Mean Time to Remediation: Why CISOs Should Care

Cloud breaches due to preventable misconfigurations have become a massive problem. A recent report from IBM X-Force[1] revealed that there was a 424% increase in data breaches resulting from cloud misconfigurations caused by human error.

With more companies embracing the cloud, configuration drifts become more likely and can expose organizations to unforeseen risks. The risks due to misconfigurations can be severe for organizations: steep regulatory fines, loss of customer data, and damage to your brand.

80%

of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities.[2]

Why is This Happening?

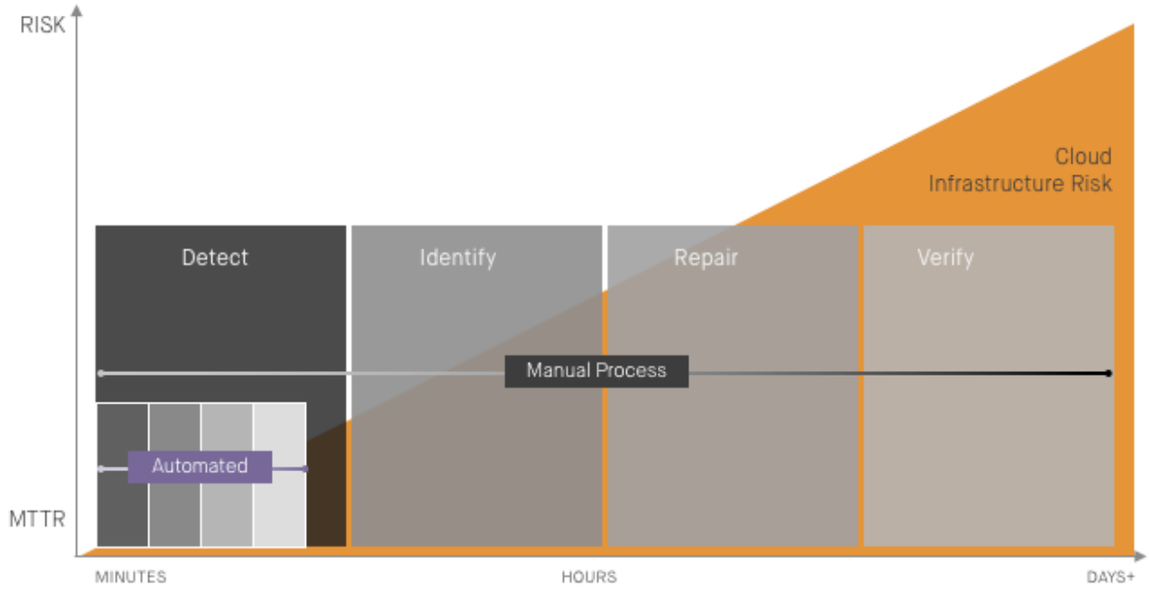
With the cloud, we can innovate much faster than we could in the datacenter. But cloud infrastructure is highly dynamic and ephemeral, with numerous interfaces to cloud APIs. The security solutions that we relied on in the datacenter just don't work in the cloud.

Why is Mean Time to Remediation so Important?

Mean Time to Remediation (MTTR) is the key security metric for measuring cloud infrastructure risk. Threats to cloud infrastructure are fully automated, constantly probing for attack vectors to exploit. The longer cloud misconfigurations go unaddressed, the greater the risk of a major security incident.

As exhibited in chart following, the MTTR when manually remediating misconfigurations is often measured in hours or days, which is unacceptably high considering the nature of the threats. Any approach that doesn't immediately and automatically identify misconfigurations and remediate them back to a known-good baseline increases the risk of a breach or major security incident.

MANUAL VS. AUTOMATED



Driving Down Your MTTR for Cloud Misconfigurations

Now that you understand the risk of cloud misconfigurations and how to measure it, here are your next steps:

1. **Determine who "owns" your cloud misconfigurations.** Which teams are monitoring and identifying cloud risks? Which teams are responsible for remediating misconfigurations? Does your organization know what its MTTR is? Are there inefficiencies and unnecessary delays in remediating misconfigurations?

2. **Set a goal for your MTTR.** Once you find out your MTTR, you're still only part of the way there. Unless it's measured in minutes, you've still got work to do.

3. **Evaluation solutions.** Understand your options. Run proof of concepts. Ask lots of questions.

LEARN MORE

To learn more about how Fugue can help you achieve an MTTR score that is measured in minutes, visit www.fugue.co.

FOOTNOTES

1. *http://newsroom.ibm.com/2018-04-04-IBM-X-Force-Report-Fewer-Records-Breached-In-2017-As-Cybercriminals-Focused-On-Ransomware-And-Destructive-Attacks*

2. *http://www.datacenterjournal.com/top-cloud-security-trends-for-2016/*

About Fugue

Fugue, a leader in cloud infrastructure automation and security, provides solutions to ensure that enterprise and public agencies cloud resources are always provisioned according to a single source of truth—and stay that way throughout the resources' lifetime. Fugue is privately held and headquartered in Maryland. Fugue was names a Cool Vendor in Cloud Computing 2017 by Gartner.

aws partner network
Advanced Technology Partner