

CSXB2105LV

vmware® EXPLORE

Best Practices for Hardening Your VMware Infrastructure

Daniel Mazzini, CXS Staff Architect, VMware

Kacy Reed, Consulting Architect, VMware

#vmwareexplore #CSXB2105LV



Presenters



Daniel Mazzini
CXS Staff Architect



Kacy Reed
Staff Architect



Agenda

The Path to Securing Your Infrastructure

Best Practices For VMware Products

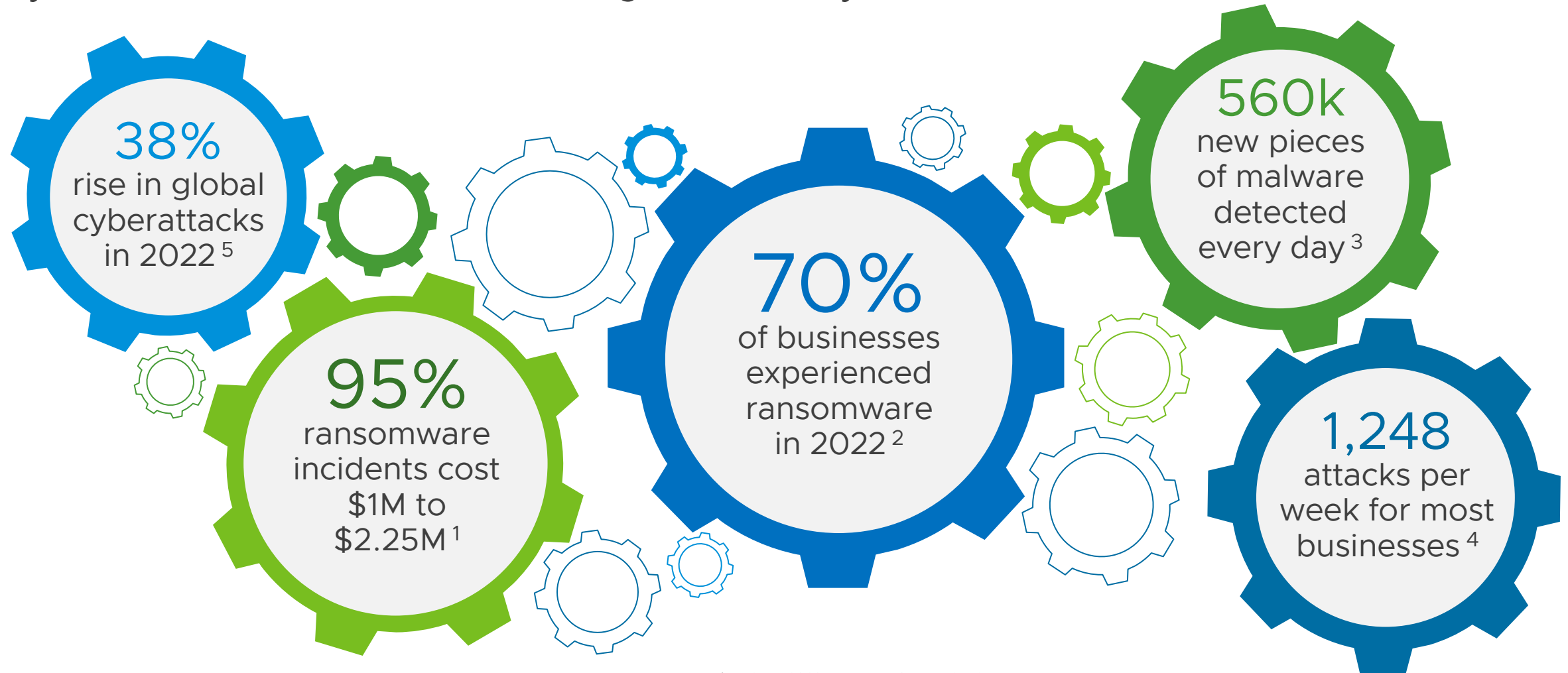
Resources

Q & A



Why Prioritizing a Secure Infrastructure Can't Wait

Cyber attackers and threat actors target data everywhere – all the time



¹ Verizon: 2023 Data Breach Investigations Report

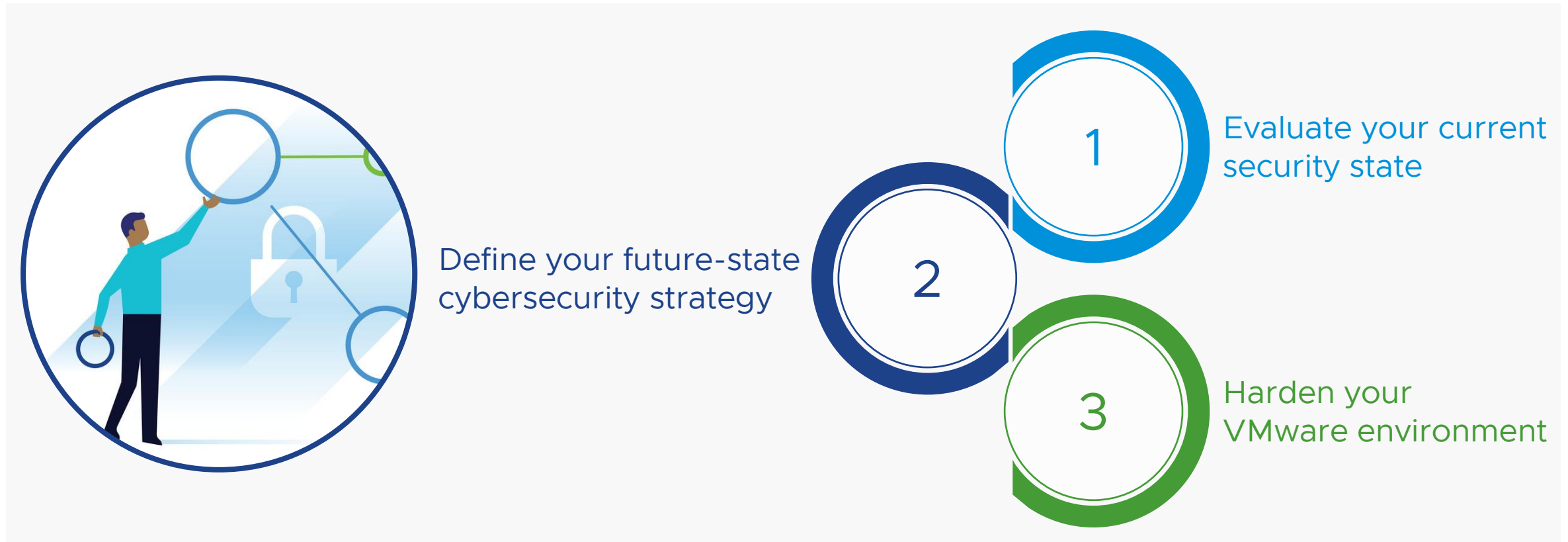
² www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

³ <https://dataprot.net/statistics/malware-statistics/>

⁴ <https://pages.checkpoint.com/forrester-wave-for-enterprise-email-security-2023.html>

⁵ <https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks>

The Steps to Securing Your Infrastructure



Assess and Evaluate Your Current State

Assessment outcomes include a plan to reach your target state

Assessment Practices

Identify and evaluate threats, vulnerabilities, risks, compliance requirements, and effectiveness of existing security controls



Suggested frequency:
Once every two years
depending on industry and regulatory compliance requirements or when major architecture changes occur

Assessment Outcomes

Gaps in current state security posture identified



Recommendations for remediation and mitigation



Action plan for remediation to achieve target state



Compliance with regulations and standards

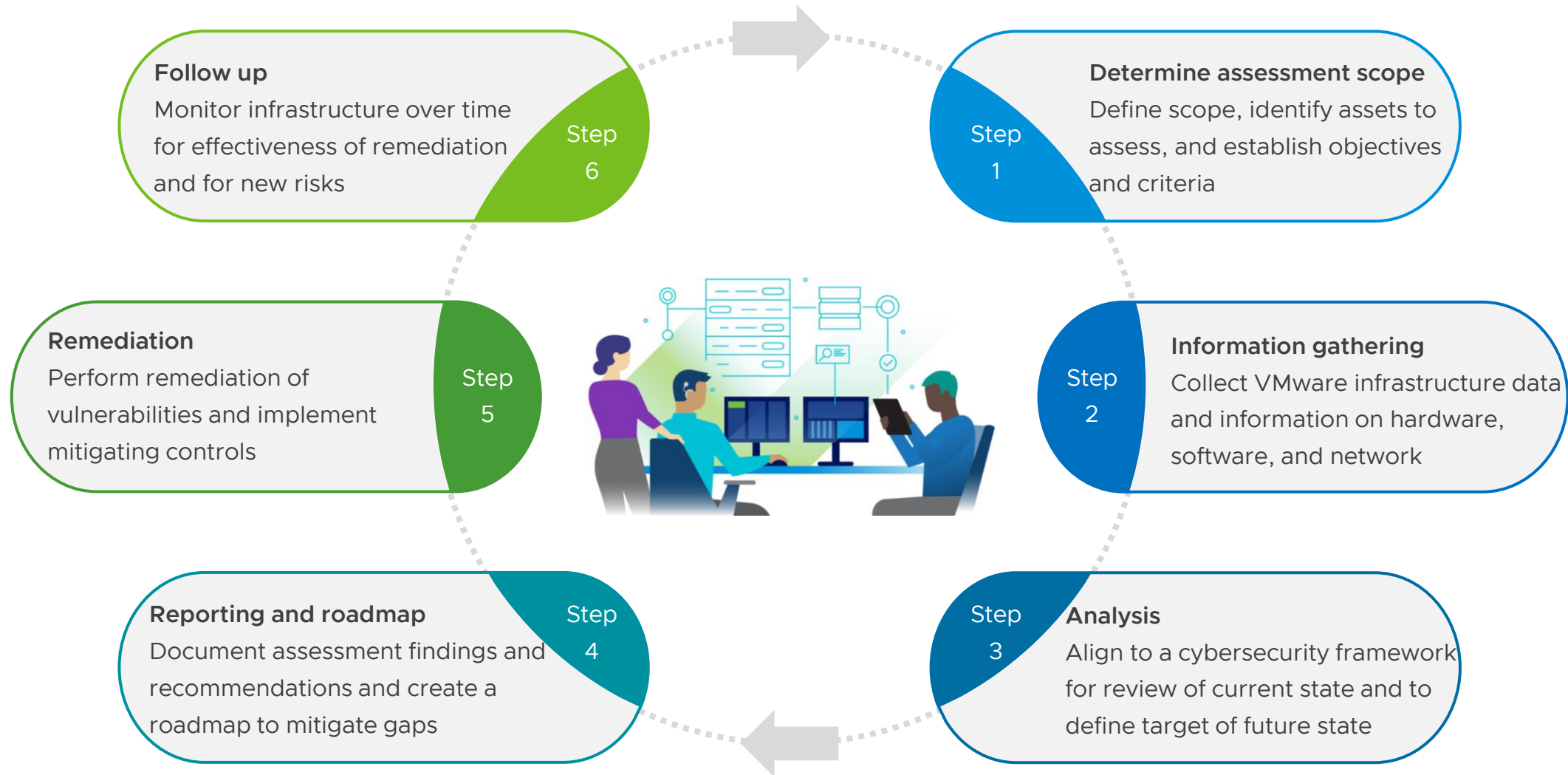


Improvement of overall security posture

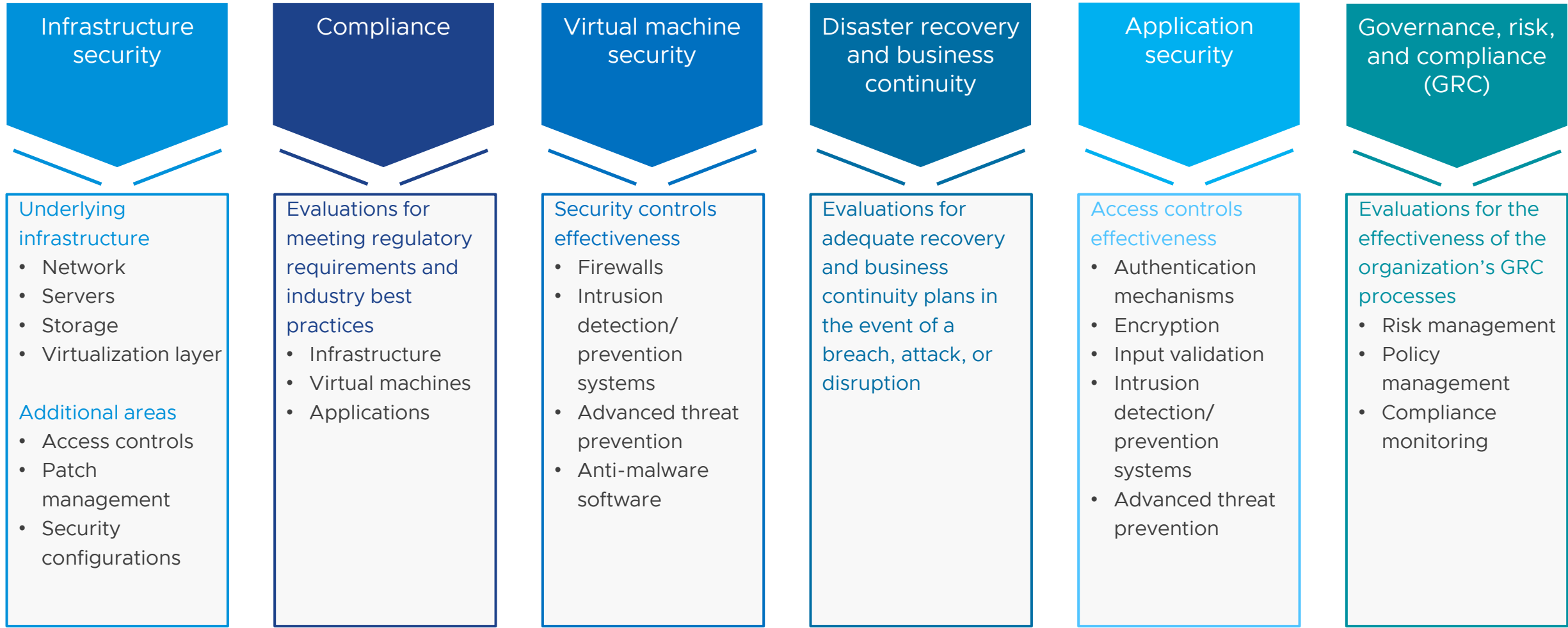


The Assessment Process

High-level evaluation process and defining the future state



Security Assessments Must Cover the Entire IT Ecosystem



Implementing Security Best Practices to Harden Your Infrastructure

Hardening outcomes reduce potential for cyber attacks and data breaches

Hardening Practices

Secure VMware infrastructure by implementing best practices aligned to an industry-recognized cybersecurity framework



Suggested frequency:
During initial implementation and throughout system life cycle until end-of-life decommissioning

Hardening Outcomes

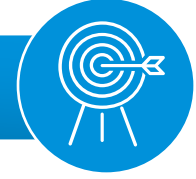
Improved access controls



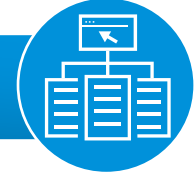
Strengthened network security



Reduced attack surfaces



Better performance

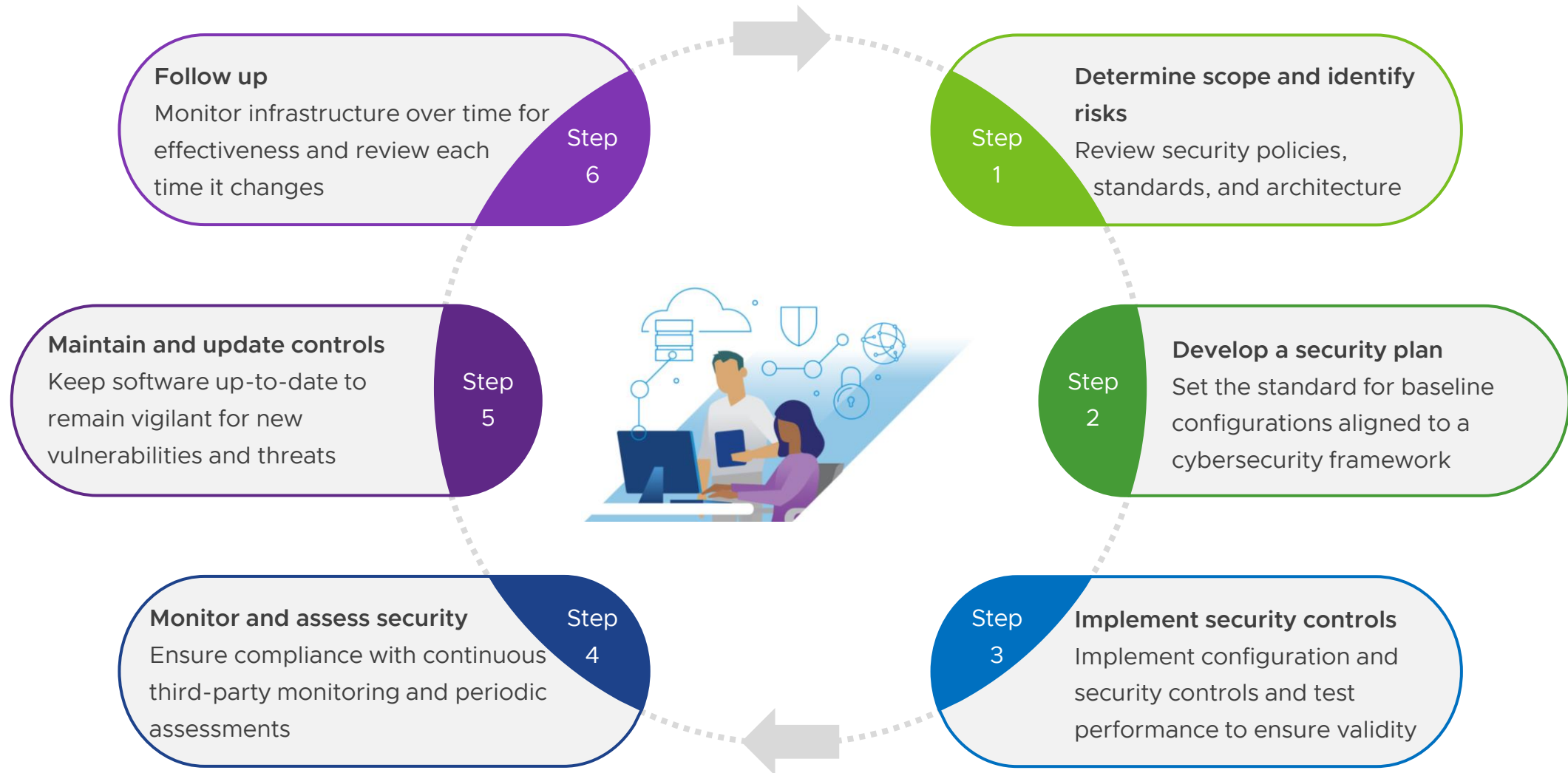


Simplified compliance

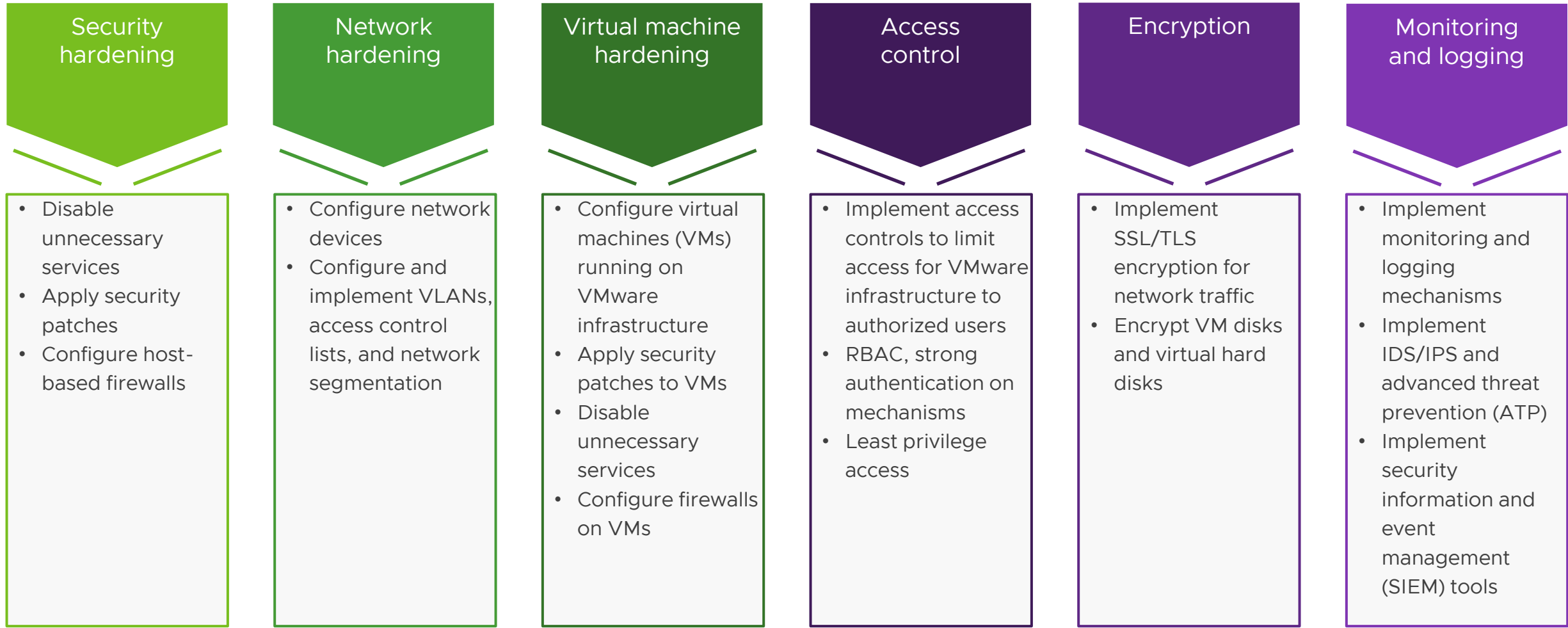


The Hardening Process

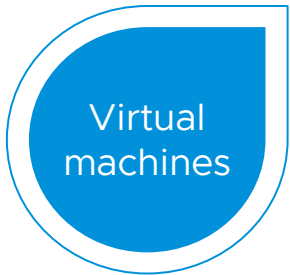
High-level process to help achieve the desired future state



Best Practices for Security Hardening



VMware vSphere® Hardening Best Practices Checklist



- UEFI secure boot
- Removable device controls
- Minimize use of VM console
- Deactivate host-guest file system (HGFS)
- Disable copy and paste, drag and drop
- Restrict API access
- vMotion encryption



- UEFI secure boot
- Enable lockdown mode
- Disable SSH
- VIS acceptance levels
- Disable SLP
- CIM access levels
- Host firewall
- Disable SNMP



- Management session restrictions
- Disable managed object browser
- Restrict cryptographic role and permissions
- SSO account alerting and restrictions
- Enable TLS 1.2
- Power CLI restrictions
- VMware vCenter server firewall
- Use approved certificates
- Use templates to deploy VMs
- Use SNMP v3



- vMotion network isolation
- ESXi management isolation
- VMware vSphere web client isolation
- Isolate virtual machine traffic

Hardening practices for all areas and products



Patch currency

- Install latest security patches and updates

Identity and access management

- Disable default accounts
- Change default passwords
- RBAC
- Centralized authentication
- Multi-factor authentication
- Single sign-on account lockout
- Unique services accounts

Remote logging

- Enable logging to appropriate levels
- Forward logs to centralized log collector
- Limit access to logs

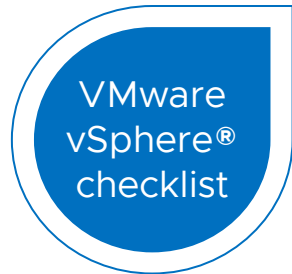
Monitoring

- VMware Aria™
- VMware vCenter server alerts
- Third-party tool

Backups

- Ensure environment is backed up

VMware Cloud Foundation™ Hardening Best Practices Checklist



- ❑ All items on VMware vSphere hardening checklist (previous slide) for virtual machines, ESXi hosts, VMware vCenter, and virtual network



- ❑ VMware NSX (formerly VMware NSX-T™ Data Center) deployment protocol and port requirements
- ❑ VMware NSX® Manager™ appliance deployment
- ❑ VMware NSX® Edge™ appliance deployment
- ❑ NSX logs and alerting*

* More details on VMware NSX hardening checklist



- ❑ VMware vSAN network isolation
- ❑ Enable VMware vSAN encryption



- ❑ VMware Cloud Foundation SDDC Manager isolation
- ❑ Use approved certificates
- ❑ Use dedicated account for updates and patches
- ❑ Deploy with FIPS mode enabled
- ❑ Schedule automatic password rotation

Hardening practices for all areas and products



Patch currency

- ❑ Install latest security patches and updates

Identity and access management

- ❑ Disable default accounts
- ❑ Change default passwords
- ❑ RBAC
- ❑ Centralized authentication
- ❑ Multi-factor authentication
- ❑ Single sign-on account lockout
- ❑ Unique services accounts

Remote logging

- ❑ Enable logging to appropriate levels
- ❑ Forward logs to centralized log collector
- ❑ Limit access to logs

Monitoring

- ❑ VMware Aria™
- ❑ VMware vCenter server alerts
- ❑ Third-party tool

Backups

- ❑ Ensure environment is backed up

VMware NSX® Hardening Best Practices Checklist

Protocols and Port Requirement

- Follow TCP/UDP port guidelines
- Block unneeded ports
- Disable unneeded network services

VMware NSX® Manager™ (Management Plane)

- VMware NSX Manager isolation
- VMware NSX® Controller™ isolation
- VMware NSX transport node isolation
- Management session restrictions
- SSH access to NSX Manager disabled
- Ensure that NTP server is authorized
- Do not install/use software unsupported by VMware
- Use SFTP for backup and restoration
- Hardening IAM policies in NSX cloud service environment
- Set NSX Manager WEB/API access using only TLS 1.2
- Disable SNMP v2
- Use approved certificates

VMware NSX Edge™ (Data Plane)

- Block access to ports not used on data plane
- Segment management and data traffic
- Isolate storage network from other networks
- Disable secure shell
- Isolate virtual network tunnel traffic (Geneve)

VMWare NSX® Certificates

- Ensure that NSX Manager certificate is valid and legitimate
- Leverage VMware NSX® Edge™ certificates and cipher suites (load balancer, IPSec, and VPN)
- User access to NSX Manager using own certificate authority

VMware NSX® Distributed Firewall™

- Implement micro-segmentation with NSX Distributed Firewall
- Implement NSX Distributed Firewall with Threat Prevention
- Implement NSX Distributed Firewall with VMware NSX® Advanced Threat Prevention™

VMware NSX® Gateway Firewall™

- Enforce security policies
- Implement NSX Gateway Firewall with Threat Prevention
- Implement NSX Gateway Firewall with Advanced Threat Prevention



Hardening practices for all areas and products



Hardening Resources on VMware.com

VMware Hardening Guides

These guides provide prescriptive guidance for customers on how to deploy and operate VMware products in a secure manner. Find them at <https://www.vmware.com/security/hardening-guides.html>.

VMware Cloud Foundation™ Compliance Kits

These kits help customers meet regulatory requirements by bridging the gap between compliance frameworks and implementation guides. Find them at <https://core.vmware.com/compliance#cloud-foundation>.

Secure Technical Implementation Guides

VMware supports the mission of the U.S. Department of Defense through security technical implementation guides – a collaborative effort between VMware and the Defense Information Systems Agency. Find them at <https://core.vmware.com/stigs>.

Product Audit and Applicability Guides

Implementation guides to assist administrators in implementing security controls for a specific compliance framework as well as helping auditors understand how product security controls apply to regulatory requirements. Find them at <https://core.vmware.com/compliance>.

VMware NSX® Firewall Ports and Protocols

This is a complete list of ports required for VMware products to be able to create dynamic lists based on the VMware products in your environment. Find them at <https://ports.esp.vmware.com>.

VMware Security Advisories

Stay up-to-date on the latest VMware security advisories and updates. Find them at <https://www.vmware.com/security/signup-for-advisories.html>.

Q & A



Please take
your survey.



Let's Keep Talking

vmware® **EXPLORE**

Attend additional sessions in the CXS Theater in The Hub

Stop by the Customer Experience and Success kiosk in the VMware booth in the Expo

Get *Social* with us

