AVIATRIX

CHECKLIST

Defend Yourself Against Ransomware

Ransomware Is on the Rise — and on the Move

According to the Verizon 2025 Data Breach Investigations Report, ransomware rose 37% over the previous year, and ransomware was present in 44% of the breaches reviewed, up from 32%. Sophisticated and organized ransomware groups are highly skilled at finding and exploiting even the smallest sliver of vulnerability.

Cybersecurity controls have gotten very good at buttoning up endpoints and other risks enumerated in the Common Vulnerabilities and Exposures (CVE) system. Continued vigilance in these areas is critical, but attackers are increasingly leveraging a vast new attack vector opened up by cloud computing: **communication pathways between cloud workloads**. Once ransomware gains a foothold, it spreads laterally through east-west cloud traffic, exploiting flat or poorly segmented networks.

Defense Requires Layered, Systemic Protections

Hybrid and multicloud network environments are complex; protecting yourself against ransomware isn't as simple as identifying a couple of gaps and patching them up. Furthermore, there's no such thing as an "unimportant" system when it comes to cybersecurity–any entry point can be weaponized. If your approach is to address specific, individual risks, you're signing up for an endless (and losing) game of Whac-A-Mole. Instead, you need a systemic, defense-in-depth strategy. Here's a checklist to help you get started.

Checklist of Systemic Ransomware Protections

Segmentation Controls

- [ ] **Enforce zero trust segmentation.** The cloud has shattered the perimeter (i.e., the fortified wall that separates the safe inside from the unsafe outside), making perimeter-based controls unsuited for this environment. Zero trust essentially puts a perimeter around every individual workload/device/etc. with never-trust-always-verify enforcement. You need to segment workloads into discrete trust zones across VPCs/VNets and clouds, enforcing explicit, identity-based connectivity policies between them.

- [ ] **Apply micro-segmentation at the workload level.** Ransomware actors look for opportunities to exploit trust relationships at fine granularity, for example, between microservices. Apply microsegmentation at the workload or tag level to restrict communication between instances, pods, or application tiers. This goes beyond coarse segmentation and prevents lateral propagation between services. Agentless, network-native segmentation ensures consistent policy enforcement across cloud providers and workload types.

- [ ] **Isolate backup networks and paths from production traffic.** A common ransomware tactic is to encrypt or corrupt backups. Use segmentation and routing controls to carve out isolated backup VPCs or transit domains that are only reachable under strict conditions.

Traffic Controls

- [ ] **Enforce east-west and north-south traffic filtering.** Traditional firewalls inspect and control north-south traffic, which flows between the internal network and the external world. You also need inline network enforcement for east-west data flows between workloads.

- [ ] **Secure egress traffic.** It's not enough to prevent attackers from accessing your systems. You also need protections to block data leakage in the event you are breached. Egress filtering prevents ransomware from calling home to command-and-control (C2) servers or exfiltrating data via malicious outbound connections.

- [ ] **Encrypt all in-transit traffic.** Ransomware actors look for network traffic they can manipulate, and unencrypted cross-cloud links are vulnerable. Ensure that all traffic between VPCs, between clouds, and from clouds to on-premises is encrypted at Layer 3.

- [ ] **Harden and isolate Kubernetes/container egress.** Ransomware often "phones home" to the attackers, and unfiltered egress from Kubernetes is a vulnerable vector. To prevent malicious external communication–for example, to attackers' command-and-control (C2) servers–you need to control and filter egress from container clusters. Harden container egress using cloud network controls rather than per-pod firewalls to ensure performance and consistency.

Policy Enforcement

- [ ] **Centralize policy management and visibility.** Fragmented policy management increases the risk of misconfigurations and can delay the detection of ransomware propagations. You want to maintain a single pane of glass for policy control, topology visualization, and consistent enforcement across clouds. A single control plane for policies across clouds reduces misconfigurations, which is the leading cause of cloud breaches.

- [ ] **Automate policy deployment.** Manual configuration is slow and error-prone. One mistake could open a path for ransomware movement. Use infrastructure-as-code (IaC) or API-based automation to enforce consistency and speed.

- [ ] **Implement role-based access control + least privilege.** Admin accounts are particularly sensitive–a compromise in these accounts provides attackers a shortcut to disabling policies there. You want to apply RBAC with separation of duties to ensure no single administrator can modify enforcement and policy layers simultaneously.

Monitoring and Maintenance

- [ ] **Implement always-on risk scoring.** Continuous assessment of your security posture can surface latent misconfigurations and anomalies and flag risky segments to maintain your network posture and reduce exploitable vulnerabilities.

- [ ] **Set up real-time alerts for suspicious traffic, policy breaches, or abrupt spikes in east-west traffic.** Early detection of unusual traffic patterns or lateral movement helps contain ransomware before it spreads.

- [ ] **Integrate threat intel and reputation feeds.** Ransomware often relies on known malicious infrastructure. Incorporate reputation-based blocking to prevent known malicious domains or IPs from communicating.

Governance and Best Practices

- [ ] **Periodically reassess and harden policies.** Policy drift—which happens when, over time, policies become looser or redundant—results in stale rules that attackers could exploit. You want to map policy audits to frameworks like CISA Zero Trust Maturity Model (ZTMM) 2.0 or NIST CSF 2.0 for structured improvement.

- [ ] **Create shadow AI controls and governance.** Shadow AI (and its precursor, shadow IT) by definition features tools that run outside the governance of IT and security teams. AI tools that interact with cloud data outside approved channels (shadow AI) can create new attack surfaces or data-leakage paths. Enforce policy consistently to stop insecure activity such as unmonitored AI agents accessing sensitive systems.

Aviatrix Provides Defense-in-Depth for Ransomware Protection

Aviatrix Cloud Native Security Fabric™ (CNSF) uses the zero trust framework to blanket your network with pervasive multicloud, hybrid, and multi-region protection against ransomware and other security risks.

- **Identity-based security policies**
  Enforce single, hybrid, or multicloud security policies based on workload, namespace, and cluster identity, instead of ephemeral attributes like IP addresses, to eliminate the identity confusion that attackers can exploit.
- **Network segmentation**
  Implement network segmentation that spans clouds, locations, and environments to prevent lateral movement.
- **Network-wide visibility:**
  Get visibility into all traffic types. This includes not just north-south traffic coming in and out of your network, but also east-west visibility so you can see what's going on between your workloads, including suspicious activity and lateral movement.
- **Egress filtering:**
  Guard the back door of your network to prevent data exfiltration.
- **Complementarity with other security solutions**
  The "fabric" in Cloud Native Security Fabric means it extends runtime enforcement and visibility to the network layer—complementing your existing CNAPP, CSPM, and EDR tools.
- **High-Performance Encryption (HPE)**
  Encrypt inter-VPC and inter-cloud traffic at Layer 3 with no trade-off between performance and security, closing the gaps left by TLS, IPsec, or MACsec.
- **Consistent security policy enforcement**
  Stop insecure activity, such as data exposed through shadow AI/IT, with visibility and identity-based security policies that are inline and in the runtime. Whether you're protecting workloads in AWS, Azure, GCP, or on premises, Aviatrix CNSF delivers consistent runtime enforcement to stop ransomware before it spreads.

Ready to experience Aviatrix CNSF for yourself?

Schedule a Demo

with our cloud network security experts

About Aviatrix

For enterprises struggling to secure cloud workloads, Aviatrix® offers a single solution for pervasive cloud security. Where current cybersecurity approaches focus on securing entry points to a trusted space, Aviatrix Cloud Native Security Fabric (CNSF) delivers runtime security and enforcement within the cloud application infrastructure itself – closing gaps between existing solutions and helping organizations regain visibility and control. Aviatrix ensures security, cloud, and networking teams are empowering developer velocity, AI, serverless, and what's next. For more information, visit aviatrix.ai.