MajorKey

Building a Powerful Framework with AWS Control Tower, Security Hub and Config for AWS Environments

Smart Security Automation Built on a Strong Foundation

Introduction

The combination of AWS Control Tower, AWS Config and AWS Security Hub is a powerful framework around which to build a cloud "home" for your enterprise, and benefit from the flexibility, accessibility and scalability of the cloud. Much like physical infrastructures, regulations and requirements must be met when building to match the environment. It's imperative that future additions (the overall master plan) are taken into consideration to ensure that they work seamlessly. Like building construction today that uses advances in prefabricated components and best practices to speed up construction, cloud adoption is accelerated by new automation tools and technologies that can make building every component faster and consistent with the requirements you need to follow.

Yet construction is only the first step. Once your "home" is built, you need monitoring of your systems to ensure compliance with those regulations and to ensure structural integrity. In a physical structure, this could be a leaky pipe you spot, a crack in a wall, or a flickering light with a buzzing sound. Spotting the signs of a problem is more difficult in a virtual environment. Automation can quickly identify and alert you to issues, so that pesky leak doesn't become a flooded basement.

In today's 24-7 landscape, this happens faster than ever before. Development cycles no longer last months or years, and your organization needs to be nimble enough to deploy cloud accounts quickly and with the confidence that all the life-cycle security events surrounding a cloud account follow the proper steps to meet the regulations and requirements your organization has set up.

DevSecOps teams can thrive together in the cloud. It all starts with understanding the master plan and building a strong foundation.

Achieving that nimbleness and agility in the cloud means assembling everything together so:

- Your security team is confident that steps are being taken to protect valuable IP
- Your development and operations teams can feel empowered to ideate and create via a self-serve model, rather than being hand-held and feeling stifled in their ingenuity and innovation
- Your overall enterprise can operate at the speed it needs without IT bottlenecks

Setting the Foundation

As precast foundations provide speed, durability, and security for constructing homes, buildings, and even bridges, AWS Control Tower accelerates cloud adoption by rapidly providing a best practice security and governance foundation.

With a few clicks, Control Tower automatically builds the cloud landing zone, a footing on which to build your cloud estate. Landing Zones are built using AWS best practice blueprints for securing and managing your environment. Prefabricated orchestration workflows automatically create and secure AWS accounts with guardrails designed to enforce control policies and detect violations. These can include identity management, federated access, centralized logging, and cross-account security auditing, among many others.

Combined with the ground rules set through AWS Config and monitoring activity through AWS Security Hub, Control Tower brings it all together with centralized consolidation and governance of multi-account environments. New accounts can be established with just a few clicks, without wondering if every line of code, every piece needed, is following specified rules and regulations.

Building To Code

If building codes set the minimum standard for construction, then AWS Config's conformance packs are more specific enforcements for those working in specialized areas. Just as homes built in San Francisco or Florida must meet regulations designed to protect buildings from earthquakes or hurricanes, respectively, financial organizations and healthcare organizations must meet Federal Financial Institutions Examination Council (FFIEC) and Health Insurance Portability Accountability Act (HIPAA) regulations.

MajorKey provides the template for these kinds of regulations. Whether an enterprise needs a HIPAA-compliant, FFIEC-compliant, or any other regulatory-compliant environment, the pre-built guidelines and automation instill confidence that the rules are being met and followed. Every time a new account or environment is created, it is consistently meeting those necessary regulations and ensuring that no one is cutting corners during construction to just get it done under the pressure of time and limited resources. And when the "building inspector" shows up in the form of an audit, these tools provide the ability to pull compliance reports and show that guardrails are in place and actively monitored.

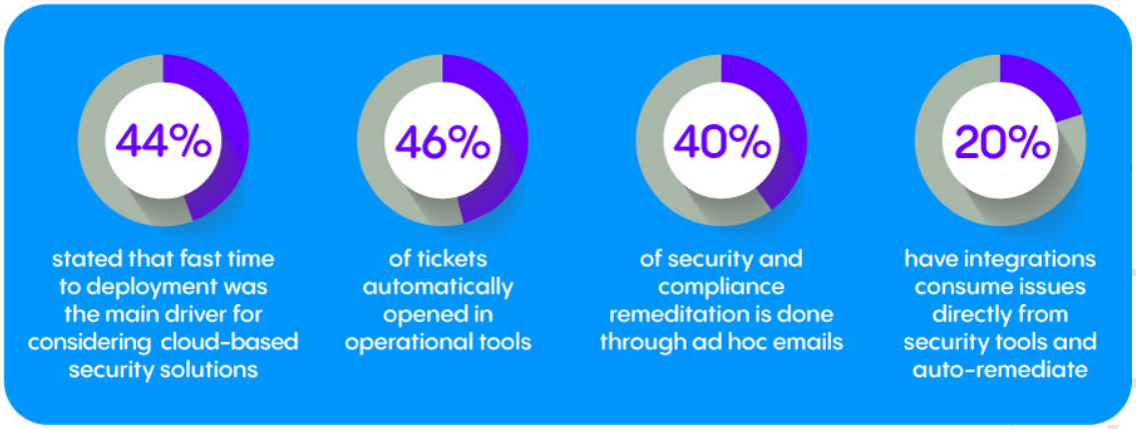
In AWS Config, you establish those rules and regulations. But what happens if a rule is broken?

Installing a Home Security System

Security isn't only setting up a guardrail. It's monitoring that guardrail to see if anything is breaching that line, putting your enterprise at risk. This is your enterprise's "home security system"—alarms, cameras, smoke detectors, all automated to alert you when something is amiss. But your house alarm or fire detectors beep on their own. The cameras are on their own network.

With your foundation set through Control Tower and Config, you can gain the full view of all your security alerts and statuses through AWS Security Hub. If your virtual camera setup has a blindspot—say, a newly deployed server that is publicly facing the web and shouldn't be—Security Hub will alert you. Instead of switching back-and-forth between all the tools you are using to protect your cloud environment, Security Hub provides a single place that aggregates, organizes and prioritizes your security alerts or findings from multiple services.

Organizations increasingly recognize the advantages of cloud native security solutions. ***Cybersecurity Insiders' 2020 AWS Cloud Security Report*** states that 44 percent of cybersecurity professionals surveyed cited fast time to deployment as the main driver for considering cloud-based security solutions. However, not fully integrating Security Hub with issue tracking puts enterprises at greater risk of missing critical security alerts. According to the report, less than half of tickets are automatically opened in operational tools like ServiceNow or Jira, while only one in five have integrations that take issues directly from security tools and auto-remediate. A concerning 40 percent of security and compliance issues are handled in ad hoc emails.

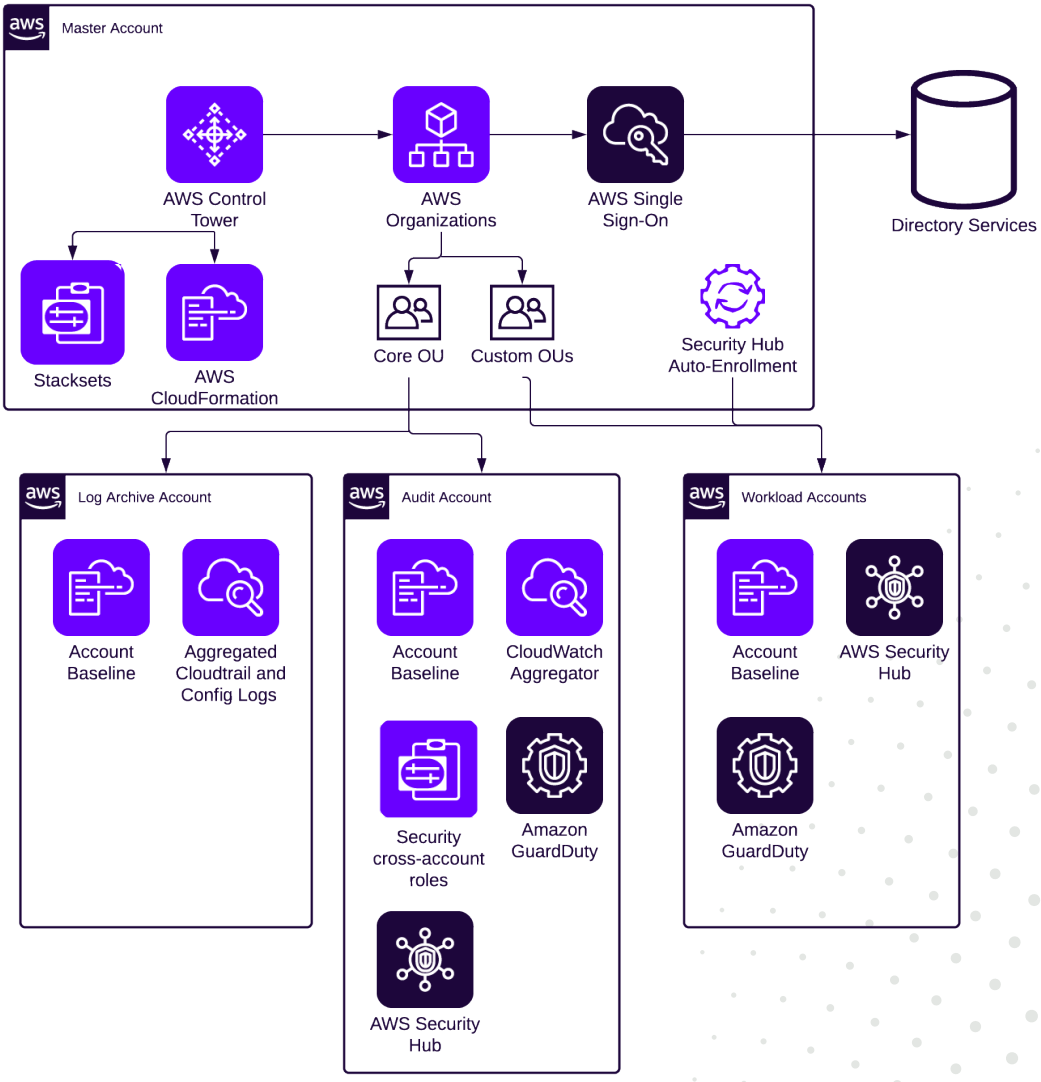


MajorKey expertly weaves together enterprise tools and systems with Security Hub, so that its customers are automatically tracking and notified of any potential issues. For instance, all issues caught by Security Hub can be automatically sent to security incident management tools, like ServiceNow ITSM or Atlassian Service Management, for tracking and project management. MajorKey's tested and proven automation gives DevSecOps teams the comfort of knowing that there are no blindspots in their security monitoring.

Case Study

In August 2020, a MajorKey client faced with a November 2020 deployment deadline underwent an AWS security audit that found several security issues that could expose the underlying application. They lacked multi-factor account authentication, security guardrails for compliance, additional logging, monitoring and alerting across the accounts, and visibility tracing if a bad actor got into the account.

In a 30-day rapid activation of AWS Security Services including Control Tower, Config and Security Hub, along with SSO and GuardDuty, MajorKey deployed a secure multi-account model with out-of-box guardrails, centralized logging and auditing. The client's email and software suite were integrated with AWS SSO. Alerts and notifications were set up through Security Hub. And critical job-based identity management access was established, so that only the proper accounts could access admin-level systems.



Within just four hours of activating the new system, MajorKey identified an additional 40 critical security issues that needed to be remediated before the November deployment. All security events were integrated with the client's issue and project tracking software, so that they would integrate into their existing notification and ticket assignment workflow, ensuring every issue would be brought to the client's attention for resolution.

The Comfort and Confidence of Security

With MajorKey at the helm harmoniously weaving together AWS Security Hub, Control Tower and Config, enterprises are scaling and growing with confidence—freeing up teams to focus on innovation instead of administration. Focusing on creating IP while having the peace of mind that they are secure from every angle. Enterprises stay strategic and focus now on growing and best serving their customers with certainty that the cloud foundation of those they serve is strong.

It's time to free up your teams to focus on innovation instead of administration. Don't wonder if you will meet compliance or audit requirements... know it.