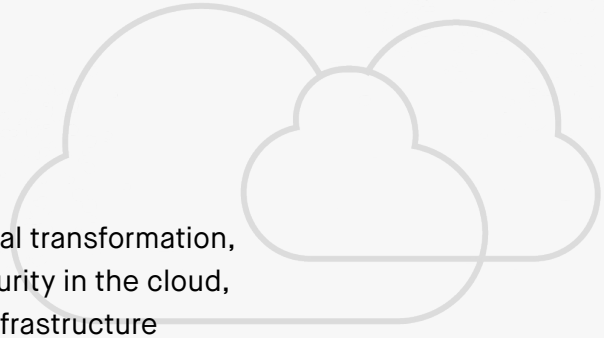
EBOOK

A COMPREHENSIVE GUIDE TO

Preventing Cloud Misconfiguration

Fugue

Cloud REVOLUTION



As organizations rapidly adopt the cloud to revolutionize their digital transformation, cloud security becomes a significant risk. When we talk about security in the cloud, misconfiguration needs to be a focus of the conversation. Cloud infrastructure misconfiguration represents the biggest threat to enterprise cloud security. It is also entirely preventable.

"Cloud configuration is complex and if not done correctly means that any security solution implemented in the cloud can't stop hackers from running away with your data.[1]" In this guide, we take a comprehensive look at cloud misconfiguration, including the causes, consequences, the different types of misconfiguration, the Mean Time to Remediation (MTTR) for misconfiguration, and the best practices required to prevent misconfiguration.

> *I'm seeing a lot of cloud configuration errors in the real world—and it's scaring the hell out of me."*
>
> — David Linthicum, Infoworld

Consequences OF CLOUD MISCONFIGURATION

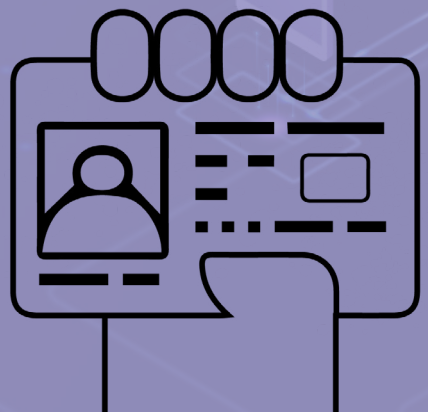
A simple misconfiguration can quickly escalate into a major security headache for an organization and its customers.

For example, a recent security incident[2] that affected an **LA-based organization accidentally exposed approximately 3.5 million records,** including personally identifiable information (PII) such as the employees' access credentials, email addresses, social security numbers, and the organization's registered sources.

The sensitive nature of the data made the security breach more damaging because the data could be used for exploitation or more destructive attacks. The breach was the result of a misconfiguration for an Amazon AWS S3 storage bucket that was configured to be public and anonymously accessible.

This is just one example of the many data breaches resulting from misconfiguration that has made the news. Others include a **FedEx breach[3] that exposed 119,000 scanned documents** due to FedEx's failure to audit the cloud assets of a company it acquired.

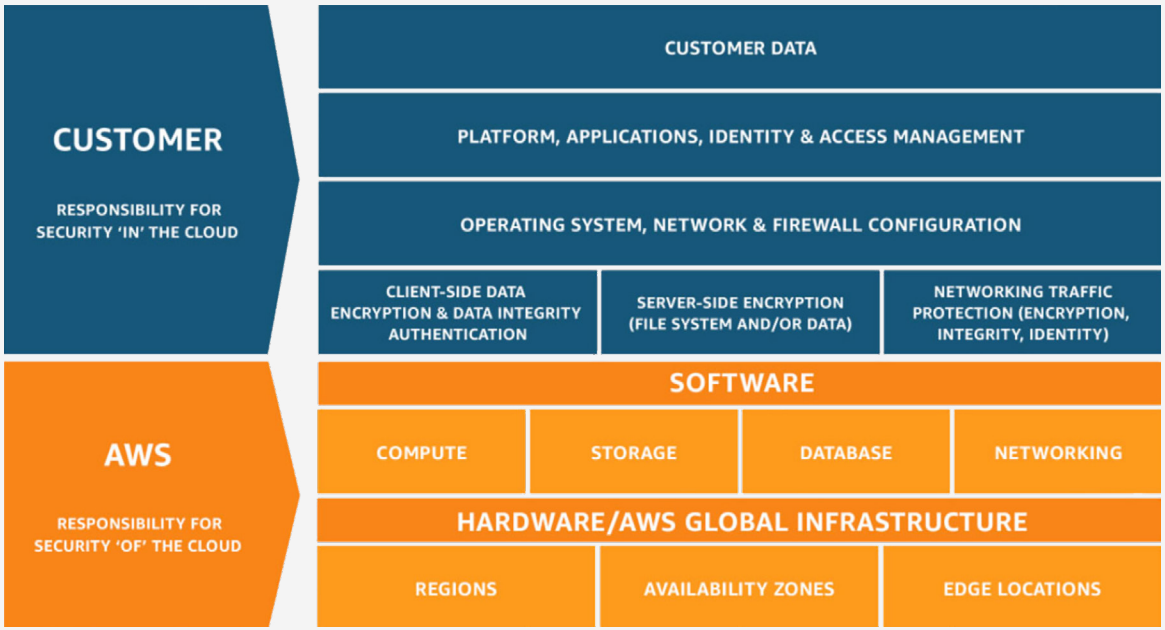
Deep Root Analytics[4] left a cloud storage server unsecure, exposing the information of 198 million US voters, and an unsecured AWS S3 bucket at **Patient Home Monitoring Corporation[5] left 150,000 patient records unprotected.**



Configuration IS THE RESPONSIBILITY OF THE ORGANIZATION

Cloud security and compliance is not the responsibility of any single entity alone, but rather it is a shared responsibility between cloud service providers (CSPs) and their customers. This shared responsibility has caused considerable confusion with CSP customers. It's not uncommon for organizations to assume that the CSP is responsible for all aspects of the security since they're charged with protecting the underlying infrastructure upon which the cloud services run. This assumption can lead to security mistakes and significant risk.

Under the Shared Responsibility Model, the CSP is responsible for "security ***of*** the cloud" which includes the hardware, software, networking, and facilities that run the cloud services. Organizations, on the other hand, are responsible for "security ***in*** the cloud" which includes how they configure and use the resources provided by the CSP.



Despite the existence of this formal model, there is still confusion regarding the demarcation of responsibility between the CSP and the enterprise. A good rule of thumb is that the CSP's API surface is the unofficial demarcation line between what organizations are responsible for, and what the CSP is responsible for. Cloud resource configurations are implemented via the APIs provided by the CSP, so they are the responsibility of the customer.

The Human Factor IN MISCONFIGURATION

We stated earlier that cloud misconfiguration remains the biggest security threat for organizations in the cloud, but it is also preventable. The reason is that human error is the most common cause of misconfiguration. The 2018 IBM X-Force Report[6] notes a 424% increase in data breaches resulting from cloud misconfiguration caused by human error. Gartner[6] indicated that by 2020, 95% of cloud security incidents will be the customer's fault.

424%

INCREASE IN DATA BREACHES AS A RESULT OF HUMAN-ERROR CLOUD MISCONFIGURATIONS

"The complexities of cloud computing, and the chance of human error will bite you in the butt, so don't skimp on security planning before deployment or security validation after deployment."

— David Linthicum, Infoworld

Common Types OF MISCONFIGURATION

There are several types of misconfiguration events that enterprises encounter when moving their workloads to the cloud. Some types of misconfiguration include:

AWS SECURITY GROUP MISCONFIGURATION:

AWS Security Groups are associated with EC2 server instances and provide security at the port and protocol access level. A Security Group misconfiguration can allow an attacker to access your cloud-based servers and exfiltrate data. A common Security Group misconfiguration is to make a server accessible on the SSH port (22) from the Internet, which typically occurs during debugging or troubleshooting activity. This misconfiguration makes it much easier for malicious users to gain access to servers from anywhere in the world.

ACCESS RESTRICTIONS:

A lack of adequate restrictions or safeguards in place to prevent unauthorized access to your infrastructure can put your organization at risk.

Unsecured AWS S3 storage buckets are perhaps the most frequently reported issue for cloud services that are left unsecured. This security issue can result in attackers accessing and downloading critical data. In some cases, it can allow bad actors to write to an organization's cloud account.

PERMISSION CONTROLS:

A failure to apply the least privilege principle can create security risks, where organizations do not limit permissions to individuals and service accounts to what they din limit permissions to individuals and service accounts to what they need to perform their required tasks.

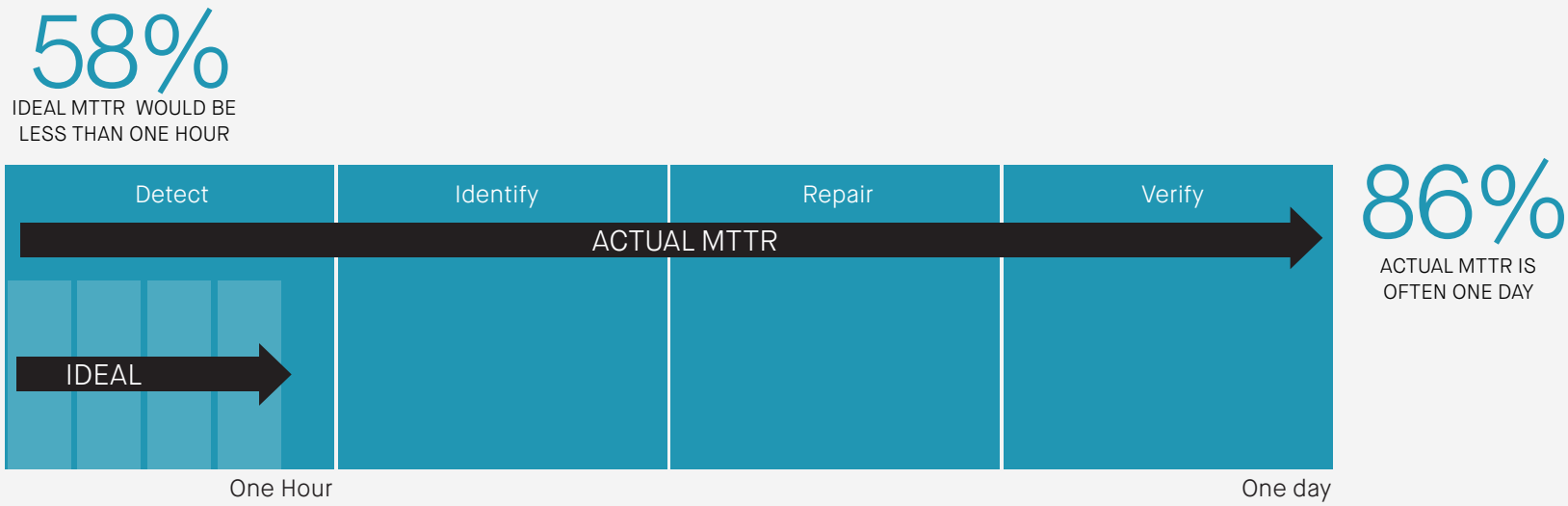
MTTR: A METRIC THAT EVERYONE SHOULD BE AWARE OF

Mean Time to Remediation (MTTR) is the time that elapses between when a misconfiguration first occurs and when it is remediated. It is the one cloud security metric that every CISO and anyone with cloud security responsibility should know. However, few have a good handle on it.

According to a recent survey[7], there is a big difference between an organization's actual MTTR and what IT and security professionals feel the ideal MTTR should be:

It's not uncommon for MTTR to be measured in days, weeks, or even months. That's a massive data breach waiting to happen. Time delays are the biggest threat to cloud infrastructure. The longer a misconfiguration is left undetected or not corrected, the higher the risk for a major security breach.

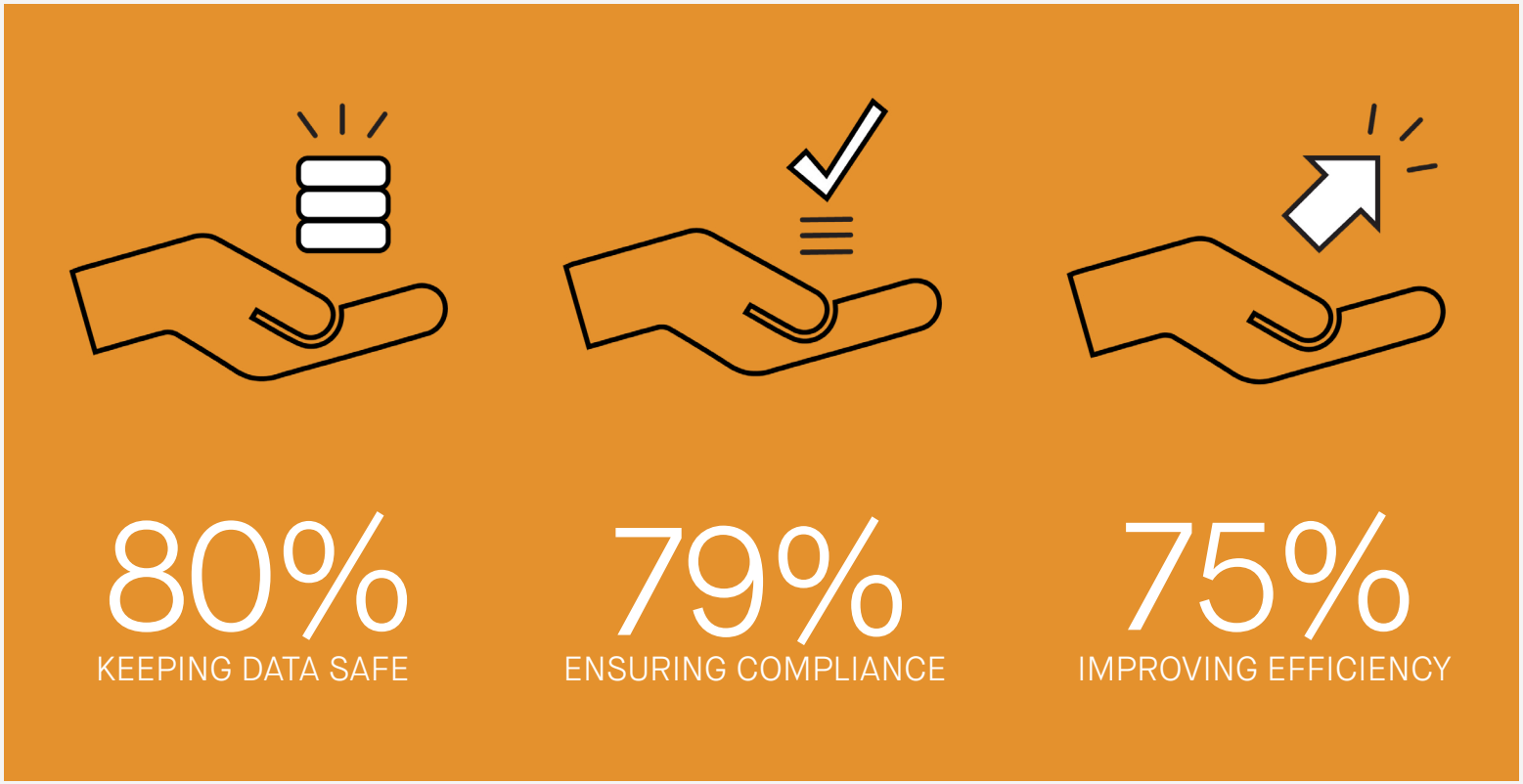
The good news is that it's possible to bring MTTR down to minutes for any misconfiguration. Enforcement of misconfiguration powered by an automated remediation solution can identify problems and implement corrections immediately.



Automated REMEDIATION

Based on a survey[8] of 300 organizations, there is significant value in automated remediation.

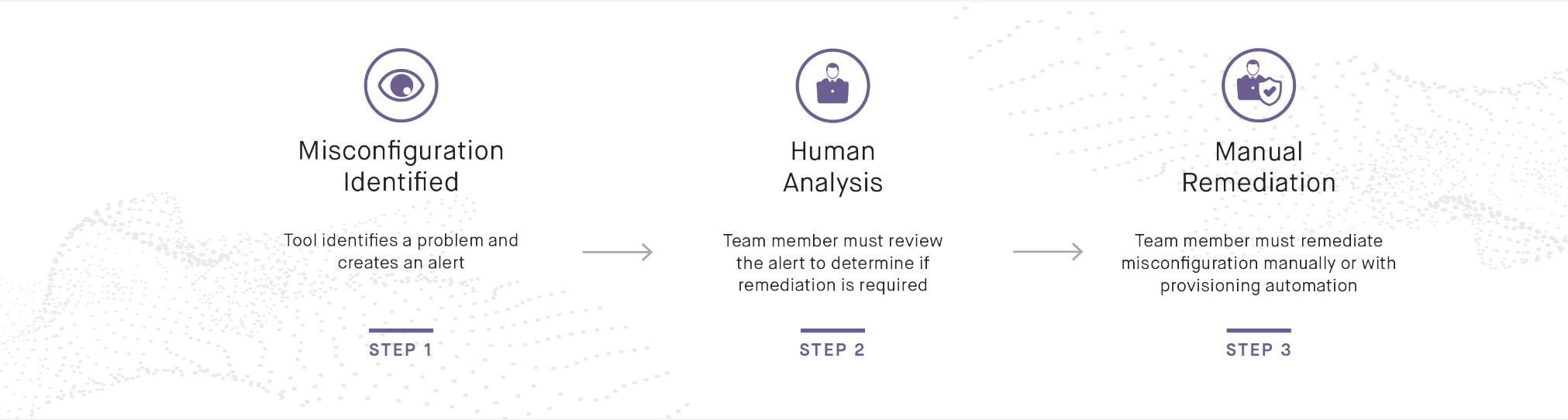
WHAT IS THE VALUE OF AUTOMATED REMEDIATION?



Type 1: ASSISTIVE REMEDIATION

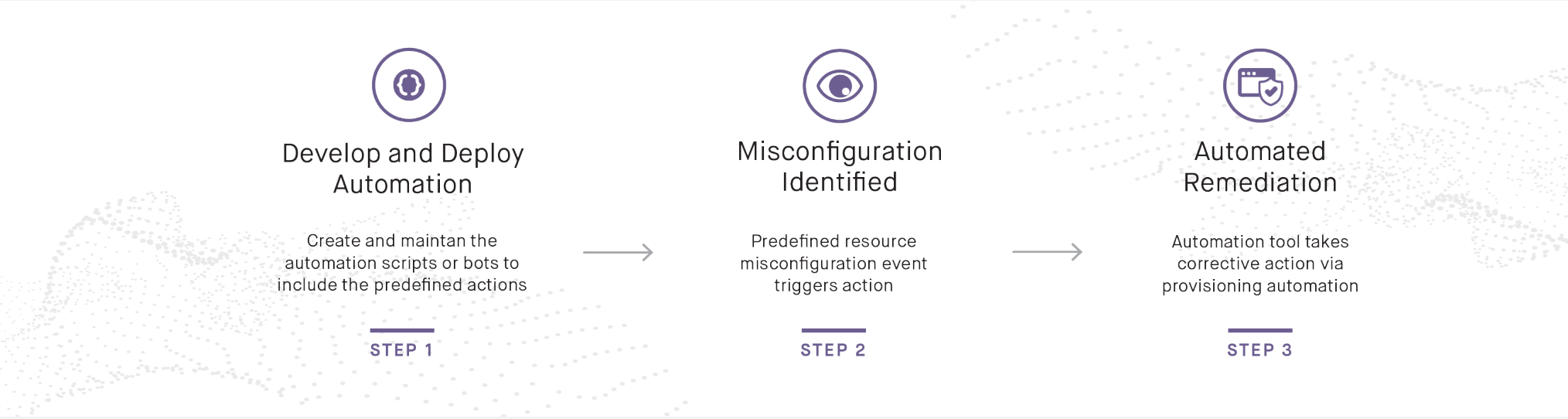
When we talk about automated remediation, there are three approaches:

Assistive Remediation is the most common approach to addressing misconfiguration, although it's not truly automated remediation. With Assistive Remediation, a tool scans your cloud infrastructure and generates an alert notifying you of potential problems. No other action is taken, but users are provided information that can help enable teams to prioritize critical issues that need to be remediated.



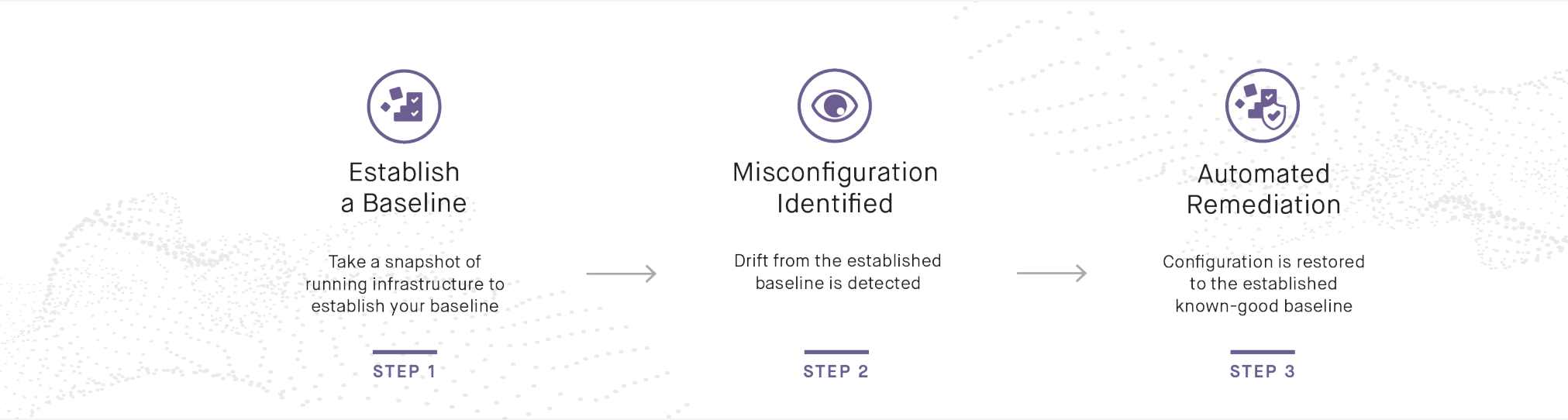
Type 2: STRUCTURED RESPONSE

Structured Response builds upon the Assistive Remediation approach. With this approach, a scanning tool provides “hooks” for additional automation scripts or bots that can automatically remediate some misconfiguration issues with a structured response. The benefit of this approach is that it allows for faster response times for specific predefined misconfiguration events with a robust audit trail. The tradeoff is that scalability can be a challenge as automation scripts need to be updated and scaled out to address new workloads.



Type 3: BASELINE ENFORCEMENT

Baseline Enforcement is the most comprehensive of the three approaches. With this approach, all unauthorized changes are identified and compared to an established baseline. Instead of implementing a defined action based on a defined problem, Baseline Enforcement restores the resource configuration back to a known-good established baseline. This approach removes issues concerning maintainability and scalability.



Best Practices TO PREVENT MISCONFIGURATION

Organizations should take cloud misconfiguration seriously and not assume that their CSP is responsible for it or that traditional security solutions are adequate to protect against them. By implementing certain best practices, you can go a long way to securing your cloud-based assets and prevent misconfiguration.

1 CHECK PERMISSION CONTROLS

Giving widespread access to employees and service accounts in your organization that only need limited permissions to perform their jobs creates a weak link in your overall security. Allowing users too much access opens the organization to risks. Apply the principle of least privilege by only giving users and service accounts the minimum set of permissions to perform their needed tasks.

2 CONTINUOUSLY AUDIT FOR MISCONFIGURATION AND COMPLIANCE

Configuring cloud resources properly and in accordance with policy is only the beginning. Ensuring these resources stay compliant throughout their lifecycles is a much bigger challenge. Organizations should implement regular audits to check for signs of misconfiguration and to maintain security and compliance policy.

3 IMPLEMENT SECURITY MEASURES SUCH AS LOGGING AND ENCRYPTION

It can be difficult to manage the number of users making changes to your cloud environment. Turning on logging will allow you to track changes made to your resources and help identify the cause of misconfiguration. Without appropriate logging, an attacker's activities can go unnoticed or unrecorded.

Enabling logging tracks all changes, while encryption allows you to securely protect data from unauthorized viewing. It's not uncommon for encryption settings for databases and object storage resources to be accidentally disabled. Logging will help you identify the cause of such incidents.

Best Practices...

4 CHECK FOR POLICY COMPLIANCE BEFORE PROVISIONING

Organizations may have strong security policies, but these are often not well integrated into the IT processes that teams use to build applications and deploy cloud infrastructure. Team members might not be aware of all the policies, and through ignorance might misconfigure settings from the start. Utilizing a security solution that offers a policy-as-code feature can help to ensure that configurations are compliant before deployment.

5 CHOOSE THE RIGHT SECURITY SOLUTION

Organizations looking to bolster their cloud security should look at security solutions that include automated remediation. Enforcement in the cloud must be done at the API level. Traditional monitoring and alerting tools are typically not enough since there is no room for human error and slowness.

As mentioned previously, there are three common approaches to automated remediation. The most comprehensive approach, Baseline Enforcement, automatically remediates policy and security violations. It will revert them back to a good known state (or baseline) ensuring that your infrastructure is always in compliance.

Unlike the Assisted Remediation, the Baseline Enforcement approach does not rely on human analysis to initiate remediation. The costs associated with having IT staff analyze alerts, prioritize, and then move to remediation can easily wipe out any savings and speed that the cloud promises.

Conclusion

Businesses operating in the cloud are taking a big and preventable risk if they are not looking at and immediately fixing all types of misconfiguration. Enforcement of cloud infrastructure must be done at the API level and span the full infrastructure stack. This cannot be done with traditional monitoring and alerting tools because there is no room for human error and excessive MTTR. Therefore, a security solution that includes continuous monitoring and automated remediation will help to secure your cloud infrastructure.

Visit www.fugue.co to learn more about our automated remediation solution which automatically reverts all unauthorized security and compliance changes back to a good-known baseline to help ensure that your infrastructure is always in compliance.

FOOTNOTES:

1. https://www.infoworld.com/article/3310841/cloud-security/cloud-misconfiguration-the-security-threat-too-often-overlooked.html
2. https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/la-county-non-profit-leaks-3-5-million-pii-via-misconfigured-amazon-s3
3. https://securityaffairs.co/wordpress/69152/data-breach/fedex-company-data-leak.html
4. https://www.wired.com/story/voter-records-exposed-database/
5. https://gizmodo.com/data-breach-exposed-medical-records-including-blood-te-1819322884
6. https://www.techrepublic.com/article/human-error-led-to-424-increase-in-misconfigured-cloud-servers-prompting-hacks/
7. https://www.gartner.com/smarterwithgartner/why-cloud-security-is-everyones-business/
8. https://www.fugue.co/resources/infographic-cloud-infrastructure-misconfiguration-report-2018

Fugue

Fugue is a security and compliance solution that identifies and eliminates cloud risks. Our patented software automatically remediates misconfigurations and policy violations in near real time and ensures they are never repeated. With Fugue, cloud resources are always provisioned according to a single source of truth – and stay that way throughout the resources' lifetime.

The reality is that public cloud configuration is complex, takes specialized training, and if not done right means any security systems you layer on top of your cloud can't stop hackers running away with your data."

— David Linthicum, Infoworld

www.fugue.co | hello@fugue.co | @FugueHQ