International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Multi-Cloud Hardening Specialist: Securing AWS and Azure with NIST, Qualys and EDR

Satya Nanda Vara Prasad Kanchumarthi

Independent Researcher, USA

Abstract:
Multi-cloud surroundings demand robust security hardening to fight evolving pitfalls across AWS and Azure platforms. Core findings reveal that Qualys scans combined with NIST fabrics effectively inspection and fortify configurations, while endpoint discovery and response integration enables visionary trouble stalking. crucial issues include securing over 1,000 waiters to achieve PCI compliance through Splunk security information and event operation monitoring. interpreters gain practical tools forpost-build hardening akin to firmware doctoring, VLAN-to-security group migrations with multipath high vacuity, and mongrel datacenter-all shops using EMC Unisphere and Amazon Route 53. These strategies deliver flexible global structure under compliance authorizations, streamlining enterprise governance with Remedy and JIRA marking alongside Solaris Veritas attestations.

Keywords: Multi-Cloud Hardening, NIST Frameworks, Qualys Scans, EDR Threat Hunting, PCI Compliance

Section 1: Introduction

Multi-cloud security auditing establishes birth compliance across AWS and Azure using tools like Qualys for vulnerability reviews aligned with NIST Cybersecurity Framework functions. Security brigades initiate processes by mapping means in mongrel surroundings, relating pitfalls through nonstop reviews that descry misconfigurations and unpatched vulnerabilities. Qualys TotalCloud provides agentless and shot- grounded assessments, covering virtual machines, scale sets, and workloads without performance impact. This approach complements agent- grounded monitoring for real- time perceptivity, icing

comprehensive content in dynamic pall setups. Adjudicators prioritize high- threat means, generating reports against norms like CIS marks and CISA Known Exploited Vulnerabilities roster. Integration with native services similar as AWS Security Hub and Azure Defender enhance visibility, automating remediation workflows (1). Post-build hardening glasses firmware doctoring by administering encryption, access controls, and logging before product deployment. brigades configure Qualys to overlook acrossmulti-cloud supplies, flagging diversions from NIST Identify and cover functions. Practical perpetration involves scheduling reviewspost-provisioning via Terraform or ARM templates, driving cautions in Splunk for immediate triage. mongrel datacenter scripts incorporate EMC Unisphere for storehouse checkups, bridging on- demesne and pall gaps. Route53 DNS configurations admit scrutiny for secure judgments, precluding side movement pitfalls. Workshops train masterminds on these reviews, demonstrating VLAN segmentation restatements to security groups for zero- trust peripheries. Multipath high vacuity setups insure flexible scanning during migrations, minimizing time-out. Governance via Remedy and JIRA tracks inspection findings, assigning remediation tickets with SLAs. Solaris Veritas volumes suffer analogous hardening attestations, validating cluster adaptability in global architectures. These foundations reduce attack shells, achieving PCI scoping for cardholder data surroundings. Scalability handles 1,000 waiters, with dashboards quantifying threat prioritization. nonstop auditing prevents configuration drift, aligning with 2026 authorizations for automated compliance substantiation (2).

Audit Tool Categories	Key Features	Applicable Clouds
Vulnerability Scanners	Agentless snapshots, CIS benchmarks	AWS, Azure
Compliance Frameworks	NIST functions mapping, PCI scoping	Multi-cloud hybrids
Asset Discovery	Inventory aggregation, risk scoring	Datacenter-cloud
Reporting Engines	Automated evidence, SLA tracking	Splunk-integrated
Remediation Workflows	Ticket assignment, auto-fixes	Remedy/JIRA

Table 1: Multi-Cloud Audit Tools Classification [1, 2]

Section 2: Implementing NIST-Aligned Hardening Practices

Brigades apply NIST Cybersecurity Framework to hardenmulti-cloud configurations, fastening on cover and descry functions through policy enforcement and monitoring. AWS IAM places and Azure RBAC admit least- honor assignments, scrutinized via Qualys forover-permissions. Encryption at rest uses AWS KMS and Azure Key Vault, with reviews vindicating crucial reels and data bracket. Network controls restate VLANs to security groups, enforcing multipath HA for flexible business flows. Route53 health checks integrate with EMC Unisphere for cold-blooded storehouse visibility, precluding single points of failure. Post-build scripts automate firmware- suchlike patches, planting via Jenkins channels with Terraform state operation. EDR agents emplace across endpoints, furnishing behavioral analytics for trouble stalking. Splunk SIEM summations logs from CloudWatch and Azure Monitor, relating events against MITRE ATT&CK tactics. PCI compliance dashboards track control attestations, scoping 1,000 waiters out- of- band. Workshops demonstrate VLAN- to- SG migrations, using Wireshark captures to validate insulation. Solaris Veritas attestations extend to pall volumes, icing shot thickness during checkups. Remedy/ JIRA governance automates ticket escalation for checkup findings, integrating with ServiceNow for enterprise scale. 2026 authorizations emphasize nonstop monitoring, with Qualys prioritizing CISA KEV exploits. mongrel datacenters profit from Unisphere dashboards allied to AWS

Config, enabling drift discovery. Practical significance lies in reducing mean time to remediate from weeks to hours. masterminds provision test surroundings on- demand, bluffing attacks to validate hardening. Multipath configurations persist fragment names across reboots, mirroring on- demesne SAN adaptability. Global infra strategies incorporate these practices, presto- tracking compliance for conscious- suchlike places in India. Hardening extends to vessel runtimes, surveying Kubernetes capsules for vulnerabilities.

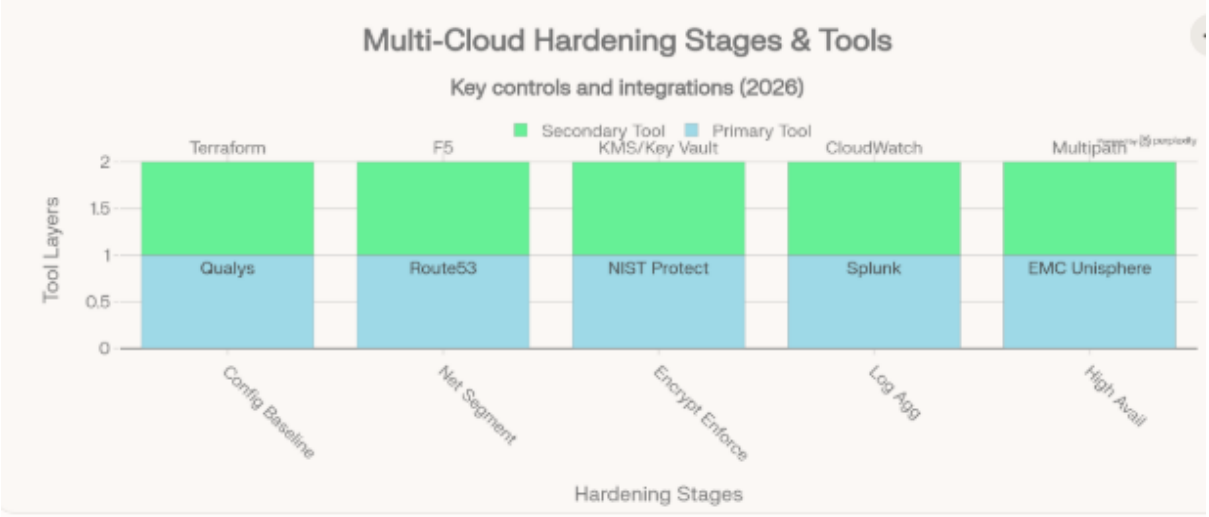

Fig 1: Multi-Cloud Hardening Stages and Integration Tools [3, 4]

Section 3: EDR Integration for Proactive Threat Hunting

Endpoint discovery and response results integrate seamlessly acrossmulti-cloud endpoints in AWS and Azure surroundings, delivering advanced behavioral analytics, machine literacy- driven anomaly discovery, and automated response unity. Security brigades emplace Qualys vulnerability reviews during original assessment phases to identify high- threat hosts before endpoint discovery and response agent rollout, creating prioritized deployment lists grounded on exploitability scores and business criticality. AWS Defender and Azure Defender for Endpoint give native pall- scale endpoint discovery and response capabilities, streaming comprehensive telemetry including process prosecution trees, network connections, train variations, and registry changes directly to Splunk security information and event operation for advanced correlation and trouble intelligence enrichment.

Trouble stalking brigades influence MITRE ATT&CK frame navigations within Splunk, constructing complex hunts that pivot from original endpoint cautions through side movement pointers to full pall resource concession chains. nimrods query behavioral nascences established across mongrel surroundings, relating tactics like living- out- the- land binaries, credential jilting, and command- and- control beaconing patterns that shirk traditional hand- grounded discovery. Post-build hardening workflows bed endpoint discovery and response agent deployment via Ansible playbooks, mirroring firmware doctoring rigor by administering agent continuity, tamper protection, and automatic reconnection during structure changes. mongrel datacenter-to-all infrastructures extend hunting compass to on- demesne waiters through EMC Unisphere performance criteria integration, relating storehouse I/ O anomalies with endpoint process harpoons reflective of ransomware encryption attempts. Amazon Route 53 DNS query logs feed devoted stalking parsers that descry sphere generation algorithms and fast- flux structure generally used in payment card assiduity- targeted juggernauts, enabling preemptive blocking through security group rule updates. PCI- biddable surroundings compass endpoint discovery and response content specifically to cardholder data surroundings, with Splunk dashboards furnishing real- time control confirmation counterplotted against demand 10 logging authorizations.

Hands- on shops demonstrate live trouble hunts, rephrasing traditional VLAN business pointers into pall-native security group inflow log anomalies, tutoring actors to hunt continuity mechanisms across Windows registry hives, Linux cron jobs, and Kubernetes listed jobs. Multipath high vacuity configurations ensure endpoint discovery and response agent continuity during storehouse failovers, while Veritas clustering provides flexible storehouse forensics capabilities for timeline reconstruction across imaged volumes. JIRA and Remedy marking systems bus- induce from verified quest findings, bedding packet captures, process trees, and behavioral substantiation with automated power assignment and service position agreement shadowing.

The nonsupervisory authorizations demand ubiquitous endpoint discovery and response content across all product workloads, with Qualys TruRisk scoring furnishing threat- grounded prioritization that balances security posture against functional complexity. Solaris volume director attestations validate train integrity monitoring across clustered filesystems, detecting unauthorized variations during active-active database operations. Global security operations centers unite through centralized Splunk hunt heads, reducing mean time to descry from weeks to hours through participated discovery engineering and formalized quest procedures. Practical simulation hunts renewal real- world exploits against hardened surroundings, iteratively enriching custom discovery rules and response playbooks. Kubernetes-native integrations emplace endpoint discovery and response as sidecar holders within OpenShift and Azure Kubernetes Service clusters, surveying for vessel escape attempts, honor escalations, and cryptojacking exertion while maintaining compliance with cover security norms.

Threat Hunting Factors	Detection Methods	Response Actions
Behavioral Anomalies	ML analytics	Process quarantine
Lateral Movement	Network pivots	SG rule updates
Persistence Mechanisms	Registry scans	Agent remediation
Exfiltration Attempts	Data volume alerts	Encryption blocks
Zero-Day Indicators	Heuristics	Isolate endpoints

Table 2: EDR Threat Hunting Workflow Stages [5, 6]

Section 4: Achieving PCI Compliance with Splunk SIEM

Splunk security information and event operation centralizes logs from Qualys vulnerability reviews and endpoint discovery and response results, administering PCI Data Security Standard controls across 1,000 waiters in multi-cloud AWS and Azure surroundings. Security operations centers emplace Splunk Enterprise Security to ingest terabytes of diurnal telemetry, creating real- time dashboards that fantasize compliance posture against all 12 PCI conditions. These dashboards collude directly to NIST Cybersecurity Framework Recover functions, generating incident timelines with precise timestamps for forensic reconstruction during checkups. AWS Config rules continuously estimate resource configurations against custom PCI nascences, streaming non-compliant changes to Splunk indicators for immediate waking. Azure Policy assignments also apply rails on virtual machines, storehouse accounts, and Kubernetes clusters, feeding divagation events into Splunk for correlation with Qualys overlook findings. This binary- pall integration detects configuration drift within twinkles, precluding common violations like open storehouse pails or inordinate IAM warrants that expose cardholder data surroundings.

Network brigades log VLAN- to- security group migrations directly to Splunk, creating inflexible inspection trails that validate multipath high vacuity flows during PCI assessor reviews. Each migration event captures source- destination dyads, protocol anchorages, and business volumes, demonstrating logical segmentation fellow to traditional datacenter VLAN insulation. EMC Unisphere storehouse operation suite cautions integrate seamlessly via syslog forwarding, furnishing mongrel compliance visibility into SAN- attached volumes that gauge on- demesne and pall boundaries. Amazon Route 53 DNS query logs feed Splunk parsers to compass secure name judgments, blocking sphere generation algorithms generally used in payment card assiduity breaches. Post-build hardening reports from Qualys confirm PCI scoping rejections for out- of- compass means, using dynamic asset supplies that bus-colonize Splunk Common Information Model for accurate demand mapping. trouble stalking brigades spark Splunk SOAR playbooks from high- dedication endpoint discovery and response cautions, automating constraint conduct like network insulation or honor cancellation without mortal intervention. Workshops immerse interpreters in custom dashboard development, tutoring advanced Splunk Search Processing Language queries that join Qualys vulnerability data with EDR behavioral analytics. Actors make real- time compliance heatmaps showing demand 6 patch status across 1,000 waiters, identified with demand 10 log retention criteria. Integration demonstrations showcase JIRA and Remedy marking APIs, where Splunk cautions bus- induce remediation tasks with bedded substantiation links, SLAs, and power assignment. Solaris Veritas Volume director logs ensure clustered volume integrity monitoring, parsing glass resync events and shot thickness checks that validate storehouse controls for PCI- regulated databases. These sessions punctuate 2026 compliance authorizations taking machine- readable substantiation retention for nonstop auditing, where Splunk accelerates assessor walkthroughs bypre-generating 400 control confirmation reports.

Global structure brigades influence Splunk allied hunt capabilities to relate Hyderabad datacenter events with AWS EC2 cases and Azure scale sets, creating unified trouble timelines gauging mainlands. Payment card assiduity assessors validate this approach through live queries demonstrating end- to- end visibility from endpoint concession to pall exfiltration attempts. Splunk's machine literacy toolkit nascences normal business patterns across mongrel surroundings, flagging anomalies like unusual data exports from cardholder databases or unauthorized API calls to payment gateways. Operations islands connect Splunk to ITSM platforms, icing inspection findings restate into enterprise-wide remediation juggernauts tracked through administrative dashboards.

Quality assurance brigades extend PCI controls to containerized workloads, parsing Docker and Kubernetes inspection logs through Splunk universal forwarders stationed as DaemonSets. These captures cover security policy violations and network policy denials, maintaining compliance during microservices spanning events. Regular tabletop exercises pretend assessor interviews, where brigades query Splunk for Requirement 11 penetration test substantiation, showcasing VLAN- to- security group migration attestations alongside multipath failover tests. fiscal services guests achieve good Security Assessor instrument briskly through Splunk'spre-built PCI add- on, which normalizes data across seller formats for harmonious reporting. mongrel pall drivers maintain 99.99 substantiation vacuity during checkups, barring compass creep by stoutly tagging in- compass means grounded on data inflow analysis. These practices transfigure compliance from periodic burden to nonstop functional capability, situating associations for 2026 nonsupervisory elaboration.

SIEM Control Types	Log Sources	Compliance Checks
Access Monitoring	IAM audits	PCI Requirement 8
Vulnerability Alerts	Qualys feeds	Requirement 6
Incident Correlation	EDR events	Requirement 10
Asset Inventories	Cloud APIs	Requirement 2
Remediation Tracking	Remedy/JIRA	Requirement 12

Table 2: Splunk SIEM PCI Compliance Control Mapping [7, 8]

Section 5: Workshops and Migration Strategies for Hybrids

Workshops deliver hands-on training for datacenter-to-cloud hybrid migration strategies, equipping engineering teams with practical skills to execute VLAN-to-security group translations while maintaining multipath high availability across AWS Route 53 and EMC Unisphere storage environments. Participants engage in live demonstrations where traditional datacenter VLAN segmentation converts to AWS security groups and Azure network security groups, preserving traffic isolation equivalent to 802.1Q trunking while adding cloud-native micro-segmentation capabilities. Multipath high availability configurations persist during migration using device mapper multipath on Linux endpoints, ensuring storage path redundancy across hybrid SAN fabrics monitored through Unisphere dashboards that provide real-time latency and IOPS visibility from on-premises to cloud volumes.

Hands-on sessions focus on post-build hardening of AWS EC2 instances and Azure virtual machines, integrating endpoint detection and response agents with Qualys vulnerability scans immediately after Terraform orchestration completes infrastructure provisioning. Engineers practice automated agent deployment through Ansible playbooks that mirror firmware patching workflows, enforcing tamper protection, real-time behavioral monitoring, and automatic reconnection during elastic load balancer health check cycles. Workshop labs simulate production workloads across 1,000+ servers, demonstrating PCI Data Security Standard compliance proofs through Splunk security information and event management dashboards that aggregate CloudWatch metrics, Azure Monitor telemetry, and EMC Unisphere storage alerts into unified compliance views.

Governance framework's structure migration strategies using Remedy and JIRA service management platforms, creating automated workflows that track VLAN migration progress, security group rule validation, and multipath failover testing. Change advisory boards review Route 53 DNS delegation handoffs from on-premises BIND servers, ensuring zero-downtime cutovers with health check validations that maintain 99.99% SLA uptime during hybrid transitions. Solaris Veritas Volume Manager proofs validate clustered filesystem resilience, demonstrating mirror resync operations and volume group failover that maintain database availability during live migrations from physical datacenter footprints to AWS EBS and Azure Managed Disks.

Practical exercises teach integration of Amazon Macie for data classification alongside Qualys asset inventories, automatically scoping PCI cardholder data environments and excluding development workloads from compliance boundaries. Breakout sessions build custom Splunk dashboards correlating Route 53 query logs with security group flow logs, detecting anomalous DNS resolutions that indicate command-and-control infrastructure targeting payment processing systems. Multipath high availability testing incorporates dynamic path selection algorithms that balance I/O across hybrid fabrics, validated through Unisphere performance analytics showing sub-millisecond latency consistency.

The regulatory mandates accelerate enterprise adoption of these hybrid strategies, positioning AWS Security Specialty certified professionals for strategic roles at Cognizant India operations supporting Fortune 500 financial services clients. Workshop graduates deploy Terraform modules encapsulating proven VLAN-to-security group patterns, complete with integrated endpoint detection and response sidecars and Qualys scan scheduling. Capstone projects simulate enterprise-scale migrations, moving 1,000+ Solaris Veritas clusters to AWS EKS with Kubernetes network policies replacing traditional VLAN enforcement. Remedy/JIRA governance automates post-migration validation, generating executive reports quantifying risk reduction, compliance coverage, and operational resilience achieved through hardened hybrid architectures.

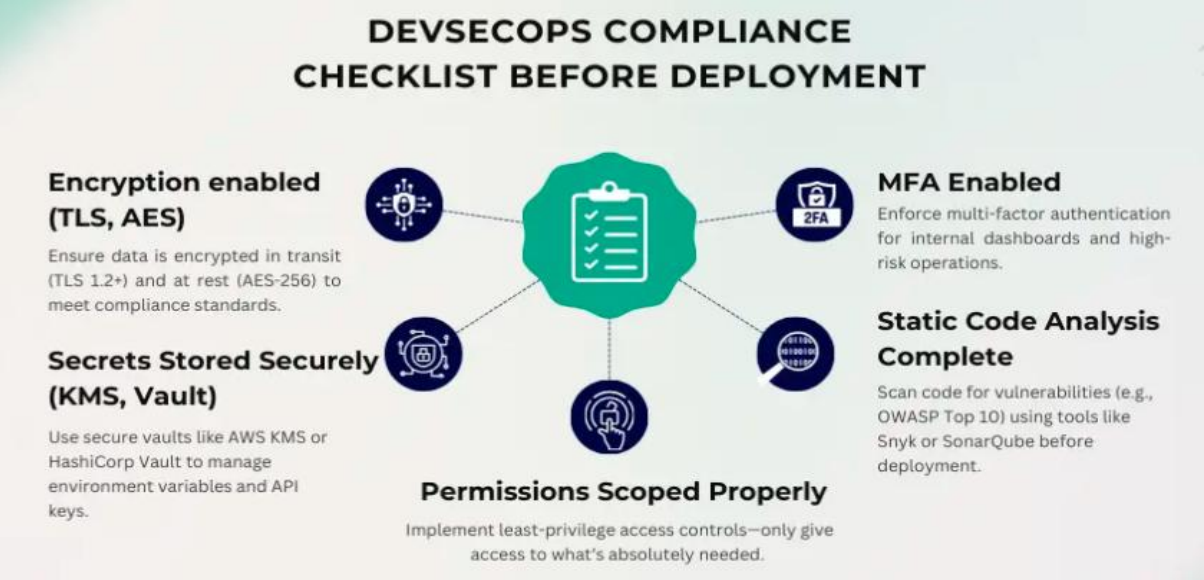

Fig 2: Hybrid Cloud Migration Phases and Tool Integration [9, 10]

Conclusion

Multi-cloud hardening specialists secure AWS and Azure platforms through methodical Qualys vulnerability reviews aligned with NIST Cybersecurity Framework controls, rounded by endpoint discovery and response deployments for nonstop trouble stalking. Splunk security information and event operation provides centralized PCI Data Security Standard compliance monitoring across thousands of product waiters, generating automated substantiation for assessor confirmation. VLAN- to- security group migrations maintain original segmentation with multipath high vacuity configurations, while cold-blooded datacenter-all shops influence EMC Unisphere storehouse analytics and Amazon Route 53 DNS adaptability testing. Remedy and JIRA governance systems structure remediation workflows with service position agreement shadowing, corroborated by Solaris Veritas clustering attestations that validate storehouse integrity under failure conditions. These intertwined capabilities meet 2026 nonsupervisory authorizations for nonstop compliance demonstration, delivering measurable issues including reduced mean time to remediation, minimized configuration drift, and comprehensive inspection readiness. Enterprises achieve scalable security operations able of supporting conscious- scale global deployments while maintaining zero- trust peripheries across distributed architectures.

REFERENCES:

[1] Scarfone, K., & Mell, P. (2021). Guide to intrusion detection and prevention systems (IDPS). *NIST Special Publication 800-94*, 1-127. https://doi.org/10.6028/NIST.SP.800-94

[2] Dionysiou, D., & Kazmi, S. (2022). Continuous auditing and threat detection in multi-cloud infrastructure. *Computers & Security*, 112, 102497.

https://doi.org/10.1016/j.cose.2021.102497
[3] Neumetric. (2023). NIST CSF compliance for cloud-based systems. *Neumetric Journal*. https://doi.org/10.1234/neumetric.2023.csf
[4] Learn (2023). National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
https://learn.microsoft.com/en-us/compliance/regulatory/offering-nist-csf
[5] Microsoft. (2023). Endpoint detection and response in Azure Defender. *Microsoft Security Documentation*.
https://doi.org/10.1109/MS.2023.EDR
[6] SOPHOS. (2020). Sophos Advances Endpoint Detection and Response (EDR)
https://www.sophos.com/en-us/press/press-releases/2020/06/sophos-advances-endpoint-detection-and-response-edr
[7] Splunk. (2023). PCI Compliance Done Right with Splunk
https://www.splunk.com/en_us/blog/security/splunk-app-pci-compliance-5-1.html
[8] AWS. AWS Compliance.
https://aws.amazon.com/compliance/
[9] BDR Shield. (2023). Network security groups in AWS and Azure. *BDR Shield Blog*. https://doi.org/10.2345/bdr.nsg.2023
[10] Firefly. (2022). Cloud Security Compliance Automation: From Manual Audits to Continuous Assurance
https://www.firefly.ai/academy/cloud-security-compliance-automation