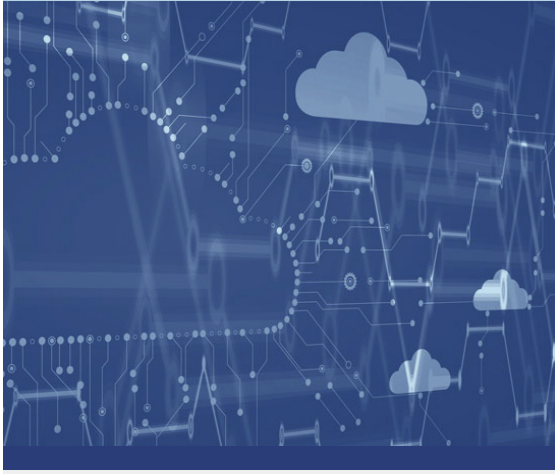

Incident Response in the Cloud

Best Practices, Challenges, and Outcomes

Incident response has a consistent and mature process for responding to security breaches, at a high level: identification, containment, eradication, and recovery.

While this is a consistent process at a very high level, the devil is always in the details – and the details vary greatly between cloud and on-premises, different types of data store, access management domains, and all of the other systems choices that go into your infrastructure.

"Cloud" Really Means Hybrid (or Multi)

Overwhelmingly, organizations are using a mix of environments. Seventy percent are using a mix of public and private cloud, and another 14% are using a mix of public clouds.[1] Over a fifth of cloud workloads have been repatriated from the cloud to on-prem (frequently related to cost, security, or performance requirements).

For incident response and remediation (IRR), that adds complexity and difficulty to any kind of management process because a breach in one area could make the entire infrastructure vulnerable through shared data or identity management systems. It also complicates recovery because of different tooling, different monitoring or logging data, and different systems and services.

Shifting Risks for Cloud-Based Security Incidents

The ease of creating public cloud instances also makes it a high-risk environment for shadow IT, shadow data, or loose security controls.

One thing to realize is that a security breach isn't a fast-moving event with a hacker hunched over a laptop. It is a long-running game of patience. Most breaches start with compromised credentials. In phishing tests, 11% of users clicked the phishing link and entered their credentials – compromising their user accounts in under 50 seconds.[2]

But then they wait. According to the IBM Cost of a Data Breach Report 2024[3], the average dwell time for a hacker was 292 days. They spend this time lurking, finding out where key resources are, looking for vulnerable or unpatched systems, and trying to escalate privileges where possible.

And cloud-based data hugely complicates response and recovery. Almost two-thirds of data breaches involve information stored only in public cloud (25%) or in hybrid public-private environments (40%). If data is stored in public cloud, then the cost of the breach tops $5 million, almost a million more than data breaches involving only on-premises or private cloud environments. Likewise, physical and private cloud breaches were identified and contained almost 70 days faster (224 days) than public cloud or hybrid breaches.

[1] *State of the Cloud Report. Flexera, 19 Mar. 2025*

[2] *Hylender, C. David, et al. Data Breach Investigations Report. Verizon Business, 1 May 2024*

[3] *Cost of a Data Breach. IBM, 30 July 2024*

Thrive's NextGen Platform

About Thrive

Thrive is a NextGen global technology outsourcing provider that empowers small and mid-market organizations to transform their technology into a strategic advantage. Offering a breadth of services from AI and cybersecurity to cloud, compliance, and traditional MSP/MSSP solutions, Thrive's team of seasoned experts develop strategies that standardize, scale, and automate technology to achieve outsized ROI. From advisory services to a 24×7×365 SOC and NOC, Thrive provides end-to-end IT and cybersecurity management so clients can focus on innovation and growth. With Thrive, your business is always supported and always secure.

Learn more at www.thrivenextgen.com or follow us on LinkedIn.

The ease and speed of deployment for public cloud instances are parallel the reasons that public cloud is more susceptible to breach:

- Every integration point is a potential vulnerability.
- Identity and access management is either centralized in a central people store, is distributed and integrated in multiple places, or is weakened to allow appropriate levels of access.
- There is no centralized monitoring tool across environments.
- Consistent logging and auditing can be difficult in cloud environments.

Cloud vs On-Prem Response

There are key differences in how to respond to a security incident depending on the type of environment involved.

- **Initial detection.** Cloud instances have built-in monitoring tools and external dashboards through the cloud provider, and this is similarly true for private cloud, where physical servers have to have external tools or agents installed for security monitoring.
- **Control and visibility.** Both on-prem systems offer direct access to the entire hardware infrastructure, from servers to networking. For private cloud, this depends on where the private cloud is hosted, while for public cloud, there is no insight or access to the underlying infrastructure.
- **Recovery and resilience.** Recovering specific instances is much faster in public cloud, since old instances can be killed and new instances spun up automatically, where physical systems have to be rebuilt manually. However, cloud environments also have more complicated dependencies and integrations, which can make slow down recovery efforts over the entire process.
- **Skills.** Recovery efforts require a mixed set of skills. Physical systems require more knowledge on domain management, networking and hardware, and tools. Cloud environments require knowledge of the different cloud services, identity and access management, and automation and scripting.

Adapt and Strengthen Your Incident Response Plan

An incident response plan needs to be clear and thorough enough to help you react immediately, without getting bogged down or missing key actions. These are the basics of what you need:

- **A complete call list.** This includes external parties like services providers and technology vendors, as well as internal contacts (and backup contacts) for IT, legal, HR, and accounting.
- **A list of insurance policies and contracts.** There could be legal obligations to inform clients or vendors of potential data loss within a certain time period.
- **An IT inventory (and ideally, an infrastructure topology showing dependencies).** Having a list of administrative accounts, operating environments, SaaS platforms, domains, and data center or physical server locations helps with containment. This can also be used to help isolate affected environments and prevent access to other systems (if possible).

A security plan has to be multi-layered to be effective. It is not possible to successfully prevent any attack of any kind, ever, but it is possible to put yourself in a position to lessen the likelihood of attacks, reduce their scope, and enhance your resilience. Tools like red team testing, vulnerability management, penetration testing, and user training augment your security tooling by reinforcing the right behaviors.