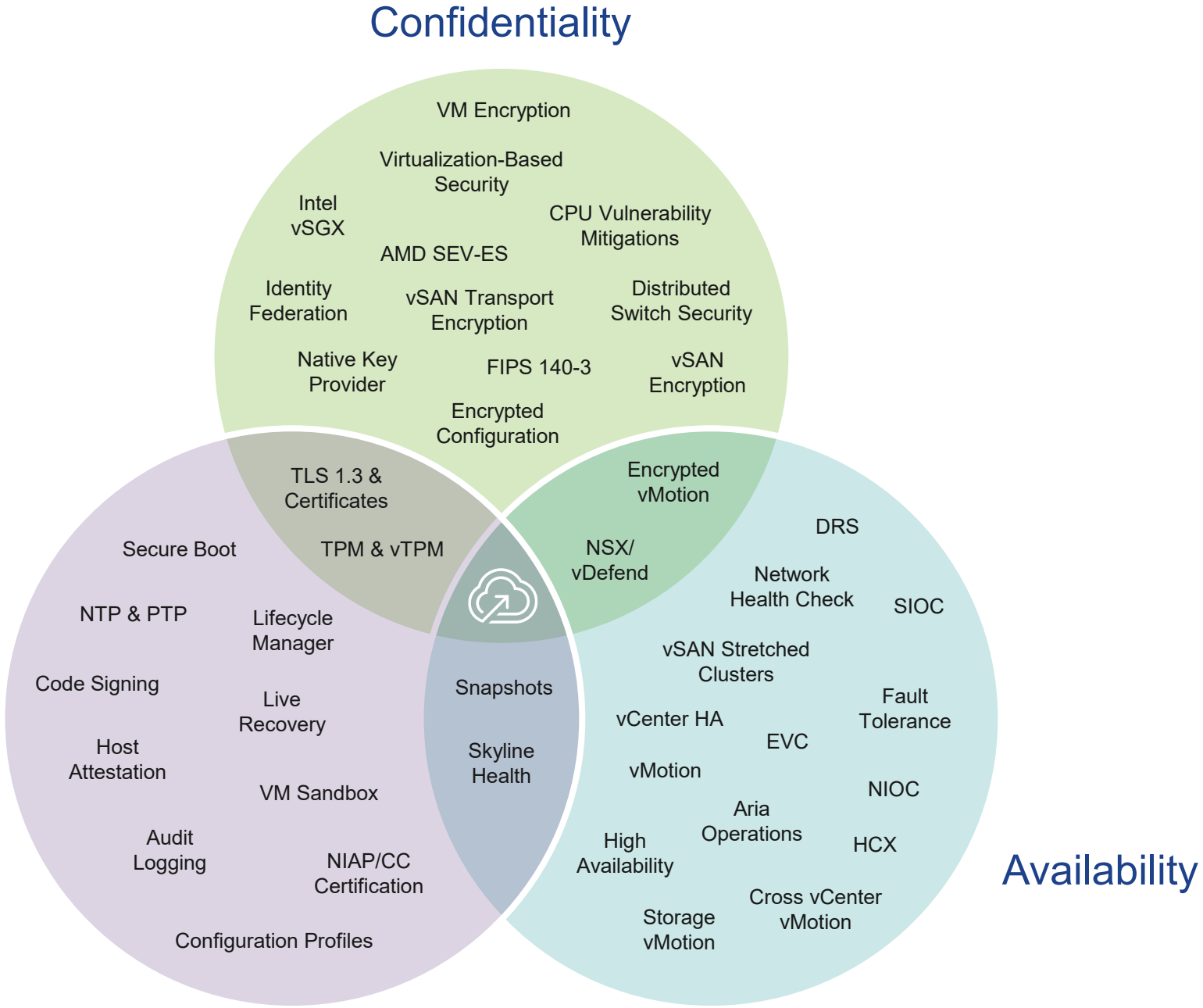
Preventing modification of data by unauthorized groups & systems



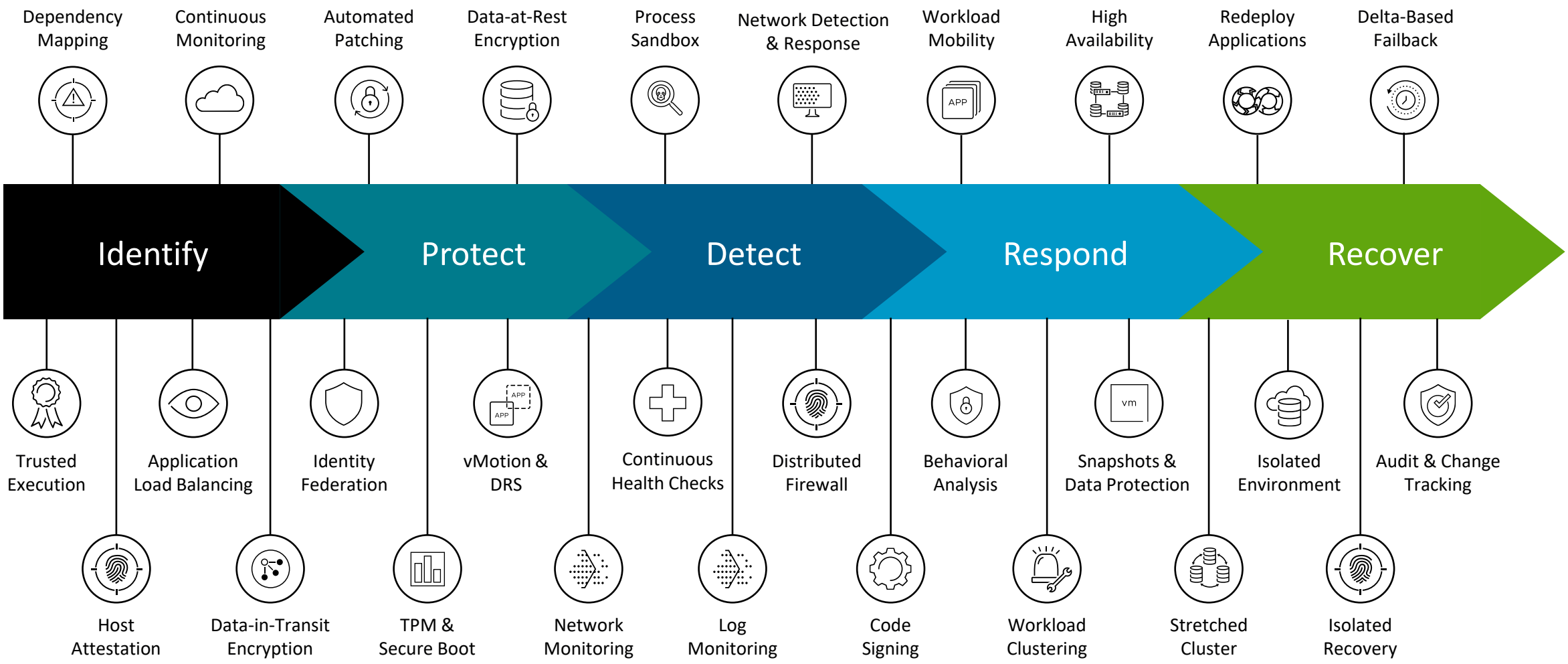
Availability

Ensuring that data is available to authorized parties when needed

Every Feature is a Security Feature

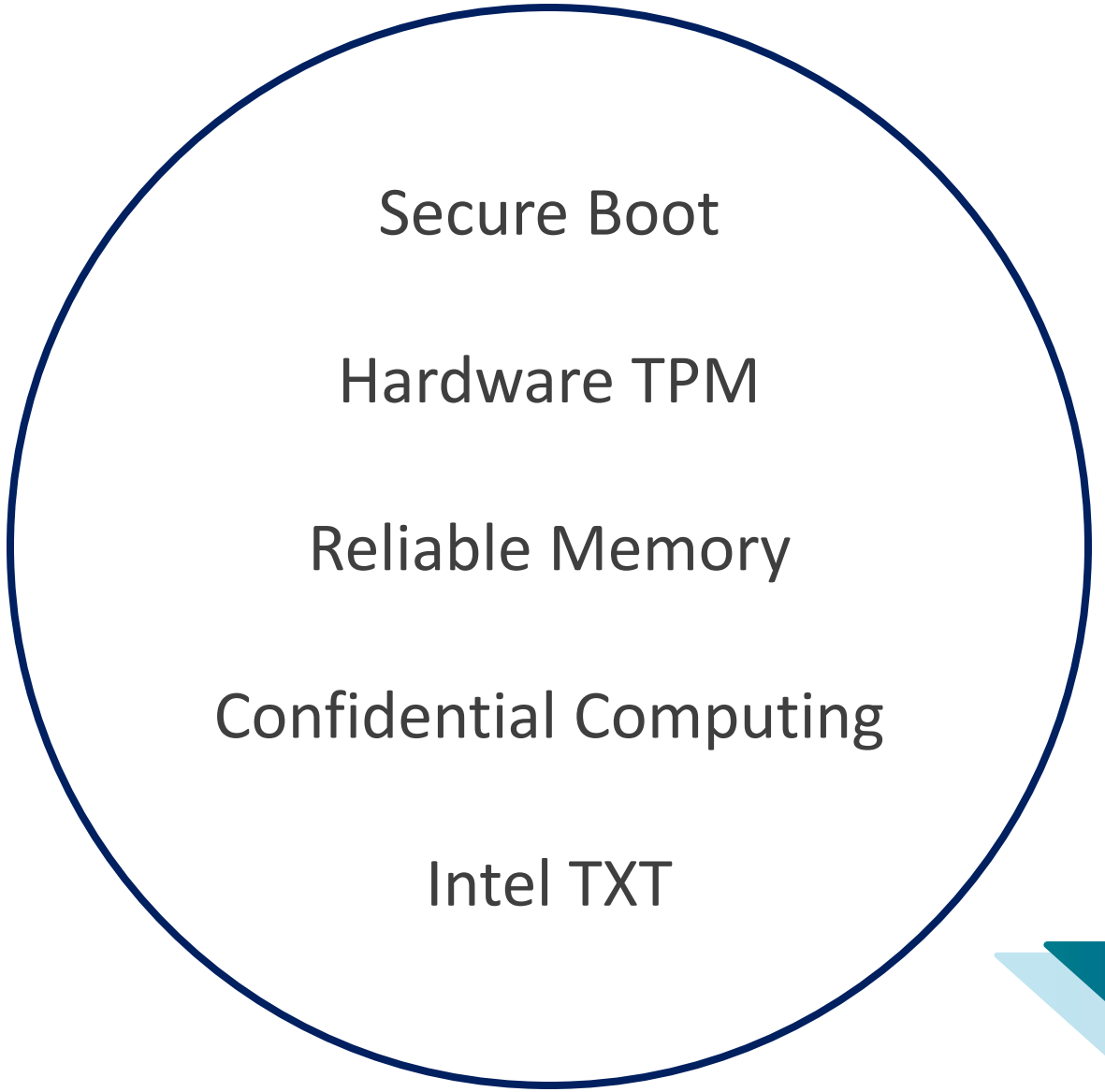


Resilience Woven Throughout VMware Cloud Foundation

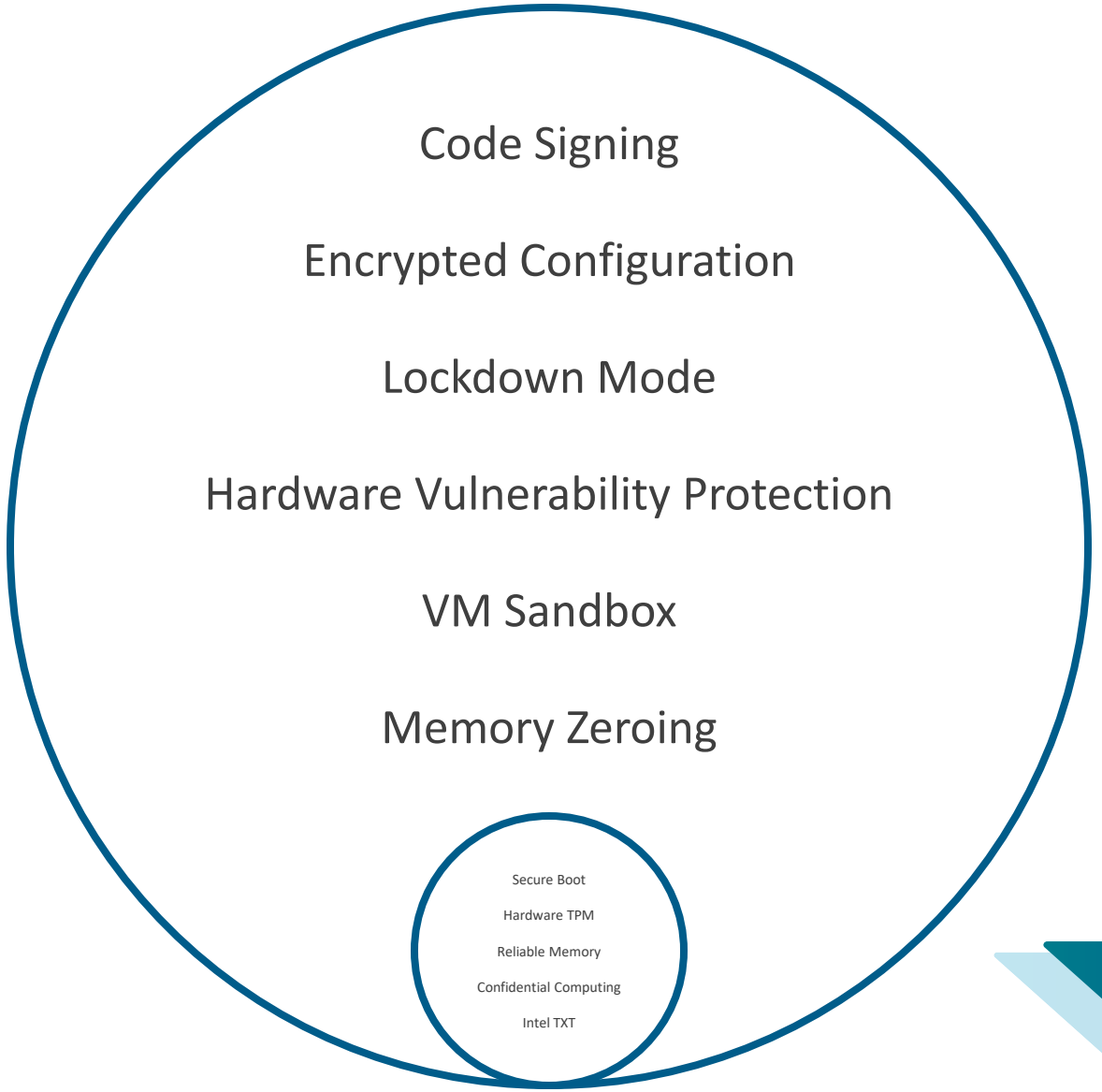


Layered Defenses

VMware Cloud Foundation 9.0



Hardware

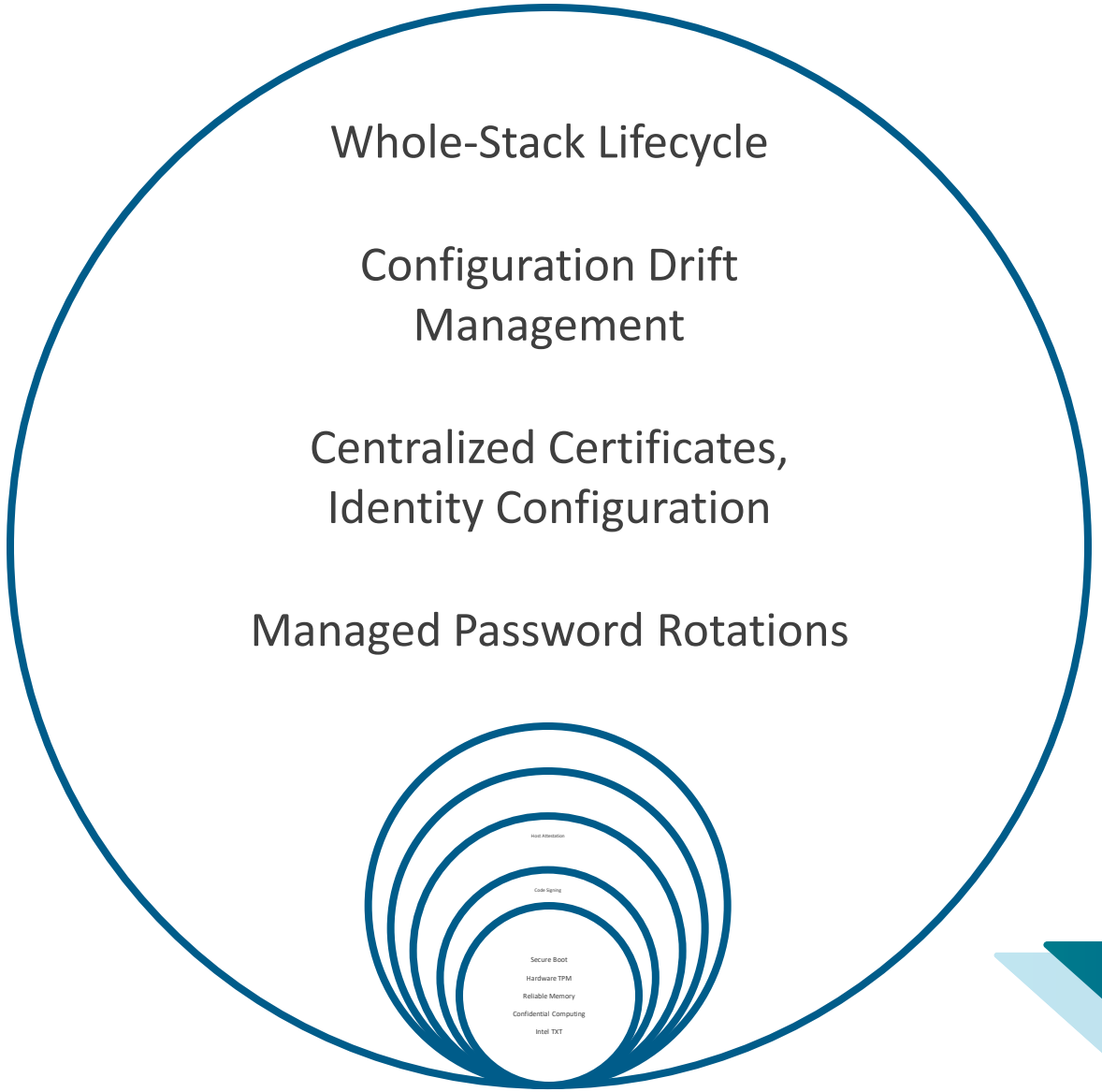


Hypervisor

vCenter

vSAN

Workloads



Operations

VCF

VMware Cloud Foundation® Operations

VMware Cloud Foundation® Automation

VMware Live Recovery™

VMware vDefend™

vmware by Broadcom

VMware Cloud Foundation® Operations

VMware Cloud Foundation® Automation

VMware Live Recovery™

VMware vDefend™

VMware Cloud Foundation® Operations

VMware Cloud Foundation® Automation

VMware Live Recovery™

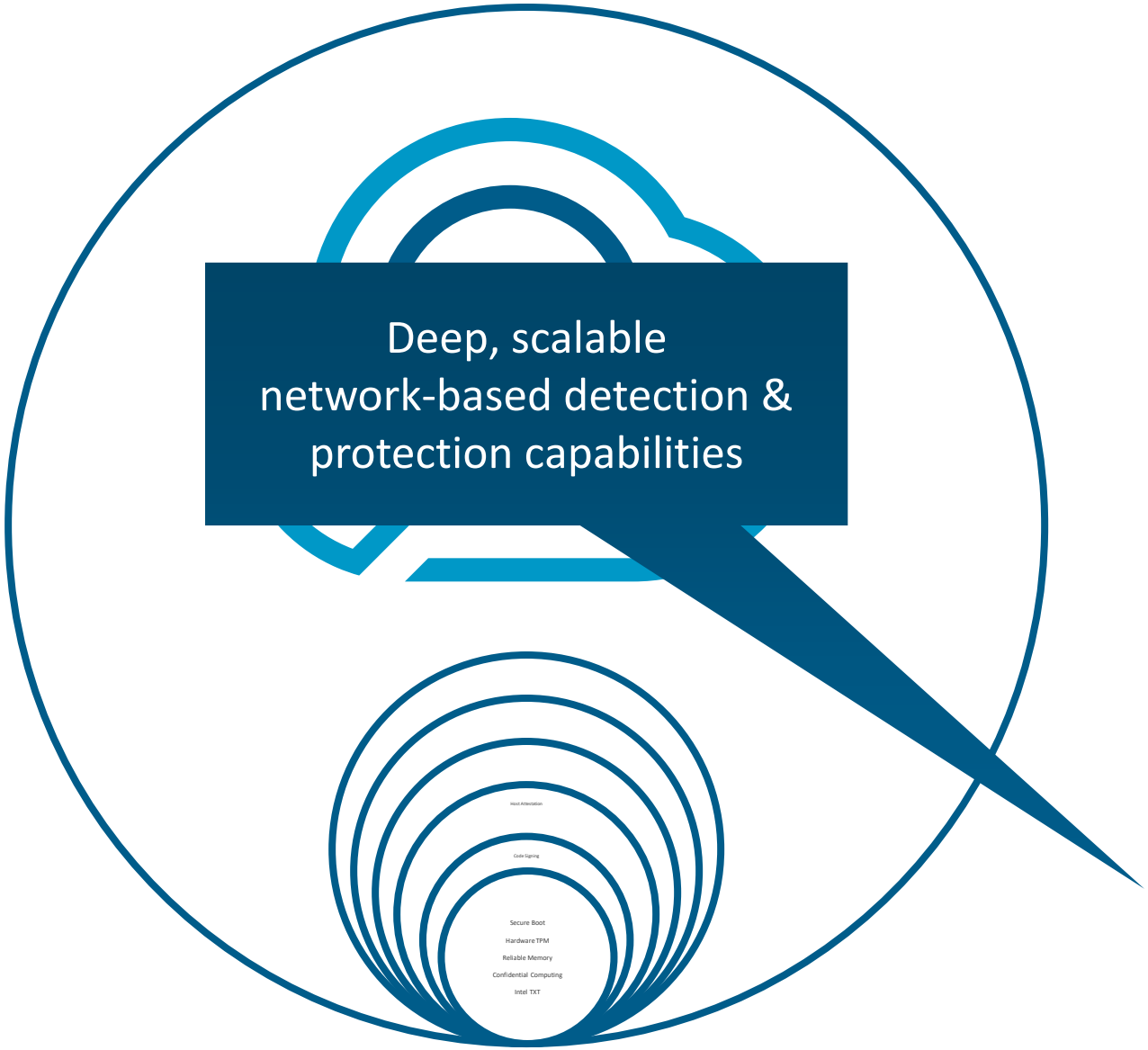
VMware vDefend™

VMware Cloud Foundation® Operations

VMware Cloud Foundation® Automation

VMware Live Recovery™

VMware vDefend™



VMware Cloud Foundation® Operations

VMware Cloud Foundation® Automation

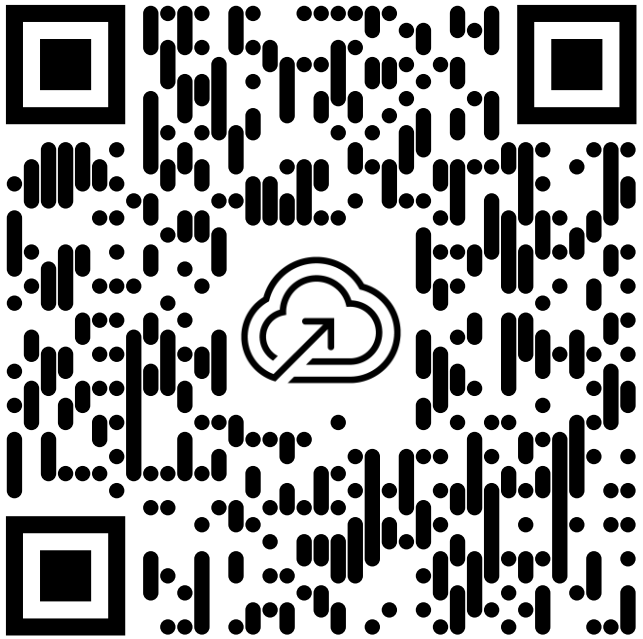
VMware Live Recovery™

VMware vDefend™

Security Hardening & Compliance Resources

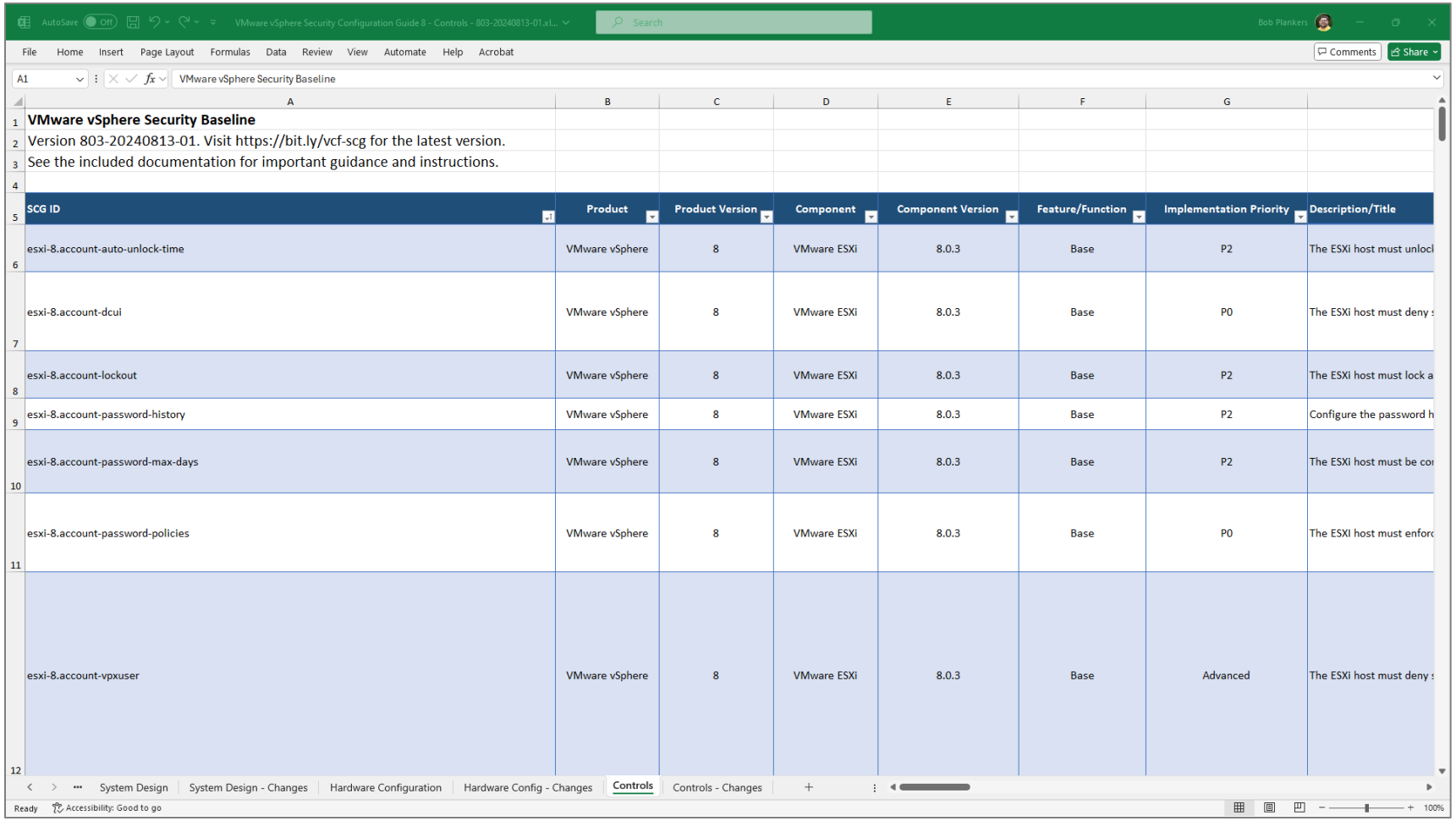
https://brcm.tech/vcf-security

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



Baseline Security Hardening Guidance

Security Configuration Guides



VMware vSphere Security Configuration Guide 8 - Controls - 803-20240813-01.xl...

File Home Insert Page Layout Formulas Data Review View Automate Help Acrobat

A1 | VMware vSphere Security Baseline

VMware vSphere Security Baseline

Version 803-20240813-01. Visit https://bit.ly/vcf-scg for the latest version.

See the included documentation for important guidance and instructions.

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
esxi-8.account-dcui	VMware vSphere	8	VMware ESXi	8.0.3	Base	P0	The ESXi host must deny s
esxi-8.account-lockout	VMware vSphere	8	VMware ESXi	8.0.3	Base	P2	The ESXi host must lock a
esxi-8.account-password-history	VMware vSphere	8	VMware ESXi	8.0.3	Base	P2	Configure the password h
esxi-8.account-password-max-days	VMware vSphere	8	VMware ESXi	8.0.3	Base	P2	The ESXi host must be cor
esxi-8.account-password-policies	VMware vSphere	8	VMware ESXi	8.0.3	Base	P0	The ESXI host must enforc
esxi-8.account-vpxuser	VMware vSphere	8	VMware ESXi	8.0.3	Base	Advanced	The ESXi host must deny s

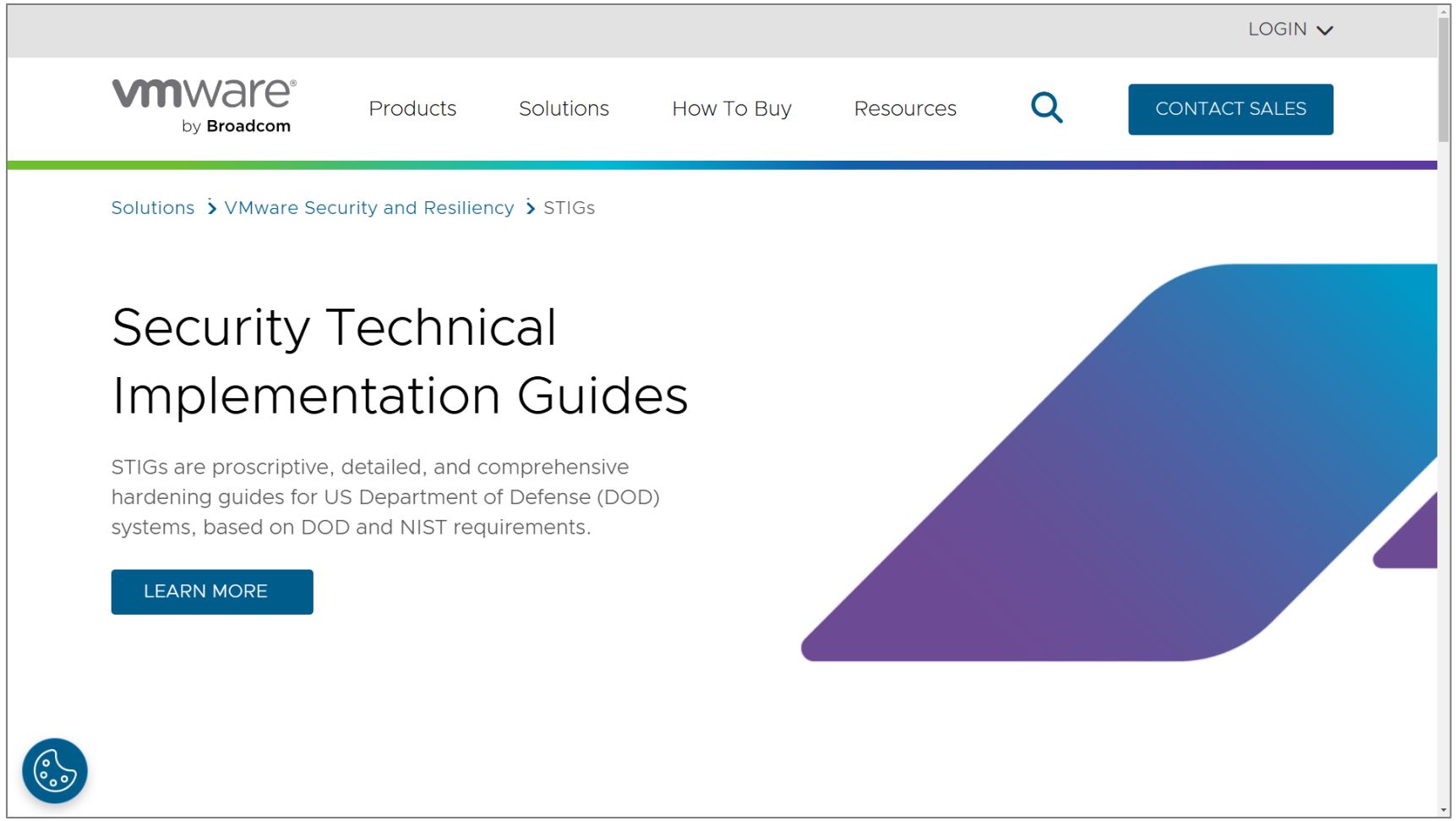
System Design | System Design - Changes | Hardware Configuration | Hardware Config - Changes | Controls | Controls - Changes

Ready | Accessibility: Good to go | 100%

- 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



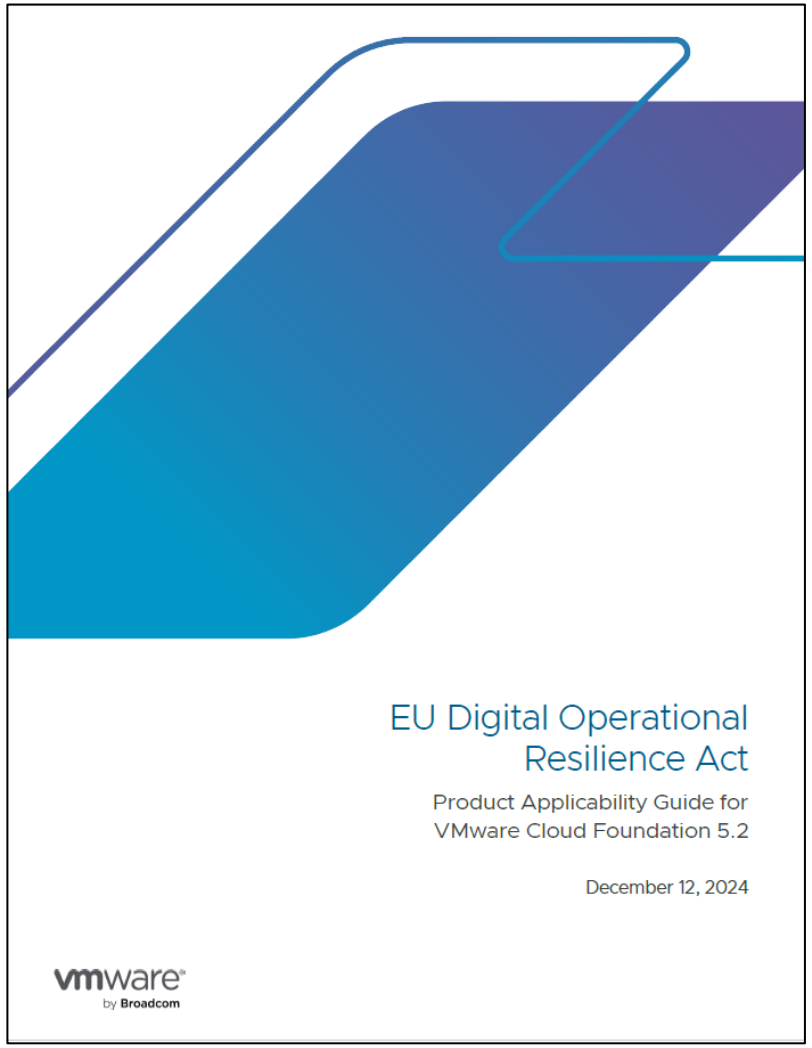
DISA-published STIGs for direct US DOD compliance

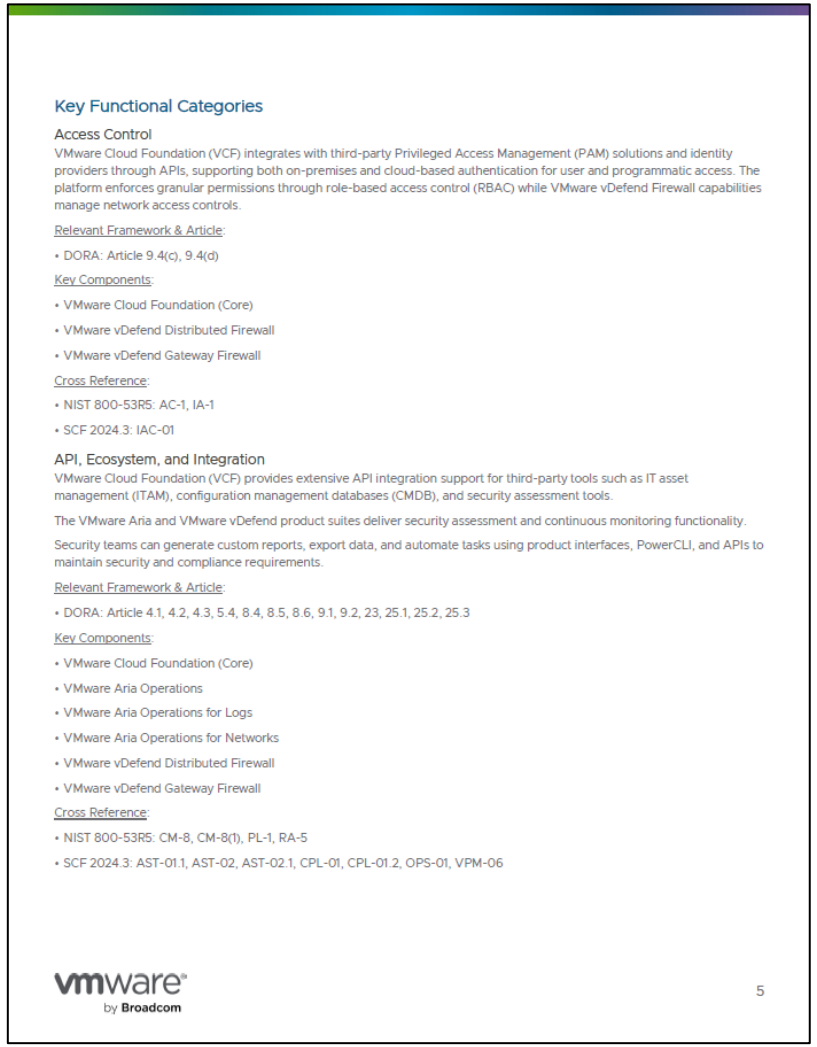
STIG Readiness Guides: what has been submitted to DISA for approval

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





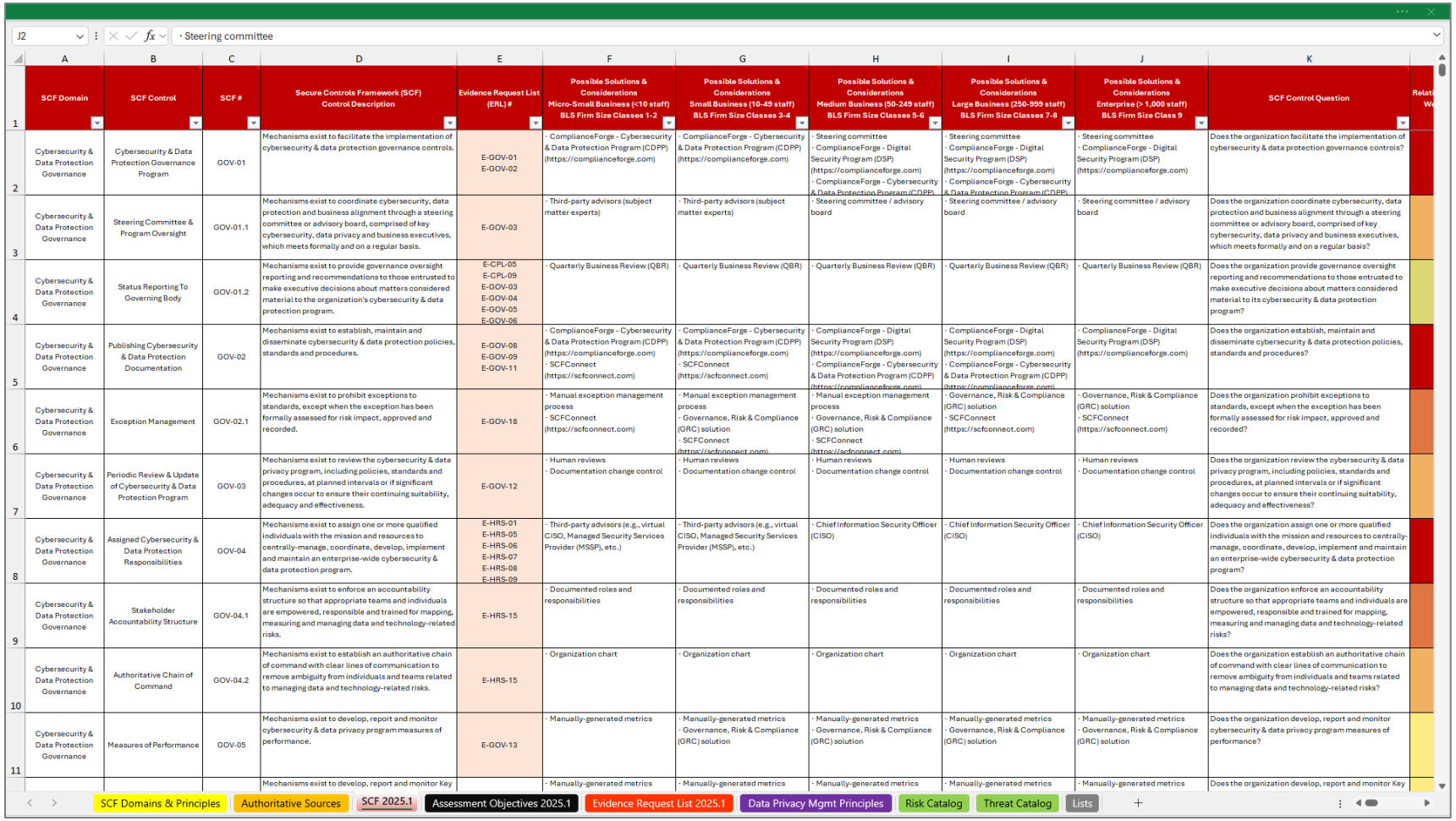
Know which features of VCF apply to a specific regulatory requirement.

Aids auditor understanding of VCF features.

Speeds design work and audits, making everyone happier.

Multiple Compliance Standards? No Problem.

Secure Controls Framework Mappings



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 Classes 7-8	Possible Solutions & Considerations Enterprise (> 1,000 staff) BLS Firm Size Class 9	SCF Control Question
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) (https://complianceforge.com)	· ComplianceForge - Cybersecurity & Data Protection Program (CDPP) (https://complianceforge.com)	· Steering committee · ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com) · ComplianceForge - Cybersecurity & Data Protection Program (CDPP)	· Steering committee · ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com) · ComplianceForge - Cybersecurity & Data Protection Program (CDPP)	· Steering committee · ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com)	Does the organization facilitate the implementation of cybersecurity & data protection governance controls?
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?
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?
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) (https://complianceforge.com) · SCFConnect (https://scfconnect.com)	· ComplianceForge - Cybersecurity & Data Protection Program (CDPP) (https://complianceforge.com) · SCFConnect (https://scfconnect.com)	· ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com) · ComplianceForge - Cybersecurity & Data Protection Program (CDPP) (https://complianceforge.com)	· ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com) · ComplianceForge - Cybersecurity & Data Protection Program (CDPP) (https://complianceforge.com)	· ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com)	Does the organization establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures?
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 (https://scfconnect.com)	· Manual exception management process · Governance, Risk & Compliance (GRC) solution · SCFConnect (https://scfconnect.com)	· Manual exception management process · Governance, Risk & Compliance (GRC) solution · SCFConnect (https://scfconnect.com)	· Governance, Risk & Compliance (GRC) solution · SCFConnect (https://scfconnect.com)	· Governance, Risk & Compliance (GRC) solution · SCFConnect (https://scfconnect.com)	Does the organization prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded?
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?
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?
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?
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?
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	· 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?
			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 Domains & Principles | Authoritative Sources | SCF 2025.1 | Assessment Objectives 2025.1 | Evidence Request List 2025.1 | Data Privacy Mgmt Principles | Risk Catalog | Threat Catalog | Lists

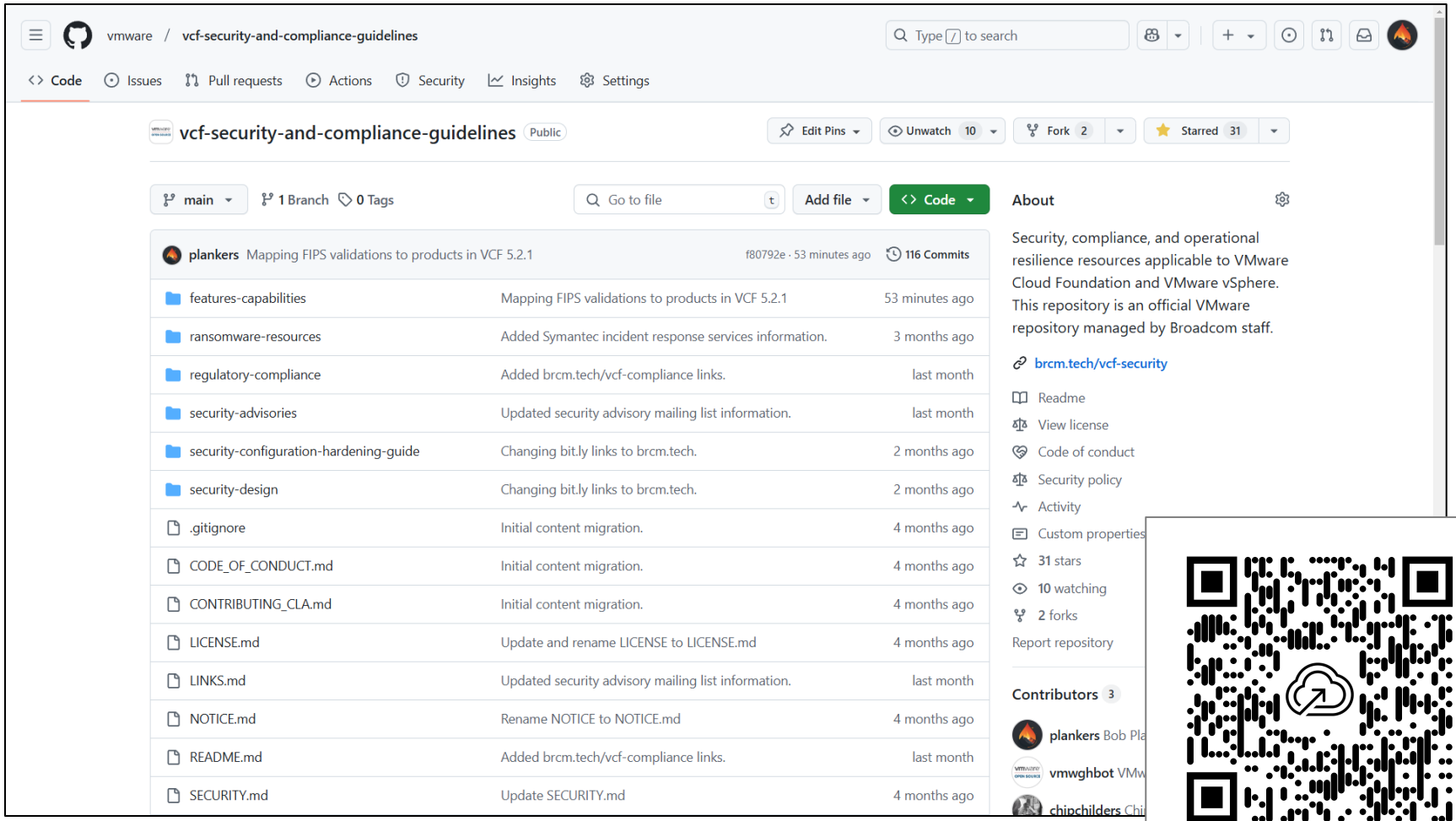
SCF is a terrific open-source meta-framework for regulatory compliance

Crosswalk between 100+ compliance standards

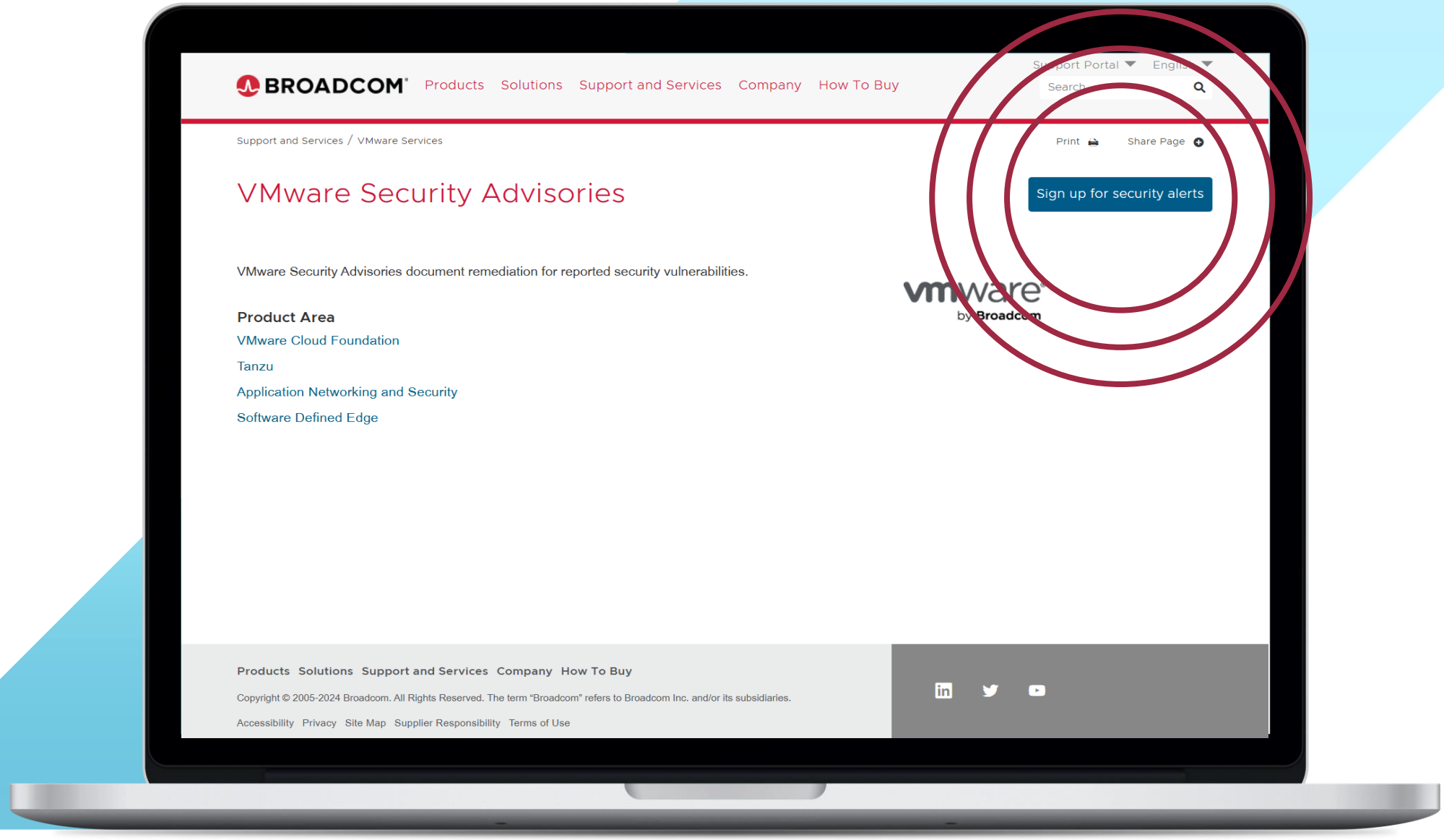
We've mapped VCF capabilities & baseline guidance to security controls

Lots of Other Security & Compliance Information

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



- 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



MBCOM TECHNOLOGIES | vmware by Broadcom

Adria Forum 2025

Thank You!