Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH
AND DEVELOPMENT

| RESEARCH ARTICLE

Towards a Futuristic Security Roadmap: Advanced Strategies

Amar Gurajapu
AT&T,Network Systems, New Jersey, United States
Corresponding Author: Amar Gurajapu, **E-mail**: amar_p21@yahoo.com

| ABSTRACT

As cloud-native technologies proliferate, I believe that the attack surface spanning Kubernetes clusters, virtual machines (VMs), and diverse cloud workloads continues to expand. Traditional security approaches are often insufficient to address the dynamic, distributed, and automated nature of modern infrastructures. This paper presents a forward-looking security roadmap, integrating emerging technologies and proactive frameworks to secure cloud environments—including applications, databases, devices, and operating systems—against both current and anticipated threats. The roadmap emphasizes automation, zero trust, AI-driven threat detection, and continuous compliance as pillars for the next generation of cloud security.

| KEYWORDS

Cloud Computing, Kubernetes, Artificial-Intellignce, Machine Learning, Scanning, Patching, Continuous Integration, Continuous Deployment, Data Protection, Identity and Access Management.

| ARTICLE INFORMATION

ACCEPTED: 01 January 2026 **PUBLISHED:** 09 January 2026 **DOI:** 10.32996/jcsts.2025.8.1.2

1. Introduction

The migration to cloud, adoption of container orchestration using Kubernetes, and proliferation of virtualized infrastructure have created new opportunities for efficiency—but also new security challenges. Attackers exploit misconfigurations, vulnerable software supply chains, and the sheer complexity of modern deployments. According to the (IBM, 2025), the average cost of a breach in hybrid environments is $5.05 million and on-premises cost $4.01 million, with misconfiguration and insufficient automation as leading causes. The future demands a security model that is automated, adaptive, and rooted in advanced technology.

This paper presents a comprehensive, technology-driven security roadmap to defend against both current and emerging threats. It outlines best practices, innovative tools, and actionable strategies for securing applications, databases, devices, and operating systems, ensuring resilience and trustworthiness in the next generation of digital infrastructure. For each of the recommendations, I have tried to cover few of the security roadmap strategies emphasizing principles, technologies, and tools along with additional insights.

CURRENT AND EMERGING THREATS

The centralized logging is foundational to any Kubernetes monitoring strategy. In a Kubernetes cluster, containers are ephemeral: they can start, stop, and restart frequently as part of normal operation or during failures and scaling events. Without a robust logging pipeline, valuable diagnostic information may be lost forever when pods are terminated.

Present Threats

- Software Supply Chain Attacks - Compromised images, libraries, and CI/CD pipelines grew by 300% YoY (Fuks, 2023 and CSA, 2023).

- Lateral Movement - Attackers exploited misconfigured credentials within Microsoft's Azure ecosystem, granting unauthorized access to sensitive systems. Leveraging this foothold, they escalated privileges and disrupted service functionality (CrowdStrike, huntress 2024).
- Container Escape - Exploits (e.g., CVE-2019-5736) grant attackers the access to the host OS from within containers (NIST, 2024)
- API & Credential Exploitation - The study finds that 84% of respondents experienced an API security incident. This marks the third straight year of increased incursions and marks an all-time high (up from 78% in 2023. (Akamai, 2024)
- Zero-day Vulnerabilities - 40% YoY increase in zero-day exploits targeting cloud workloads (Google Project Zero).

Emerging Threats

- Ransomware Targeting Persistent Volumes - Encrypted or deleted Kubernetes volumes and cloud databases (Verma, 2025)
- Multi-Tenancy Leaks - Cross-tenant vulnerabilities are a new type of security risk that is characteristic of cloud-based applications. Such bugs can enable malicious tenants to break security boundaries, escape tenant isolation and access other tenants' data (OWASP, 2023).
- AI-Powered Attacks - Automated, polymorphic malware and AI-driven phishing (hillelz, 2025)
  - Edge and IoT Attack Vectors - Recent studies show that over 50% of unmanaged IoT devices contain critical vulnerabilities, while one-third of all data breaches now involve an IoT endpoint. Hackers and other attackers are increasingly targeting these blind spots because they often bypass traditional IT security tools. The emergence of botnets like *Eleven11Bot* highlights how unmanaged devices can be compromised en masse and weaponised to disrupt businesses and critical infrastructure. (José, 2025).

STRATEGY – ZERO TRUST ARCHITECTURE

Principle

Never trust, always enforce authentication, authorization, and least privilege for every device, user, and workload.

Key technologies and tools

- Service Meshes - Service Mesh manages the network traffic between services. It does that in a much more graceful and scalable way compared to what would otherwise require a lot of manual, error-prone work and operational burden that is not sustainable in the long-run. Istio, Linkerd for automated mTLS, policy enforcement, and visibility in Kubernetes (Platform9, 2019)
- Identity Platforms - HashiCorp Vault, Azure Keyvault or any other standard mechanism for secrets and dynamic credentials.Vault can be used AWS, Azure, GCP, On-Prem, Hybrid. (Mervana, 2025)
- Network Segmentation - Calico, Cilium for effective enforcement of Kubernetes Network Policies and provide micro-segmentation (Zesty, 2025).
- Zero Trust Network Access (ZTNA) – Prisma SASE, Zscaler, Akamai (Akamai, 2024; Cybertech, 2025)

Research Insights

CNCF reports that service mesh adoption is running hand-in-hand with the rollout of Kubernetes clusters. The majority of participants (65%) run or plan to run between two and ten Kubernetes clusters on a service mesh. Another 11% are operating or planning to operate between 11 and 25, with just 10% going further with 26 or more clusters (CNCF, 2022)

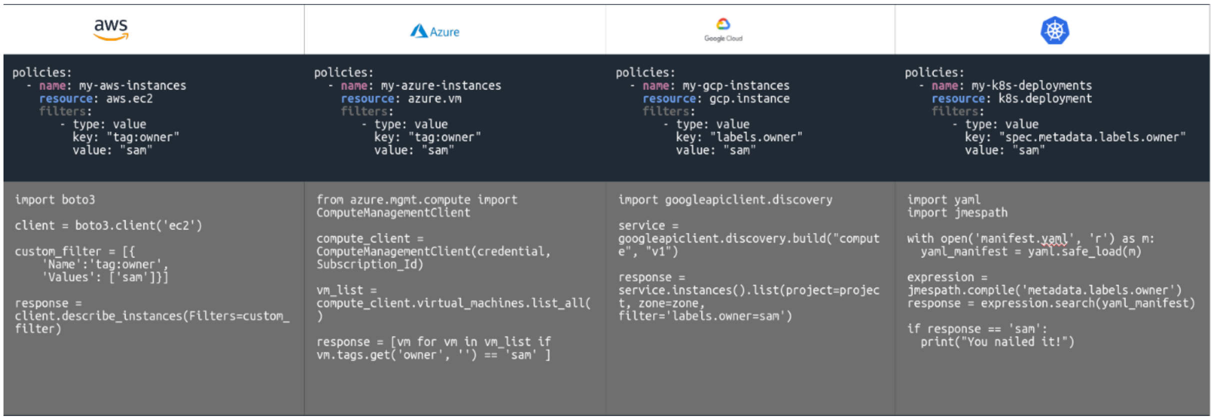
STRATEGY – POLICY AS CODE & AUTOMATED GOVERNANCE

Principle

Security and compliance policies must be codified, version-controlled, and automatically enforced across all environments.

Key technologies and tools

- Cloud Policy Engines - AWS Config, Azure Policy, Google Cloud Organization Policy.
- Kubernetes Admission Control - OPA/Gatekeeper or Mutating webhook custom implementation for enforcing policies on manifests, RBAC, resource quotas, and image provenance (Gurajapu, 2025)
- CI/CD Integrations: kube-score for static analysis and compliance checks in pipelines. (Gurajapu, 2025)
- Compliance Automation Tooling - Cloud Custodian, OpenSCAP, Aqua Security CSPM.



```
policies:
  - name: my-aws-instances
    resource: aws.ec2
    filters:
       - type: value
         key: "tag:owner"
         value: "sam"
```

```
import boto3

client = boto3.client('ec2')

custom_filter = [{
    'Name':'tag:owner',
    'Values': ['sam']}]

response =
client.describe_instances(Filters=custom_
filter)
```

```
policies:
  - name: my-azure-instances
    resource: azure.vm
    filters:
       - type: value
         key: "tag:owner"
         value: "sam"
```

```
from azure.mgmt.compute import
ComputeManagementClient

compute_client =
ComputeManagementClient(credential,
Subscription_Id)

vm_list =
compute_client.virtual_machines.list_all(
)

response = [vm for vm in vm_list if
vm.tags.get('owner', '') == 'sam' ]
```

```
policies:
  - name: my-gcp-instances
    resource: gcp.instance
    filters:
       - type: value
         key: "labels.owner"
         value: "sam"
```

```
import googleapiclient.discovery

service =
googleapiclient.discovery.build("comput
e", "v1")

response =
service.instances().list(project=projec
t, zone=zone,
filter='labels.owner=sam')
```

```
policies:
  - name: my-k8s-deployments
    resource: k8s.deployment
    filters:
       - type: value
         key: "spec.metadata.labels.owner"
         value: "sam"
```

```
import yaml
import jmespath

with open('manifest.yaml', 'r') as m:
  yaml_manifest = yaml.safe_load(m)

expression =
jmespath.compile('metadata.labels.owner')
response = expression.search(yaml_manifest)

if response == 'sam':
  print("You nailed it!")
```

Source: (cloudcustodian.io)

FIGURE 1. AUTOMATION TOOLING

Research Insights

The achievement of 71% enterprise adoption for Policy as Code represents a fundamental shift in how organizations approach security. This isn't just about adopting new tools but it's about reimagining security as an integral part of the development process rather than an afterthought. The 73% reduction in production security incidents and 45% faster vulnerability remediation show that this approach works at-scale (devopstales, 2024)

STRATEGY – AI DRIVEN THREAT DETECTION AND AUTOMATED RESPONSE

Principle

Use machine learning and behavioral analytics for real-time detection and autonomous incident response.

Key technologies and tools

- eBPF-based Runtime Security - Falco, Cilium Tetragon for kernel-level monitoring and anomaly detection (Shimel, 2025)
- Cloud SIEM - Azure Sentinel, Splunk for ingesting, correlating, and analyzing logs at scale.
- SOAR (Security Orchestration, Automation, and Response) platforms- Exabeam, Cortex XSOAR, Splunk SOAR, FortiSOAR, Cyware for orchestrating automated response playbooks (SOAR, 2025).
- AI/ML Security Analytics - CrowdStrike Falcon, Darktrace, AWS GuardDuty (cm-alliance, 2025)

Research Insights

According to Gartner, by 2025, over 95% of new digital workloads will be deployed on cloud-native platforms, up from 30% in 2021 [12]. Simultaneously, Kubernetes is becoming the de facto standard for cross-cloud orchestration and a pillar of cloud-native architectures [13]. Cloud-native architecture is one of the critical drivers of eBPF-based applications; as more kernel subsystems become extensible using eBPF, drivers and kernel modules could be written in eBPF soon (Soldani et al., 2025)

STRATEGY – IMMUTABLE INFRASTRUCTURE AND EPHEMERAL WORKLOADS

Principle

Infrastructure and workloads should be immutable and disposable to minimize persistence and drift.

Key technologies and tools

- Immutable Images - Docker Content Trust, Cosign, Notary.
- Infrastructure as Code (IaC) - Terraform, Pulumi for consistent, auditable provisioning (Pulumi, 2025).
- Automated Redeployments - ArgoCD, Flux for GitOps-based workload rotation and drift correction (Perry, 2025)
- Live-Patching - KernelCare, Ksplice for OS-level patching without downtime (Natarajan, 2025)

Research Insights

Scality notes that 69% consider immutable data storage essential to their corporate cybersecurity. Manufacturing organizations (95%) are most likely to deploy immutable storage. 84% consider it essential to their corporate cybersecurity. Financial services firms (74%) report the lowest reliance on immutable storage. 60% say it's essential to their corporate cybersecurity (Scality, 2024)

STRATEGY – CONTINUOUS VULNERABILITY AND CONFIGURATION MANAGEMENT

Principle

Constantly scan, patch, and harden across OS, containers, databases, and devices.

Key technologies and tools

- Container/Image Scanning - Trivy, Clair, Anchore, Aqua Security, Sysdig Secure (Amir, 2024)
- OS & Database Hardening - Lynis, Lunar, LSAT, OpenSCAP, CIS Benchmarks (Piskunov, 2022)
- Automated Patching & Updates - Unattended Upgrades, WSUS, Patch My PC (patchmypc, 2025)
- Device Monitoring - Tanium, Qualys for endpoint and firmware scanning (Tanium, 2025).

Research Insights

The top 10 vulnerabilities scanned in 2022 were mostly related to the ability to conduct remote code execution (CSA, 2023). The survey found that 85% of organizations don’t conduct regular patching. A majority install patches quarterly or less often, which leaves them exposed to attacks for extended periods of time (Kovacs, 2025)

STRATEGY – SECURE SOFTWARE SUPPLY CHAIN

Principle

Ensure integrity and trust in all code, dependencies, and deployment artifacts.

Key technologies and tools

- Supply Chain Frameworks - SLSA, In-toto (SLSA, 2025)
- Artifact Signing & Verification - Sigstore, Cosign, Notary v2 (jfrog, 2025)
- SBOM (Software Bill of Materials) - Syft, CycloneDX, XRAY (JFrog, 2025 and OX Security, 2025).
- CI/CD Security – Veracode, Sonar, GitGuardian, Snyk, Sonatype Nexus Firewall.

Research Insights

According to the State of Code Security report 2025, 35% of the enterprises use self hosted runnrs in the cloud, introducing high risks due to weak security controls. The SLSA framework can help mitigate these risks (Wiz, 2025)

STRATEGY – ADVANCED DATA PROTECTION

Principle

One of the fundamental needs for data protection is to enforce data must be secured at rest, in transit, and during processing.

Key technologies and tools

- Encryption - Azure Key Vault, HashiCorp Vault, GCP CMEK, AWS KMS.
- Confidential Computing - Intel SGX, AMD SEV, Azure Confidential VMs (CVM, 2023)
- Immutable/Ransomware-Resistant Storage – Azure Immutable Storage, AWS S3 Object Lock, Rubrik, Veeam Immutability.
- Data Masking/Tokenization - Protegrity, Informatica Data Masking.

Research Insights

The confidential computing market size is expected to see exponential growth in the next few years. It will grow to $41.17 billion in 2029 at a compound annual growth rate (CAGR) of 35.3%. (Businessresearchcompany, 2025).

STRATEGY – UNIFIED OBSERVABILITY

Principle

Achieve deep, real-time visibility and rapid evidence collection across all platforms.

Key technologies and tools

- Centralized Logging & Metrics - Prometheus, Grafana Loki, Elasticsearch/Kibana, Fluent Bit.
- Distributed Tracing - Jaeger, OpenTelemetry.
- Forensics & Snapshots - Velero for Kubernetes backups, AWS CloudTrail, Azure Monitor, Falcon Forensics.
- Kernel-Level Monitoring - Sysdig, Falco, eBPF.

Research Insights

As per Dimensional Research's Observability Landscape Report, over 60% of organizations have reduced MTTR with mature solutions (Sharma, 2025).

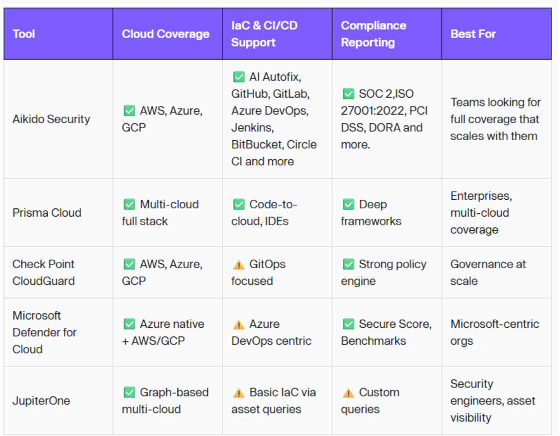
STRATEGY – CROSS-PLATFORM SECURITY FABRIC

Principle

Enforce consistent security controls across Kubernetes, VMs, serverless, and all cloud environments.

Key technologies and tools

- Unified IAM - AWS IAM, Azure Active Directory, Google Cloud IAM, Okta.
- Multi-Cloud Security Posture Management (CSPM) - Prisma Cloud, Fugue, Wiz, Orca Security (Alkido, 2025)
- Service Meshes - Consul Connect, [Istio], [Linkerd] for cross-environment mTLS and policy.
- Policy Federation - [OPA/Gatekeeper] with multi-cluster or multi-cloud support.



Tool	Cloud Coverage	IaC & CI/CD Support	Compliance Reporting	Best For
Aikido Security	✅ AWS, Azure, GCP	✅ AI Autofix, GitHub, GitLab, Azure DevOps, Jenkins, BitBucket, Circle CI and more	✅ SOC 2,ISO 27001:2022, PCI DSS, DORA and more.	Teams looking for full coverage that scales with them
Prisma Cloud	✅ Multi-cloud full stack	✅ Code-to-cloud, IDEs	✅ Deep frameworks	Enterprises, multi-cloud coverage
Check Point CloudGuard	✅ AWS, Azure, GCP	⚠️ GitOps focused	✅ Strong policy engine	Governance at scale
Microsoft Defender for Cloud	✅ Azure native + AWS/GCP	⚠️ Azure DevOps centric	✅ Secure Score, Benchmarks	Microsoft-centric orgs
JupiterOne	✅ Graph-based multi-cloud	⚠️ Basic IaC via asset queries	⚠️ Custom queries	Security engineers, asset visibility

Source: (alkido.dev)

FIGURE 2. COMMON CSPM TOOLING

Research Insights

Latest research from JumpCloud, in collaboration with Google Workspace, reveals that only 6% of IT leaders say their current setup works perfectly. Today, they are forced to manage an average of over nine different tools. This is why 87% of IT leaders will consider changing from their current productivity suite to adopt a more unified and secure platform (WJBF, 2025)

FUTURISTIC DIRECTIONS

Autonomous Security Operations

AI-driven "self-healing" clusters and cloud systems. (Arora, 2024)

Quantum-Resistant Cryptography

NIST standardizing post-quantum crypto (NIST, 2017 and AWS)

Blockchain for Supply Chain Integrity

Framework for Blockchain-Based Access Logs and Tamper-Proof Audit Trails (Rajuroy, 2025)

Privacy-Enhancing Computation

Confidential Computing use cases and companies (Hiter, 2023)

CONCLUSION

Securing the next generation of digital infrastructure requires more than incremental improvements. It demands holistic, technology-driven transformation. By embracing zero trust, policy automation, AI-powered detection, immutable and ephemeral workloads, robust supply chain defenses, advanced data protection, and unified security fabrics, organizations can outpace both current and future adversaries. Modern tools and platforms make these practices achievably provided they are integrated thoughtfully and continuously adapted as threats and technologies evolve.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1]Project Zero, "Project Zero," Blogspot.com, Nov. 18, 2019. https://googleprojectzero.blogspot.com/

[2]Gartner, "Gartner: Fueling the Future of Business," Gartner, 2023. https://www.gartner.com/en

[3]Sysdig, "WHITEPAPER. Securing AI Workloads," Sysdig, 2025. https://sysdig.pathfactory.com/c/pf-securing-ai-workload?x=u_WFRi&_gl=1 (accessed Dec. 29, 2025).

[4]Aqua, "Aqua Cloud Native Security, Container Security & Serverless Security," Aqua. https://www.aquasec.com/

[5]NIST, "Post-Quantum Cryptography | CSRC | CSRC," CSRC | NIST, Jan. 03, 2017. https://csrc.nist.gov/projects/post-quantum-cryptography

[6]I. T. L. Computer Security Division, "Cryptographic Standards and Guidelines | CSRC | CSRC," CSRC | NIST, Dec. 29, 2016. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines

[7]CNCF, "Cloud Native Security," Github.com, 2025. https://github.com/cncf/tag-security?tab=readme-ov-file (accessed Dec. 29, 2025).

[8]IBM, "Cost of Data Breach," Ibm.com, Nov. 12, 2025. https://www.ibm.com/think/insights/data-matters/cost-of-a-data-breach

[9]L. Fuks, A. Sheps, and A. Eitani, "Lena Fuks," Aqua, Jun. 27, 2023. https://www.aquasec.com/blog/2023-nautilus-cyber-security-report-insights-revealed/ (accessed Dec. 29, 2025).

[10]huntress, "Crowdstrike Microsoft Data Breach: What Happened, Impact, and Lessons | Huntress," Huntress, 2015. https://www.huntress.com/threat-library/data-breach/crowdstrike-microsoft-outage-data-breach (accessed Dec. 29, 2025).

[11]NIST, "NVD - CVE-2019-5736," nvd.nist.gov, Nov. 20, 2024. https://nvd.nist.gov/vuln/detail/CVE-2019-5736

[12]Akamai, "New Study Finds 84% of Security Professionals Experienced an API Security Incident in the Past Year," Akamai, Nov. 13, 2024. https://www.akamai.com/newsroom/press-release/new-study-finds-84-of-security-professionals-experienced-an-api-security-incident-in-the-past-year

[13]Akamai, "Application Security Report 2024 | Akamai," Akamai, 2024. https://www.akamai.com/resources/state-of-the-internet/securing-apps-report-2024

[14]Y. Verma, "Breaking Down S3 Ransomware: Variants, Attack Paths and Trend Vision OneTM Defenses," Trend Micro, Nov. 18, 2025. https://www.trendmicro.com/en_us/research/25/k/s3-ransomware.html (accessed Dec. 29, 2025).

[15]OWASP, "OWASP Cloud Tenant Isolation | OWASP Foundation," Owasp.org, 2023. https://owasp.org/www-project-cloud-tenant-isolation/ (accessed Dec. 29, 2025).

[16]hillelz, “AI Phishing Attacks - An Evolving Threat,” Check Point Software, Jul. 03, 2025. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/ai-phishing-attacks/

[17]L. José, “Unmanaged IoT Device Security: The Hidden Cybersecurity Risk Enterprises Can’t Ignore - Device Authority,” Device Authority, Sep. 03, 2025. https://deviceauthority.com/unmanaged-iot-device-security-the-hidden-cybersecurity-risk-enterprises-cant-ignore/ (accessed Dec. 29, 2025).

[18]Platform9, “Kubernetes Service Mesh: A Comparison of Istio, Linkerd, and Consul,” Platform9, Oct. 21, 2019. https://platform9.com/blog/kubernetes-service-mesh/ (accessed Dec. 29, 2025).

[19]Priya Mervana, “Azure Key Vault vs HashiCorp Vault [2025 In-Depth Comparison],” SSLInsights, Apr. 08, 2025. https://sslinsights.com/azure-key-vault-vs-hashicorp-vault/

[20]Zesty, “Calico vs. Cilium: Which Kubernetes CNI Is Right for You?,” Zesty, May 26, 2025. https://zesty.co/finops-glossary/calico-vs-cilium-in-kubernetes-networking/ (accessed Dec. 29, 2025).

[21]Akamai, “What Is Zero Trust Network Access (ZTNA)? | Akamai,” Akamai, 2024. https://www.akamai.com/glossary/what-is-ztna

[22]C. Writer, “Top 10 Zero Trust Network Access (ZTNA) Solutions for Enterprise Security - cybertechnologyinsights.com,” cybertechnologyinsights.com -, May 29, 2025. https://cybertechnologyinsights.com/cybertech-insights/top-10-zero-trust-network-access-ztna-solutions-for-enterprise-security/ (accessed Dec. 29, 2025).

[23]CNCF, “Service meshes are on the rise -but greater understanding and experience are required,” cloud native computing foundation, 2022. Available: https://www.cncf.io/wp-content/uploads/2022/05/CNCF_Service_Mesh_MicroSurvey_Final.pdf

[24]Amar Gurajapu, “Static Analysis of Kubernetes Object Definitions Using kube-score: Enhancing Security and Resilience,” ResearchGate, Dec. 2025, doi: https://doi.org/10.13140/RG.2.2.22384.11528.

[25]Amar Gurajapu, “Best Practices for Monitoring Kubernetes Clusters: Reliability and Minimise Operational Overhead,” Research Gate, Oct. 28, 2025. https://www.researchgate.net/publication/399121579_Best_Practices_for_Monitoring_Kubernetes_Clusters_Reliability_and_Minimise_Operational_Overhead?channel=doi&linkId=6950c8100c98040d48236e62&showFulltext=true

[26]cloudcustodian, “Cloud Custodian,” cloudcustodian.io. https://cloudcustodian.io/

[27]“Policy as Code Reaches 71% Enterprise Adoption as DevSecOps Shifts Left Successfully – Let’s Talk DevOps,” Devopstales.com, 2024. https://devopstales.com/devops/policy-as-code-reaches-71-enterprise-adoption-as-devsecops-shifts-left-successfully/ (accessed Dec. 29, 2025).

[28]A. Shimel, “Best of 2025: eBPF: The Silent Power Behind Cloud Native’s Next Phase,” Cloud Native Now, Dec. 23, 2025. https://cloudnativenow.com/editorial-calendar/best-of-2025/ebpf-the-silent-power-behind-cloud-natives-next-phase-2/ (accessed Dec. 29, 2025).

[29]SOAR, “Best SOAR Tools: Top 5 Options in 2026,” Exabeam, Nov. 12, 2025. https://www.exabeam.com/explainers/soar/best-soar-tools-top-5-options-this-year/ (accessed Dec. 29, 2025).

[30]cm-alliance, “Top 10 AI-Powered Cloud Security Tools for 2025,” Cm-alliance.com, 2025. https://www.cm-alliance.com/cybersecurity-blog/top-10-ai-powered-cloud-security-tools-for-2025

[31]D. Soldani et al., “IEEE Xplore Full-Text PDF”:, Ieee.org, 2025. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10138542 (accessed Dec. 29, 2025).

[32]D. Perry, “Mastering GitOps with Flux and Argo CD: Automating Infrastructure as Code in Kubernetes | Clutch Events,” Clutchevents.co, 2025. https://www.clutchevents.co/resources/mastering-gitops-with-flux-and-argo-cd-automating-infrastructure-as-code-in-kubernetes (accessed Dec. 29, 2025).

[33]Pulumi, “Most Effective Infrastructure as Code (IaC) Tools,” pulumi, 2025. https://www.pulumi.com/blog/infrastructure-as-code-tools/

[34]T. Natarajan, “The Ultimate Guide to Linux Kernel Live Patching: Technologies, Tools, and Enterprise Solutions,” Medium, Jun. 13, 2025. https://thamizhelango.medium.com/the-ultimate-guide-to-linux-kernel-live-patching-technologies-tools-and-enterprise-solutions-23dfb1b29121 (accessed Dec. 29, 2025).

[35]Scality, “94% of IT leaders rely on immutable storage to protect data as ransomware attacks skyrocket,” www.prnewswire.com, Mar. 06, 2024. https://www.prnewswire.com/news-releases/94-of-it-leaders-rely-on-immutable-storage-to-protect-data-as-ransomware-attacks-skyrocket-302080995.html

[36]R. Amir, “Open-Source Container Security: A Deep Dive into Trivy, Clair, and Grype,” Stakater, Nov. 26, 2024. https://www.stakater.com/post/open-source-container-security-a-deep-dive-into-trivy-clair-and-grype

[37]I. Piskunov, “Linux Hardening. We select tools for a comprehensive security audit,” Medium, Jul. 2022. https://ivanpiskunov.medium.com/linux-hardening-we-select-tools-for-a-comprehensive-security-audit-93dbabf27eaa

[38]patchmypc, “Patch Management,” Patch My PC, Apr. 08, 2025. https://patchmypc.com/patch-management/

[39]Tanium, “Tanium vs. Qualys | Tanium,” Tanium, Jul. 31, 2025. https://www.tanium.com/platform/tanium-vs-qualys/ (accessed Dec. 29, 2025).

[40]CSA, “Highlights from the 2023 Cloud Threat Report | CSA,” blog.aquasec.com, Jul. 24, 2023. https://cloudsecurityalliance.org/blog/2023/07/24/highlights-from-the-2023-cloud-threat-report

[41]E. Kovacs, “Organizations Still Not Patching OT Due to Disruption Concerns: Survey,” SecurityWeek, Mar. 05, 2025. https://www.securityweek.com/organizations-still-not-patching-ot-due-to-disruption-concerns-survey/

[42]“Software attestations,” SLSA, 2025. https://slsa.dev/attestation-model#recommended-suite (accessed Dec. 29, 2025).

[43]“Code Signing,” JFrog, May 30, 2025. https://jfrog.com/learn/devsecops/code-signing/

[44]OX Security, “Top 5 SBOM Tools 2025: Secure Your Software Supply Chain,” OX Security, Dec. 17, 2025. https://www.ox.security/blog/sbom-tools/ (accessed Dec. 29, 2025).

[45]Wiz, “What is the SLSA Framework?,” wiz.io, Feb. 13, 2025. https://www.wiz.io/academy/application-security/slsa-framework (accessed Dec. 29, 2025).

[46]CVM, “Introduction to confidential virtual machines,” Redhat.com, 2023. https://www.redhat.com/en/blog/introduction-confidential-virtual-machines (accessed Dec. 29, 2025).

[47]Businessresearchcompany, “Confidential Computing Global Market Report 2025,” Thebusinessresearchcompany.com, Dec. 16, 2025. https://www.thebusinessresearchcompany.com/report/confidential-computing-global-market-report (accessed Dec. 29, 2025).

[48]A. Sharma, “Unified Observability in Multi-Cloud & Hybrid IT Environments,” Motadata, Jan. 10, 2025. https://www.motadata.com/blog/unified-observability-in-multi-cloud-and-hybrid-it-environments/ (accessed Dec. 29, 2025).

[49]Aikido, “Top Cloud Security Posture Management (CSPM) Tools in 2025,” Aikido.dev, Mar. 27, 2025. https://www.aikido.dev/blog/top-cloud-security-posture-management-cspm-tools

[50]J. Inc, “WJBF,” WJBF, Dec. 16, 2025. https://www.wjbf.com/business/press-releases/cision/20251216LA48782/the-mandate-is-clear-87-of-enterprises-demand-unified-security-platforms/ (accessed Dec. 29, 2025).

[51]R. Arora, “AI-Driven Self-Healing Cloud Systems: Enhancing Reliability and Reducing Downtime through Event- Driven Automation,” ResearchGate, 2024. https://www.researchgate.net/publication/384258456_AI-Driven_Self-Healing_Cloud_Systems_Enhancing_Reliability_and_Reducing_Downtime_through_Event-_Driven_Automation

[52]“Post-Quantum Crypto - Amazon Web Services (AWS),” Amazon Web Services, Inc. https://aws.amazon.com/security/post-quantum-cryptography/

[53]A. Rajuroy, “A Framework for Blockchain-Based Access Logs and Tamper-Proof Audit Trails,” ResearchGate, Jun. 2025. https://www.researchgate.net/publication/392312120_A_Framework_for_Blockchain-Based_Access_Logs_and_Tamper-Proof_Audit_Trails

[54]S. Hiter, “What is Confidential Computing? Definition, Benefits, & Uses,” eSecurity Planet, May 26, 2023. https://www.esecurityplanet.com/applications/confidential-computing/

About the Authors

The author works for AT&T and has extensive work experience leading Cybersecurity initiatives for VP Org.

Amar Gurajapu is Principal Member of Technical Staff at AT&T. Amar has 25 years of experience in Telecom Software Engineering. He is leading multi-cloud transformation programs, and digital initiatives for key Network systems portfolio aligned with AT&T organization goals