Digital Transformation and IT Modernization for Elections in AWS

June 16, 2021

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

This paper has been archived

For the latest technical content, refer to the AWS Whitepapers & Guides page:
https://aws.amazon.com/whitepapers

Contents

Abstract

This whitepaper provides the elections community with an understanding of how cloud-based technologies such as artificial intelligence and machine learning, along with consumer Alexa-enabled devices can be used to help educate voters and facilitate accessibility. It includes security best practices that align with the National Institute of Standards and Technology's Cybersecurity Framework. We also share sample case studies, use cases, and reference architecture across AWS elections customer segments.

This content is intended for national, state/provincial, and local elections officials; elections technology providers; cybersecurity professionals; risk management officers; or other organization-wide decision makers considering how to improve an existing cybersecurity framework in their organization, and/or DevOps personnel who plan to develop, deploy, assess, or secure solutions in Amazon Web Services.

Introduction

Elections have long been among the most vital administrative processes underlying democratic governments, and today they face an array of sophisticated threats designed to undermine system integrity and public trust. In 2002, the U.S. Congress passed the Help America Vote Act (HAVA) to help states improve election systems and practices.[1] HAVA was the first piece of federal legislation to provide funding for election administration improvements, and states used the opportunity to enhance the security, accessibility, accuracy, and reliability of election systems.[2] Most recently, Congress appropriated HAVA Election Security Funds in 2020 and 2018 to provide states with additional resources to secure and improve election systems. The US Election Assistance Commission (EAC) provides guidance for each state's application and use of such election security grants. The implementation of HAVA helped improve the voting experience for all Americans over the last two decades. However, confirmed hacking attempts and breaches from the 2016 election highlight that threat actors are determined and have the advanced capabilities to disrupt our democratic process.[3] This threat continued in the 2018 midterm elections[4] and 2020 presidential election.[5]

The potential cyber threat posed by international adversaries combined with aging infrastructure and technology adds to the struggle faced by election officials. Decisions about what to build, buy, or consume as a utility are already difficult due to competing priorities, lack of funds, and breadth of technical options. However, these decisions are now muddled with political biases and fear, uncertainty, and doubt (FUD). Fortunately, the commitment by election officials, policymakers, and other political stakeholders to establish a dynamic electorate in a secure, scalable, resilient, and cost-effective way is not partisan.

In addition, the coronavirus pandemic upended the U.S. elections process in 2020. States across the country had to postpone primary elections and evaluate vote-by-mail and electronic voting options. Because of this, it was imperative that elections technology vendors and local election officials built or had access to secure systems that could maintain the integrity of the elections process and trust of the public. To help election administrators navigate the challenges arising from the pandemic, Congress appropriated $400 million as part of the CARES Act for coronavirus-related election expenses.[6]

This paper is designed to assist four primary customer groups navigate these evolving environments:

- **Election administrators** which may include national and provincial level elections officials outside of the US, US secretaries of state, boards of elections, county election registrars and clerks, and related stakeholders who are tasked with overseeing constituent voting and related administrative processes. Election administrators' functions include voter registration, election night reporting, candidate certification verification, and campaign finance reporting.
- **Political campaign administrators** include national and local committees that manage candidate nominations and influence the decision-making process among the electorate on behalf of a particular party or individual.
- **Civic engagement organizations** consist of nonprofit organizations focused on increasing voter registration and participation during elections. These organizations launch comprehensive initiatives ahead of the presidential and mid-term elections.
- **AWS Independent Software Vendors (ISV) and AWS Partner Network (APN) Technology partners** are those companies and nonprofits who build and offer technical solutions across a wide variety of elections process, including voter registration, voter education tools, electronic pollbooks, polling place lookup, sample interactive ballots, ballot marking, electronic ballot delivery, election night reporting, campaign finance, and campaign management.

Customer Mission

The AWS Elections vertical works backward from the mission of our elections customers, which is to:

1. Encourage citizen participation in elections through efficient solutions and services;
2. Ensure the integrity of free, fair, and secure elections;
3. Enhance public confidence and protect democracy;

The Elections vertical's cross-functional team of domain experts helps to earn customer trust and enhance public confidence in the integrity of electoral processes. As trusted advocates of the mission, the Elections vertical promotes elections-related successes by helping customers innovate, optimize their AWS infrastructure, and increase security and performance. The Elections team pays attention to competitors, but obsesses over customers.

The AWS elections cross-functional team consists of industry experts with experience as elections officials and in technology companies supporting elections, as well as

security experts with experience in senior government roles and technology providers. Since its inception, the AWS Elections team has established relationships and conducted executive briefings with federal, state, and local election leaders. Additionally, the team has built and grown a comprehensive network of APN partners with AWS-powered SaaS solutions deployed with election customers across counties and states nationwide. With guidance from the AWS elections team experts and deployment of AWS-powered solutions, elections customers can consume secure and resilient technology and infrastructure as a utility. Consuming cloud-based solutions as a utility means that customers only pay for what they use on a monthly basis, rather than expending large capital investments in hardware, software, and data center facilities to support a periodic process with large dwell times. Utility consumption also provides customers with the agility to quickly adapt to unexpected business and market changes, such as what the COVID-19 pandemic brought. With lean IT staffs, customers are able to focus their technical staff on their specific mission and not spend a lot of time on the undifferentiated heavy lifting of basic systems management.

Expanding voter education and accessibility with AI and ML solutions

As the demographic makeup of the US and international electorate shifts, expectations for levels of engagement and accessibility have evolved. At the same time, global events and national disasters are forcing government organizations to change the way they interact with constituents. There is a desire for new communication channels which allow remote interaction.

AWS enables election stakeholders to offer personalized omni-channel interactions that leverage a single source of truth through the use of artificial intelligence-based solutions. Validated information can be disseminated based on voter preferences and accessibility needs through multiple channels including web, mobile, social, email, call centers, opt-in text notifications, Alexa voice, chatbot, and others.

These new communication vehicles anchor a data-driven omni-channel strategy adopted by many state and local government election customers, to modernize the voter experience and help deliver information securely and accurately. The AWS Global Infrastructure helps state and local government to deliver these services in a secure, reliable, and highly scalable manner.

Delivering a great experience for constituents with AWS

Amazon Web Services (AWS) empowers election officials and other political stakeholders to focus on the core needs of the dynamic electorate in a secure, scalable, resilient, and cost-effective way. This allows election stakeholders to focus on these core needs rather than on building and maintaining the underlying infrastructure to support their mission-critical efforts.

Artificial intelligence and machine learning solutions from AWS can help elections administrators deliver a great digital experience for constituents and voters during elections.

Specifically, solutions built with services such as Alexa, Amazon Lex, and Amazon Connect can be designed to provide intuitive interfaces and easily accessible election information to voters. These services are built on top of the AWS Global Infrastructure, and are designed to provide high availability, reliability, and scalability necessary for you to ensure that voters can access information when they need it.

Alexa

Alexa is Amazon's cloud-based voice service. It is available on hundreds of millions of devices from Amazon and third-party device manufacturers. With Alexa, you can build natural voice experiences that offer customers a more intuitive way to interact with the technology they use every day. We offer a collection of tools, APIs, reference solutions, and documentation to make it easier to build for Alexa.

As a result, Alexa is a powerful tool for improving voter engagement and accessibility. Government organizations can build custom Alexa election skills for their use case or benefit from native Alexa election features.[7] Today, US constituents can ask Alexa general questions such as, “Alexa, when is the next debate?” or "Alexa, how does [candidate name] stand on Education?" In delivering these capabilities, Amazon federates across hundreds of information sources, and collaborates with nonpartisan organizations to provide customers with information on polls, ballots, results, and more. Alexa herself does not have opinions on politics or candidates.

Elections officials can also build custom Alexa skills to deliver specific information to their constituents. For example, constituents can ask questions such as, “Alexa, what is the voter registration deadline?” or “Alexa, how to I request an absentee ballot?”

For elections organizations that want to build custom skills, there are several options. Alexa Skill Blueprints[8] provide templates for common use cases and are the fastest way to build a custom skill. Or, for more complex use cases and maximum flexibility, government customers can leverage the Alexa Skills Kit[9] to build Alexa skills, which are backed by AWS Lambda functions. In either case, these Alexa skills can be published to the Alexa Skills Store so that constituents can find and benefit from them. Elections officials can also work with APN Partners to develop custom Alexa skills, by building a repository of frequently asked questions.

Amazon Lex

Amazon Lex[10] can improve voter accessibility by providing natural-language understanding (NLU) through multiple channels, including web, mobile, SMS, social media, and contact center. The same backend Amazon Lex *bot* can be used for each of these channels. This is a significant benefit for constituents. They will have a consistent experience and receive identical information across channels.

For example, an elections office could publish a Questions and Answer bot[11] about the upcoming election using Amazon Lex on their public website. The Amazon Lex bot invokes an AWS Lambda function. This function subsequently invokes a backend Amazon DynamoDB database (or it could invoke an existing API). The elections office could then publish the same bot to their social media account[12], so that Amazon Lex could handle inquiries received there. The elections office could create and advertise a phone number to which constituents can send SMS messages, and Amazon Lex would read and respond to those messages. Finally, the elections office could create interactive voice functionality in their Amazon Connect call center with the same Amazon Lex bot, so that constituents can call in and have the same Questions and Answers experience using the phone.

In each case, the same Amazon Lex bot is used and the same backend database (DynamoDB) is queried to receive the latest information. Constituents have a consistent experience and always get data from a single source of truth.

Voice-first technologies like Amazon Lex and Alexa utilize NLU. NLU is artificial intelligence centered on recognizing patterns and meaning within human language. With NLU, computers can deduce what a speaker actually means, and not just the words they say. In short, it is what enables voice technology like Alexa to infer that you're probably asking for a local weather forecast when you ask, "Alexa, what's it like outside?"

Amazon Connect: Cloud-based call center

A call center is another critical channel for interacting with constituents to provide timely election information. Unfortunately, maintaining insufficient call center staff during peak times (like election day) may result in long hold times which can prevent voters from getting the information they need. Amazon Connect is an easy-to-use omni-channel cloud contact center that helps companies provide superior customer service at a lower cost.[13] Amazon Connect is AI-enabled by default, allowing AI services to be connected and immediately used. Specifically, Amazon Lex can be integrated immediately to automate interactions and improve customer service. For example, Los Angeles County recently moved a call center to Amazon Connect and was able to automate 20% of calls and reduce hold times.[14] Amazon Connect can even be used to conduct outbound call campaigns to update voters on the latest election information, or remind constituents of an upcoming election to increase voter participation.[15]

Amazon Connect has natural text-to-speech built in and can be used to create personalized messages for constituents. This capability is powered by Amazon Polly, which uses advanced deep learning technologies to synthesize natural sound human speech. Amazon Polly provides a variety of different voices in multiple languages[16] so that callers hear natural voices and accents in their own language.

Finally, Amazon Connect allows state and local election officials to be responsive to changing constituent demands, even on election day. With Amazon Connect, customers can make changes in minutes to manage flows using the intuitive UI that allows administrators to create voice and chat contact flows, without any coding, rather than custom development that can take months and cost millions of dollars.

The services mentioned above are built on top of the AWS Global Infrastructure, which provides a high degree of availability and reliability for constituents. The North Carolina State Board of Elections uses AWS to run a highly reliable elections application. “For us, the overarching feature of using AWS is reliability. On election night, I trusted that I wouldn’t have to worry about capacity or load, and could instead focus on delivering results,” said Marc Burris, Chief Information Office, NC State Board of Elections and Ethics.

Improving the efficiency of operating an election

Beyond improving the voter experience, Customers can use AWS to improve the efficiency of operating elections for national, state/provincial, and local government in three ways:

1. Elections administrators and IT professionals can use AI and automation to enable self-service to improve the efficiency of agents.
2. Elections offices can take advantage of utility-based pricing and the elasticity of AWS to significantly reduce the cost of operating an election.
3. With cloud-based solutions, elections administrations can ensure business continuity for critical events, even during emergencies and natural disasters, such as floods, fires, hurricanes, tornadoes, earthquakes, or pandemics.

First, elections administrators can take advantage of AI capabilities from AWS to better enable their constituents to conduct self-service information gathering for many election-related questions. Amazon Lex, Lambda, and Alexa Skills are able to answer many of the questions for constituents on many different platforms, before ever reaching a person. For example, a voter might be able to ask Alexa for the nearest polling location or to check on voter registration status. Or a voter might send an SMS message to an Amazon Lex chatbot to get the same information. Finally, a voter might call into an Amazon Connect contact center and interact with a NLU-enabled chatbot. These self-service capabilities mean that agents will spend less time on repetitive, low value interactions and more time on complex calls.

In addition, a single Amazon Lex chatbot and Lambda (the compute service that powers Alexa) function can be used to interact with constituents through multiple channels. This creates a single source to update and configure. Election officials can more efficiency utilize developer resources for implementation and even offload configuration to power users with simple-to-use interfaces for Amazon Lex and Alexa Skills. These services allow a single source of configuration to connect with the many constituents facing interfaces like Facebook, a website, a call center, etc. without having to choreograph a complex deployment across all these systems.

Second, elections offices can take advantage of utility-based pricing and the elasticity of AWS services to significantly reduce the IT costs of interacting with constituents during an election. Organizations used to overprovision to ensure they had enough capacity to handle their business operations at the peak level of activity. Now, AWS customers can provision the amount of resources that they actually need, knowing they can instantly

scale up or down along with the needs of their business, which also reduces cost and improves their ability to meet constituent's demands.

Amazon Connect's pricing is based on a per minute/chat price and there are no licensing costs. For election officials, this means the price of the call center will scale up and down throughout the election season based on utilization. There is no requirement to commit to long-term contracts and election officials can shut off their use of Amazon Connect at any time. Officials can bring on additional staff and have them answering calls in a matter of minutes, but if the phones do not ring then there is no fee or penalty for having the additional unused agents. This allows the cost of the call center to match the pattern of the election personnel better than traditional call center technologies. Other AI-based AWS services, like Alexa and Amazon Lex, provide the same elasticity and incur costs only when they are used by constituents.

Finally, cloud-based services mean that government organizations can continue to provide public services for constituents even during highly unusual natural disasters. Agents can take calls from an Amazon Connect call center from anywhere - even at home or from a coffee shop. The only requirement is a computer and internet connectivity. This is a significant benefit for business continuity compared to legacy contact center solutions which require physical equipment and agents to be on-site.

Measuring results and iterating to improve engagement

Any effort to improve voter education and accessibility must have a way to define and measure the results. How are voters getting information currently? What methods would they prefer to use? Is the information they're receiving accurate? Is it resulting in changed behavior (for example, an increase in mail-in ballot requests after a campaign to inform voters that restrictions are being relaxed)?

In order to answer these and many other questions, data must be collected from a variety of sources, analyzed, and presented to election officials in a clear and actionable manner. AWS provides a number of tools that facilitate this collection and processing, leveraging AI/ML algorithms to do so.

Amazon Connect

Amazon Connect provides a number of basic metrics that measure items such as the total call volume, average call duration, and amount of time a contact spends in each possible state (for example, on hold, in queue, talking to agent). You can analyze this information to look for desired outcomes, such as a decrease in call volume after the roll

out of a new FAQ website intended to answer basic questions so that voters do not need to call for information.

For deeper analysis of call center effectiveness, Contact Lens for Amazon Connect is a set of machine learning (ML) capabilities integrated into Amazon Connect. Using AWS ML natural language processing (NLP) and speech-to-text, Contact Lens for Amazon Connect transcribes contact center calls to create a fully searchable archive and surface valuable insights. With Contact Lens for Amazon Connect, customer service supervisors can quickly and more easily discover emerging themes and trends from voter conversations, directly in Amazon Connect.

The machine learning models that power Contact Lens for Amazon Connect have been trained specifically to understand the nuances of contact center conversations including multiple languages and custom vocabularies. With Contact Lens for Amazon Connect, supervisors can conduct fast, full-text search on call and chat transcripts to quickly troubleshoot voter issues. They can also leverage call and chat-specific analytics, including sentiment analysis and silence detection to improve customer service agents' performance. Contact Lens for Amazon Connect will also allow supervisors to be alerted to issues, like when an agent is unable to help a frustrated caller, giving them the ability to intervene before the call ends having a poor experience. These capabilities can be used both to improve agent training and adjust messaging to voters.

Amazon Lex

Using Amazon Lex[17], a service that allows you to create intelligent conversational chatbots across multiple channels (web chat, SMS, voice), you can turn your call center contact flows into natural conversations that provide personalized experiences for your callers. Using the same technology that powers Amazon Alexa, an Amazon Lex chatbot can be attached to your contact flow to recognize the intent of your caller, ask follow-up questions, and provide answers.

You can track metrics for your bot on the Monitoring dashboard in the Amazon Lex Console. Currently, you can track the number of missed utterances, request latency, and traffic by channel for your bot. You can view a list of utterances not recognized by your bot or 'missed utterances'. With these monitoring capabilities, you can view how voters are interacting with the bot and make improvements, such as adding more answers so that unanswered questions decrease over time, or providing alternate phrasings of questions. These metrics also provide insight into areas of voter confusion, and when it might be appropriate to clarify with further education (such as via an outreach with Amazon Pinpoint).

Bot responses can be paired with “was this helpful” questions to get feedback from voters on whether or not their queries were sufficiently answered. Counts of calls/chats that are transferred to a human agent also measure answer sufficiency, and can be used to track if automated systems are reducing load on call center agents. Finally, each interaction can conclude with an optional survey to get further insight into the adequacy of the information being presented, as well as the effectiveness of the bot.

Amazon Pinpoint

In addition to receiving questions and feedback from voters though Connect, Amazon Pinpoint[18] enables you to deliver voter-centric engagement experiences. Amazon Pinpoint is built on the highly scalable infrastructure of AWS, allowing you send messages through multiple channels, such as SMS or voice, with confidence. With rich analytics, easy-to-use campaign and journey tools, and multiple engagement channels, Amazon Pinpoint helps you reach voters with the right message at the right time.

Combine proprietary data, third-party data, and real-time data from sources such as public databases, DMV records, VRS databases in one place for a holistic view of your voters. Use that deep understanding to create tailored audience segments, and then send those segments contextually relevant, personalized messages through the channel they prefer. You can also create journeys—end-to-end engagement experiences that send personalized content based on voters' interactions.

Amazon Comprehend

Amazon Comprehend[19] is a natural language processing (NLP) service that uses machine learning to find insights and relationships in text. Amazon Comprehend lets you integrate Amazon Pinpoint with other AWS services to create a solution that meets your unique needs. Machine learning is particularly good at accurately identifying specific items of interest inside vast swathes of text, such as letters, emails, customer service interaction logs, even social media feeds. It can learn the sentiment hidden inside language (identifying negative voting experiences, or positive customer interactions with customer service agents), at almost limitless scale.

One example of Amazon Comprehend in action is an AI-Driven Social Media Dashboard,[20] a solution that automatically provisions and configures the AWS services necessary to capture multi-language tweets in near real-time, translate them, and store both the raw and enriched datasets durably in the solution's data lake. You can then analyze this data and create meaningful dashboards powered by Amazon QuickSight to

visualize and understand voter's feelings about the election process, and gain actionable insights in real time (for example, if there are technical problems at a polling station).

All of the above data sources can be joined with data ingested from other systems available to election officials, such as voter registration systems (VRS), to provide a rich picture of voter needs. For example, an Amazon Pinpoint outreach campaign educating voters on new rules for mail-in ballot requests can be measured against reports from the VRS to see if there has been an increase in requested mail-in ballots, and a decrease in rejected requests.

Or on election day, poll station activity collected by electronic poll books can be analyzed along with trending statements in social media to determine a health metric for each poll station, insight that can be used in real-time to divert resources where they are needed most.

AWS Lake Formation and Amazon QuickSight

With all of the preceding solutions, data needs to be catalogued and stored in a centralized location where it can be made easily available to those who need it. AWS Lake Formation[21] is a service that makes it easy to set up such a data lake. A data lake is a centralized, curated, and secured repository that stores all your data, both in its original form and prepared for analysis. A data lake enables you to break down data silos and combine different types of analytics to gain insights and guide better decisions.

With Lake Formation, you can move, store, catalog, and clean your data faster. Point Lake Formation at your data sources, and Lake Formation crawls those sources and moves the data into your new Amazon S3 data lake. Lake Formation organizes data in Amazon S3 around frequently used query terms and into right-sized chunks to increase efficiency. Lake Formation also changes data into formats, like Apache Parquet and ORC, for faster analytics. Also, Lake Formation has built-in machine learning to deduplicate and find matching records (that is, two entries that refer to the same thing) to increase data quality.

Using this data lake, you can run queries using Amazon Athena or Amazon Redshift to answer complex questions. The data can then be visualized on an Amazon QuickSight dashboard to gain actionable insights.[22] Amazon QuickSight lets you easily create and publish interactive dashboards. You can choose from an extensive library of visualizations, charts, and tables, and add interactive features such as drill-downs and filters. Possibilities include a geographic map of polling locations with colors

representing real-time views associated voter feedback, or a graph showing breakdowns by demographic of how various voter education channels are being utilized over time.

Further, QuickSight ML Insights uses AWS's proven machine learning and natural language capabilities to help you gain deeper insights from your data. These powerful, out-of-the-box features make it easy for anyone to discover hidden trends and outliers, identify key business drivers, and perform powerful what-if analysis and forecasting with no technical expertise or ML experience needed. In today's digitally transformed world, election officials increasingly need the ability to see how their voter education efforts are being received, and AWS provides the capability to gain valuable insights.[23]

Amazon Translate

Amazon Translate helps election administrators meet their mission of delivering bilingual election materials, as required under Section 203 of the Voting Rights Act and changing Census data.[24] (Amazon Translate also helps campaigns and civic engagement organizations with expanded voter outreach solutions. Amazon Translate is a neural machine translation service that delivers fast, high-quality, and affordable language translation. Neural machine translation is a form of language translation automation that uses deep learning models to deliver more accurate and more natural sounding translation than traditional statistical and rule-based translation algorithms. With Amazon Translate, elections organizations can localize content such as websites and applications for diverse users, easily translate large volumes of text for analysis, and efficiently enable cross-lingual communication between users. With the power of machine translation, Amazon Translate is about a 1000x cheaper than having content manually translated by a professional translator.

Intento recently ranked Amazon Translate as the top machine translation provider in 2020 across 14 language pairs, 16 industry sectors and 8 content types.
https://aws.amazon.com/translate/

Securing elections workloads

Cybersecurity and privacy are essential to the effective management of democratic elections and campaigns, globally. Amid unclassified reports from the US intelligence community that foreign actors attempted to tamper with US voting systems in at least 39 US states during the 2016 presidential election,[25] the vulnerabilities of legacy equipment

and their inadequate supporting infrastructure have garnered renewed scrutiny. As a result, in January 2017, the US Department of Homeland Security (DHS) declared the electoral system as "critical infrastructure," which places election equipment in the same category as the US power grid or financial sector.

Later, in September 2017, DHS notified at least 21 US states of foreign efforts to tamper with their election systems in 2016. The Election Infrastructure – Sector Coordinating Council (EI-SCC) is a group of technology providers with subject matter expertise that advises DHS on election security and critical infrastructure.

Since 2017, the AWS elections team has been actively involved with the EI-SCC to support elections technology vendors and elections officials operating in the Cloud. The EI-SCC is one of many sector councils (for example, financial services and healthcare) established to share threat information between the federal government and council partners, advancing risk management efforts, and prioritizing focus of services available to sector partners in a trusted environment. This mission will be accomplished through voluntary actions of the infrastructure owners and operators represented in the Council, as set forth in Presidential Policy Directive/PPD-21[26] and related authorities. The EI-SCC serves as the principal asset owner and works with other private critical infrastructure sectors, as well as with the Department of Homeland Security (DHS), the US Election Assistance Commission (EAC), state/local/tribal governments (SLTTs), and the Election Infrastructure Sector Government Coordinating Council (EI-GCC).

AWS understands the obligations of elections administrators and has worked diligently to help election administrators understand what configuration & compliance options are available in AWS that can help them meet their security requirements. Security and privacy are top priorities for AWS. Our global infrastructure is designed and managed to meet recognized-security best practices and over 90 international standards. AWS provides an array of security and privacy services that allow customers to automate strict governance of their systems and data, monitor for configuration changes and threats, and automate response actions. AWS meets over 90 international compliance standards, certifications, frameworks, and authorizations such as FedRAMP in the US and ISO 27001/27017/27018 internationally, and provides services that adhere to the high privacy bar and data protection standards required of data processors by the GDPR for data privacy in the EU. AWS offers services and resources to help our customers meet these same standards, certifications, and frameworks.

Cybersecurity framework

Many organizations find that it's helpful to use a government or industry-created framework when they evaluate new and emerging technologies. In particular, the National Institute of Standards and Technology's (NIST) voluntary Cybersecurity Framework (CSF) represents a thoughtful collaboration between the government and private sector. The collaboration permits entities to pick and choose the components of the framework that best meet their cybersecurity objectives. This allows a comparison between unbiased objectives and standards with the new technology rather than comparing to the organization's existing technology where people may have emotional bonds.

Introduced in 2014, the CSF has gained international recognition and has helped AWS customers, especially those who operate critical infrastructure. Organizations have used CSF to help build their cybersecurity program, assess their current cybersecurity state, determine where they want to be, and prioritize policies and procedures, procurement, staffing, and training.

The CSF is composed of three parts: The Core, Tiers, and Profiles.

The Core represents a set of cybersecurity practices, outcomes, and technical, operational, and managerial security activities that support five risk management functions – Identify, Protect, Detect, Respond, and Recover. The Core consists of five functions, 23 categories, and 108 subcategories (outcome-based security activities).

The Tier model describes the consistency and sophistication for how each activity is performed.

The Profile model demonstrates alignment of the Core with business requirements, risk tolerance, and resources to determine an organization's current and desired postures. Together, these three elements enable organizations to prioritize and address cybersecurity risks consistent with their business and mission needs.

Incorporating elements of a framework that help align an organization's security program to its mission and business needs is essential. Frameworks such as the CSF can facilitate that.

For more information about the CSF and how it can be used with our services, see Aligning to the NIST CSF in the AWS Cloud. The whitepaper contains a worksheet that

maps each of the 108 CSF subcategories to AWS services and capabilities that can be used to help improve cybersecurity posture in alignment with CSF.

Privacy

The protection of personal data (e.g., names, addresses, party affiliations, signatures) collected and used in the course of your election related activities is another critical aspect to consider for your cybersecurity program. Trust among election officials and APN partners can seriously be impacted if personal data is not handled responsibly in accordance with applicable laws, regulations, and best practices.

NIST's *Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (version 1.0) (Privacy Framework)* helps organizations plan and manage their privacy risks and is meant to be used in conjunction with the CSF.[27] Similar to the NIST CSF, the three primary components of the NIST Privacy Framework are the Core, Profile, and Implementation Tiers. Election officials and their elections technology APN partners might consider using all five CSF functions in tandem with the Privacy Framework's Identify-P, Govern-P, Control-P, and Communicate-P functions to manage both their privacy and cybersecurity risks. [28]

Also, if you are migrating your elections operations to the cloud, AWS has mapped the NIST Privacy Framework to the *AWS Cloud Adoption Framework*, which helps create an enterprise-wide cloud migration plan for your organization.[29]

Elections and the shared responsibility model

Election officials and elections technology APN partners can align to the NIST CSF in AWS through the shared responsibility model. Security and Compliance is a shared responsibility between AWS and the customer, and this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud. In traditional on-premises data centers and networks, the organization is responsible for everything about the security and operations of their technology stack. This spans physical security, technical security of the network, servers, and storage; applications and data.

In the cloud, however, AWS is responsible for protecting the infrastructure that runs all AWS Cloud services, which is composed of the hardware, software, networking, and facilities that run AWS Cloud services. This reduces what the customer is responsible for and the level of effort required to implement and manage security controls, allowing for the customer to focus more precisely on protecting their assets and data in the

cloud. In addition, AWS complies with over 90 international compliance standards, frameworks, regulations, and authorizations to maintain the security and compliance of the cloud and help customers meet the requirements applicable to them.

Customer responsibility is determined by the AWS Cloud service that a customer selects. Customers continue to manage who has access to their data in the cloud, whether the data is encrypted in transit or at rest, and the securing and updating of the applications they buy or build. AWS services can help customers perform their responsibilities, such as AWS Key Management Service (KMS), which provides a FIPS 140-2, Level-2 validated method to manage encryption keys. You can bring your own keys (BYOK) or use KMS-managed keys to auto-generation, rotation, and destruction. Customer responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations.

The following discussion describes examples of how AWS can help you meet your election security objectives through alignment with the CSF. If you are interested in learning more, review the whitepaper and associated workbook,[30] and contact your AWS account manager to discuss specific elections offerings.

AWS account Solutions Architects and Technical Account Managers (TAM), for those customers with enterprise support, can help you design an architecture that incorporates AWS services and offerings to meet each of the five functions of the CSF (Identify, Protect, Detect, Respond, and Recover). If you need more hands-on, long-term engagements to train your staff and implement a secure architecture, AWS Professional Services and AWS APN Consulting Partners have several offerings that can help.

CSF functions and elections

Identify

One category of the Identify function is conducting security risk assessments. An example for this function is the Risk Assessment 1 (ID.RA-1) subcategory, where asset vulnerabilities are identified and documented. There are a few AWS services that you can use to perform this activity, such as AWS Systems Manager, AWS IAM Access Analyzer, AWS Trusted Advisor, Amazon Inspector, and Amazon Macie.

Election officials and elections technology partners should also incorporate privacy by design concepts with their applications and infrastructure. In addition to general security

risks, it is important to identify specific privacy compliance requirements and risks to personal data in their systems, applications, and networks and implement appropriate mitigations.

AWS Trusted Advisor

Trusted Advisor is a tool that provides real-time guidance to help you provision your resources following AWS best practices in five categories: Cost Optimization, Performance, Security, Fault Tolerance, and Service Limits. For more information, see AWS Trusted Advisor.

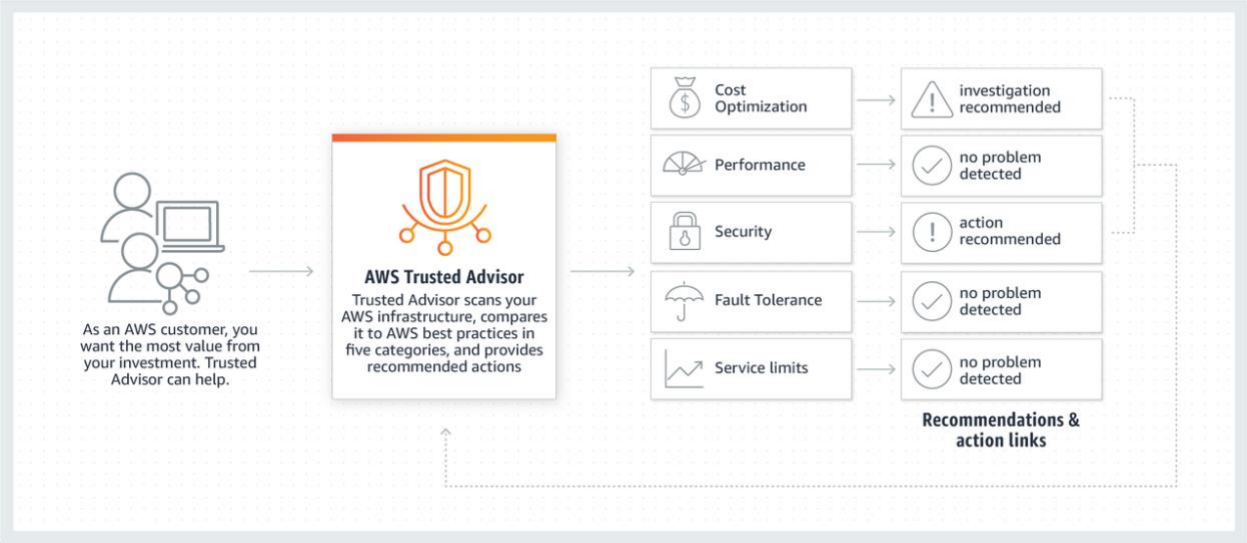

Figure 1 – Summary of AWS Trusted Advisor

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API. For more information, see Amazon Inspector.

Amazon Macie

Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

Macie automates the discovery of sensitive data at scale and lowers the cost of protecting your data. It automatically provides an inventory of Amazon Simple Storage Service (Amazon S3) buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with AWS accounts outside those you have defined in AWS Organizations. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII). Macie's alerts, or findings, can be searched and filtered in the AWS Management Console and sent to Amazon CloudWatch Events for easy integration with existing workflow or event management systems, or to be used in combination with AWS services, such as AWS Step Functions to take automated remediation actions. For more information, see Amazon Macie.

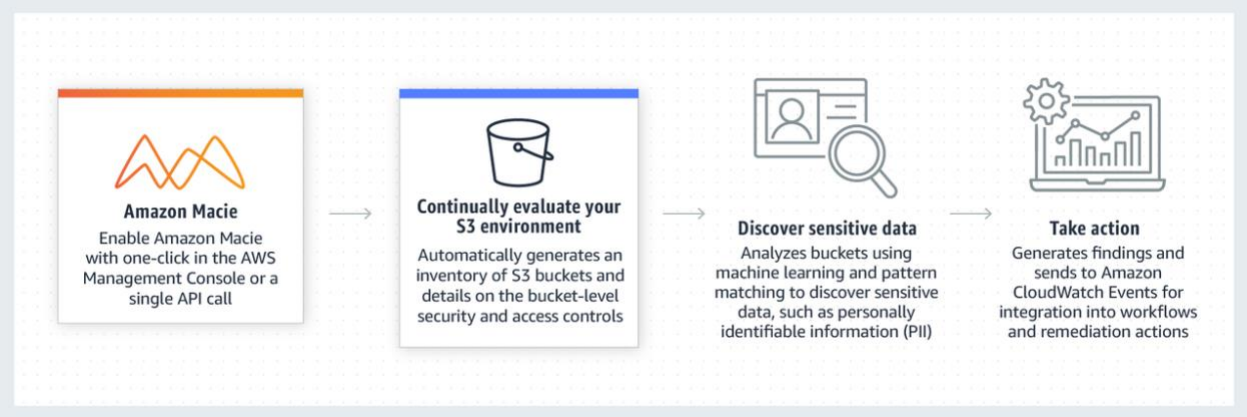

Figure 2 – Summary of Amazon Macie

AWS also has a couple of engagement offerings that can help customers identify vulnerabilities, not just from hackers, but risks to the application's availability if demand is higher than expected or there is some natural or artificial disaster.

Security and resiliency-focused Well-Architected Review

The AWS Well-Architected Framework was developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars (operational excellence, security, reliability, performance efficiency, and cost optimization), the framework provides a consistent approach for customers and APN partners to evaluate architectures, and implement designs that will scale over time.

A security and resiliency-focused Well-Architected Review is an engagement where an AWS solutions architect or AWS partner will coordinate with you to assess a single elections application hosted in AWS and provide a report on the adherence to AWS

best practices as outlined in the framework. The report identifies strengths and opportunities to improve with recommendations. This report can be used by you, an APN Partner, or AWS professional services as a guide to implement changes in the environment to tighten security and improve resiliency. Contact your account manager to request a review. For more information, see AWS Well-Architected, with specific guidance in the security pillar and reliability pillar.

AWS Infrastructure Event Management

A structured program available to Enterprise Support customers (and Business Support customers, for an additional fee) that helps you plan for large-scale events such as product or application launches, marketing events, or elections. With Infrastructure Event Management, you get strategic planning assistance before your event, as well as real-time support during these moments that matter most for your business. Contact your account manager to request this offering. For more information, see AWS Infrastructure Event Management.

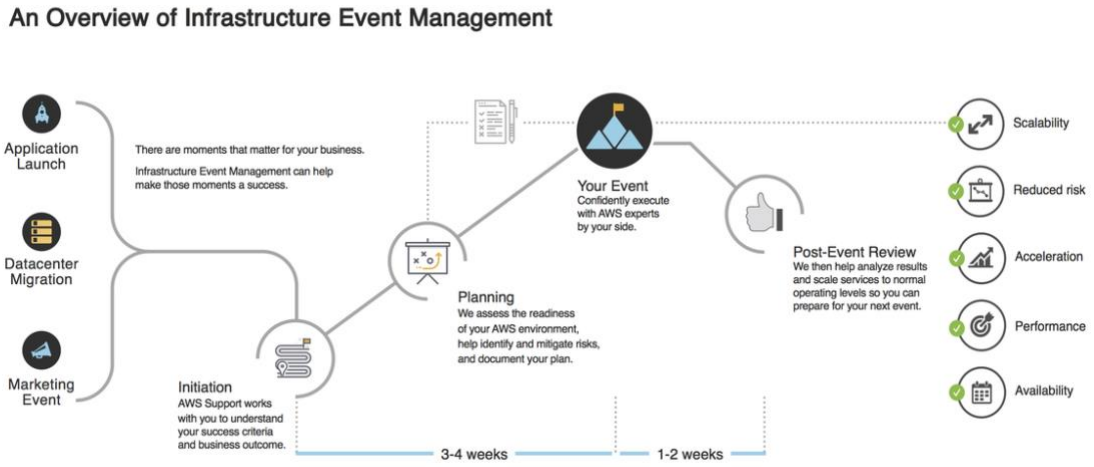

Figure 3 – Summary of AWS Infrastructure Event Management

AWS has the largest network of security partners who can serve as advisors or technology providers to meet the individual needs of each customer and across each of the five CSF functions. You can search through our partners by visiting our AWS Marketplace.

Protect

Protecting your elections infrastructure from unauthorized access is paramount. This includes access control, data security, and information protection processes and procedures. It is essential that the appropriate identity management, physical and data security, and Distributed Denial of Service (DDoS) protection services are incorporated into your cybersecurity and privacy risk management strategies. These services should be operated in accordance with well-documented data protection policies, processes, and procedures. There are a few examples that would be beneficial to highlight here, leveraging the shared responsibility model and AWS services.

Identity and Access Management (IAM) and Authentication

There are several CSF subcategories in this area that IAM and other AWS identity and authentication services can assist with. These include:

- **PR.AC-1** – identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes),
- **PR.AC-4** – Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties), and
- **PR.AC-7** – Users, devices, and other assets are authenticated (e.g., single-factor or multi-factor) commensurate with the risk of the transaction (e.g., to name a few.

For more information, see AWS Identity and Access Management (IAM), Amazon Cognito, AWS Single Sign-On, and AWS Certificate Manager.

Physical Security

The first is Access Control 2 (PR.AC-2) which requires that physical access to assets be managed and protected. In AWS, physical assets that comprise our infrastructure and services are the responsibility of AWS. For an application that wholly resides in AWS, this can be an expensive and complex burden that has been lifted from the customer. The customer would only retain responsibility for any physical assets they own outside of AWS such as desktops and laptops that may connect to the application hosted in AWS. For more information about our data center and physical security, visit Our Data Centers webpage.

Data Security

Another example from this function is Data Security 1 (PR.DR-1) which requires that data at rest be protected. Here, the customer is responsible for determining the level of protection required and for employing the appropriate AWS or third-party service to meet their requirement. AWS offers several encryption options such as client-side encryption, a few different server-side encryption options depending on the AWS storage services used, and key management services that are FIPS 140-2 Level 2 (AWS KMS) or Level 3 (AWS CloudHSM) validated. For more information about encryption services and options, see AWS Cryptography and PKI Documentation.

Perimeter Security

AWS offers several services for boundary protection to build a defense-in-depth strategy at each layer of the customer's application. This supports several CSF subcategories such as PR.AC-5 (Network integrity is protected).

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield: Standard and Advanced.

All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications. When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

AWS Shield Advanced

For higher levels of protection against attacks targeting your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator and Amazon Route 53 resources, you can subscribe to AWS Shield Advanced. In addition to the network and transport layer protections that come with Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall. AWS

Shield Advanced also gives you 24x7 access to the AWS DDoS Response Team (DRT) and protection against DDoS related spikes in your Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator and Amazon Route 53 charges. For information about AWS Shield and AWS Shield Advanced, see AWS Shield.

> In support of the 2020 US elections, we offered a tailored offering of our AWS Shield Advanced service specifically to elections customers at a discounted price and reducing the annual commitment to just two months.

AWS Web Application Firewall (AWS WAF)

AWS WAF helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define. You can get started quickly using Managed Rules for AWS WAF, a pre-configured set of rules managed by AWS or AWS Marketplace Sellers. The Managed Rules for AWS WAF address issues like the OWASP Top 10 security risks. These rules are regularly updated as new issues emerge. AWS WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of security rules. For more information, see AWS WAF – Web Application Firewall.

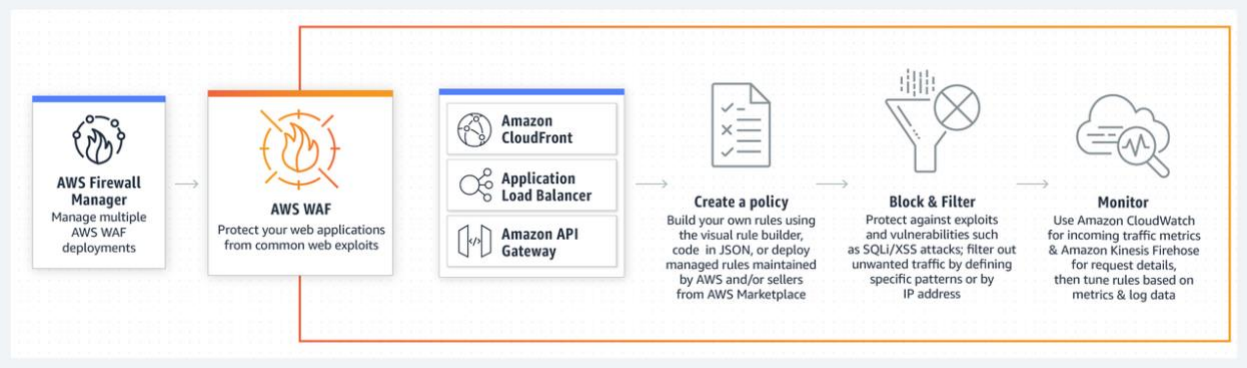

Figure 4 – Summary of AWS WAF

AWS Network Firewall

AWS Network Firewall is a managed service that makes it easy to deploy essential network protections for all of your Amazon Virtual Private Clouds (VPCs). The service can be setup with just a few clicks and scales automatically with your network traffic, so

you don't have to worry about deploying and managing any infrastructure. AWS Network Firewall's flexible rules engine lets you define firewall rules that give you fine-grained control over network traffic, such as blocking outbound Server Message Block (SMB) requests to prevent the spread of malicious activity. You can also import rules you've already written in common open-source rule formats as well as enable integrations with managed intelligence feeds sourced by AWS partners. AWS Network Firewall works together with AWS Firewall Manager so you can build policies based on AWS Network Firewall rules and then centrally apply those policies across your VPCs and accounts.

AWS Network Firewall includes features that provide protections from common network threats. AWS Network Firewall's stateful firewall can incorporate context from traffic flows, like tracking connections and protocol identification, to enforce policies such as preventing your VPCs from accessing domains using an unauthorized protocol. AWS Network Firewall's intrusion prevention system (IPS) provides active traffic flow inspection so you can identify and block vulnerability exploits using signature-based detection. AWS Network Firewall also offers web filtering that can stop traffic to known bad URLs and monitor fully qualified domain names. For information, see [AWS Network Firewall].

Figure 5 – Summary of AWS Network Firewall

Amazon VPC

The Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications. You can easily customize the network configuration of your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the internet. You can also place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. For more information, see Amazon Virtual Private Cloud.

Access Control Lists (ACLs)

An ACL is an optional layer of security for your VPC that acts as a stateless firewall for controlling traffic in and out of one or more subnets. You can set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. For more information, see Network ACLs in the Amazon VPC documentation.

Security Groups

A security group acts as a virtual stateful firewall for your Amazon EC2 instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign security groups to the instance. Security groups act at the instance elastic network interface level, not the subnet level. Therefore, each instance elastic network interface in a subnet in your VPC can be assigned to a different set of security groups. For more information, see Security groups for your VPC.

Detect

Recent industry reporting[31] indicates that the average time to detect a data breach for a US organization is 186 days. This means that a data breach that occurs 6 months prior to the election may not even be detected until after the election, when it's too late to respond and save the integrity of the election. The detect function is the ability to discover a cybersecurity event, such as anomalies and events, through security continuous monitoring. This is a critical CSF function where AWS has been building advanced capabilities for customers through a number of new services over the past

few years. You can improve your alignment with several CSF subcategories using these services, such as DE.AE-1 through -5 and DE.CM-1 through -5, -7, and -8.

The CSF Detect activities generally provide for building a baseline of known good configurations and behavior. Event data is collected and analyzed from multiple sources, and vulnerability scans are performed—all to detect anomalies and unauthorized changes.

Amazon GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time-consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, you have an intelligent and cost-effective option for continuous threat detection in the AWS Cloud.

The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs. With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain. By integrating with AWS Security Hub and Amazon EventBridge, your GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems.

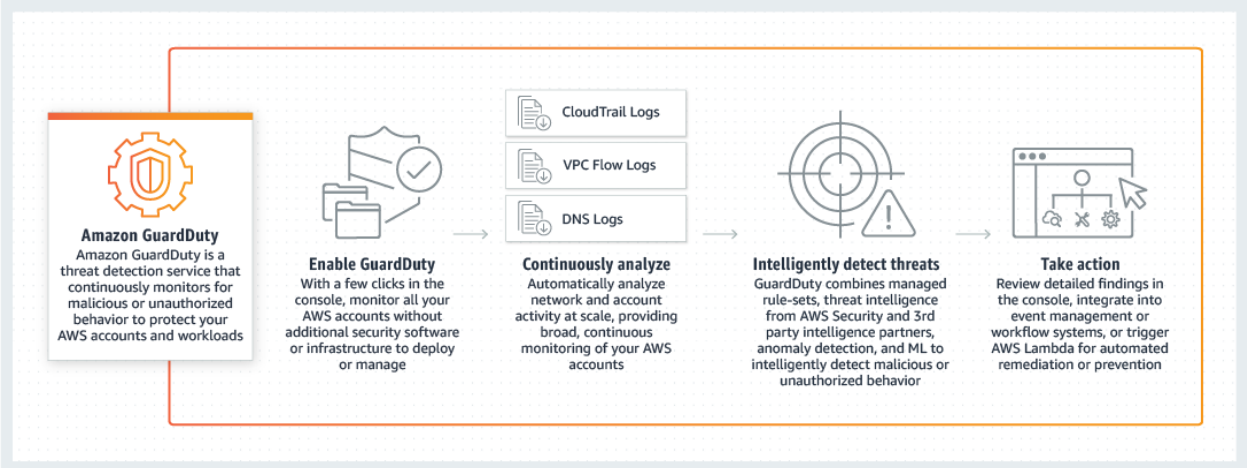

Figure 6 – Summary of Amazon GuardDuty

AWS CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. Also, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting. For more information, see AWS CloudTrail.

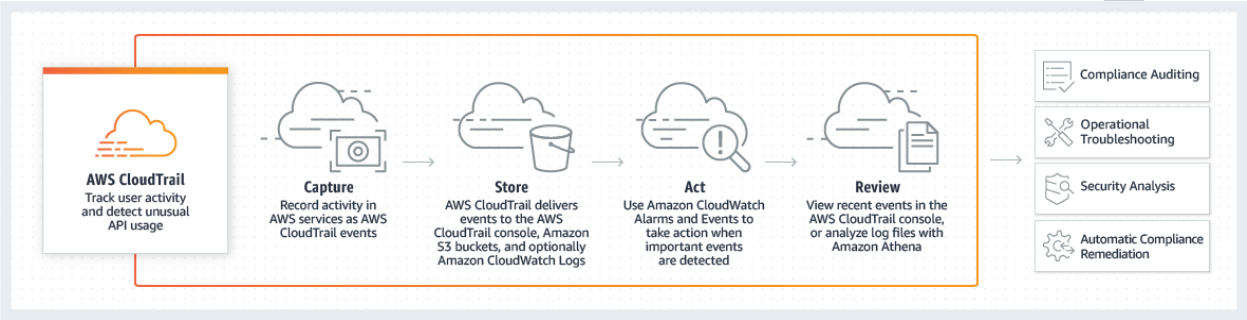

Figure 7 – Summary of AWS CloudTrail

Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, security teams, site reliability engineers (SREs), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications, and services that run on AWS and on-premises servers. You can use CloudWatch to detect anomalous behavior in your environments, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep your applications running smoothly. For more information, see Amazon CloudWatch.

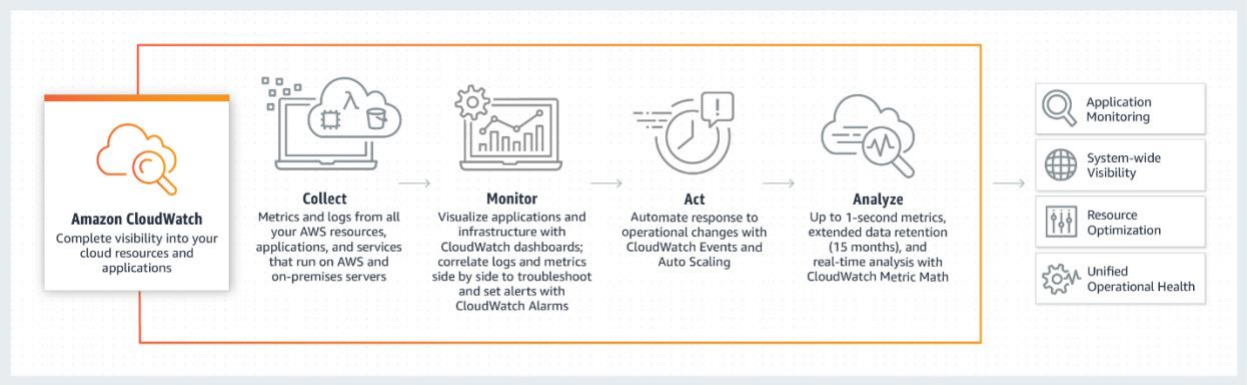

Figure 8 – Summary of Amazon CloudWatch

AWS Trusted Advisor

AWS Trusted Advisor is an online tool that provides you real time guidance to help you provision your resources following AWS best practices, to include security and fault tolerance. For more information, see [AWS Trusted Advisor.]

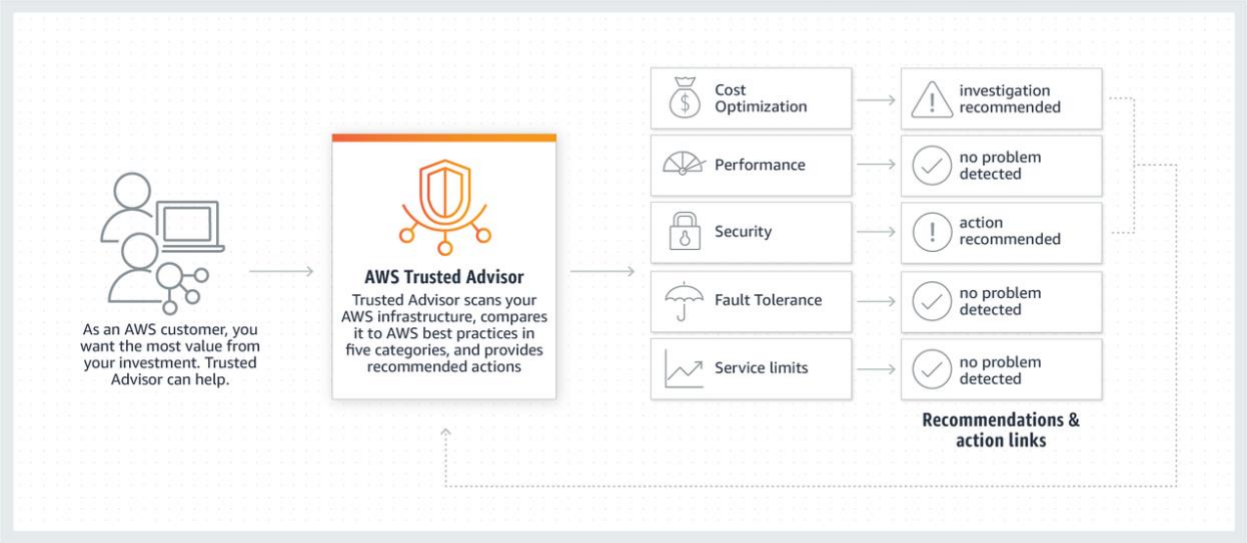

Figure 9 – Summary of AWS Trusted Advisor

AWS Config

This is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With AWS Config, you can review changes in configurations and relationships between AWS resources, dive into detailed

resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting. For more information, see AWS Config.

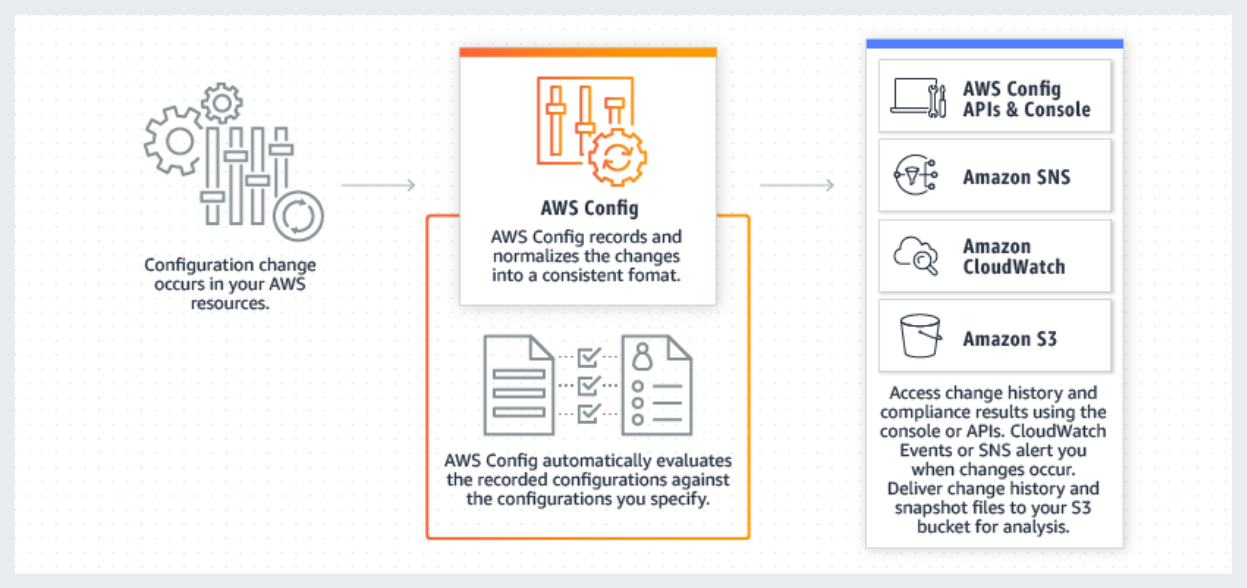

Figure 10 – Summary of AWS Config

AWS Security Hub

AWS Security Hub gives you a comprehensive view of your high-priority security alerts and security posture across your AWS accounts. There are a range of powerful security tools at your disposal, from firewalls and endpoint protection to vulnerability and compliance scanners. But this often leaves your team switching back-and-forth between these tools to deal with hundreds, and sometimes thousands, of security alerts every day.

With Security Hub, you have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, as well as from APN Partner solutions.

AWS Security Hub continuously monitors your environment using automated security checks based on the AWS best practices and industry standards that your organization follows. You can also take action on these security findings by investigating them in Amazon Detective or by using Amazon CloudWatch Event rules to send the findings to

ticketing, chat, Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), and incident management tools or to custom remediation playbooks. Get started with AWS Security Hub in just a few clicks in the Management Console and once enabled, Security Hub will begin aggregating and prioritizing findings and conducting security checks. For more information, see AWS Security Hub.

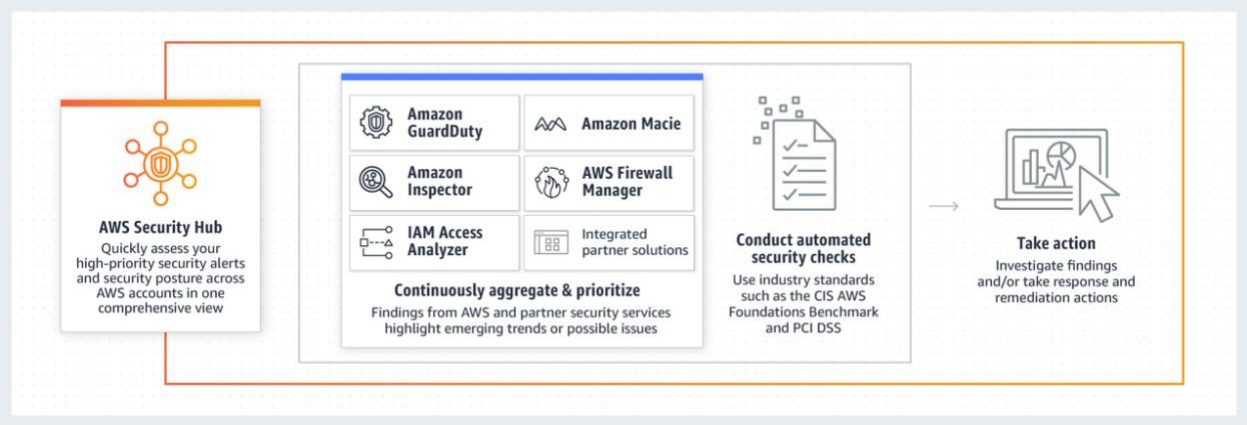

Figure 11 – Summary of AWS Security Hub

Amazon Detective

This service makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations.

AWS security services like Amazon GuardDuty, Amazon Macie, and AWS Security Hub, as well as partner security products, can be used to identify potential security issues, or findings. These services are really helpful in alerting you when something is wrong and pointing out where to go to fix it.

But sometimes there might be a security finding where you need to dig a lot deeper and analyze more information to isolate the root cause and take action. Determining the root cause of security findings can be a complex process that often involves collecting and combining logs from many separate data sources, using extract, transform, and load (ETL) tools or custom scripting to organize the data, and then security analysts having to analyze the data and conduct lengthy investigations.

Amazon Detective simplifies this process by enabling your security teams to easily investigate and quickly get to the root cause of a finding. Amazon Detective can analyze trillions of events from multiple data sources such as Virtual Private Cloud (VPC) Flow Logs, AWS CloudTrail, and Amazon GuardDuty, and automatically creates a unified, interactive view of your resources, users, and the interactions between them over time. With this unified view, you can visualize all the details and context in one place to identify the underlying reasons for the findings, drill down into relevant historical activities, and quickly determine the root cause. For more information, see Amazon Detective.

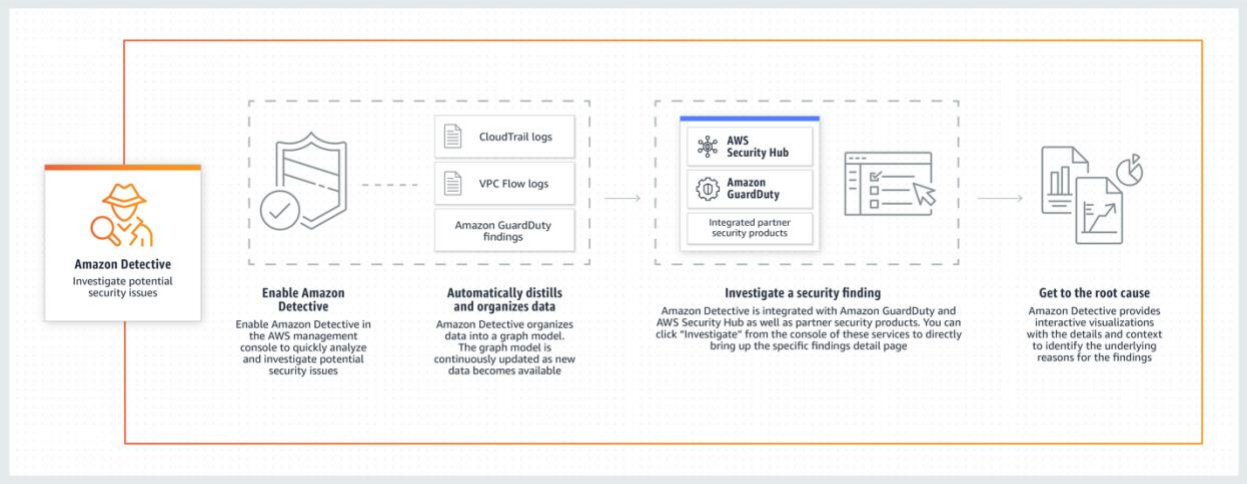

Figure 12 – Summary of Amazon Detective

Respond

Outages and attacks happen fast, and the time between detecting a suspicious activity or event and responding to it is critical. Even with a well-trained staff that is able to monitor and respond to every detected event, they cannot respond at the speed of cyber. Humans need work-breaks, and even when following the same procedures, have different levels of knowledge, experience, and judgment resulting in inconsistent results. We are not the best tool for rote procedures where there is an expectation of consistency and reliability for every action. This is where computers are ideal, and automation is key to speed and consistency.

The same industry report[21] mentioned in the Detect section above found that the average time for US organizations to contain a breach is 51 days. Our government elections customers and elections technology partners have expressed that this is unacceptable. In the Respond function, there are a few CSF subcategories where AWS

can elevate an elections technology solution, such as RS.RP-1 (response plan is executed during or after an incident) that would include RS-MI-1/2 (incidents are contained and incidents are mitigated). Some of these AWS services include the following.

Amazon EventBridge

Amazon EventBridge is a serverless event bus that makes it easy to connect applications together using data from your own applications, integrated software as a service (SaaS) applications, and AWS services. EventBridge delivers a stream of real-time data from event sources, such as Zendesk, Datadog, or Pagerduty, and routes that data to targets like AWS Lambda. You can set up routing rules to determine where to send your data to build application architectures that react in real time to all of your data sources. For more information, see Amazon EventBridge.

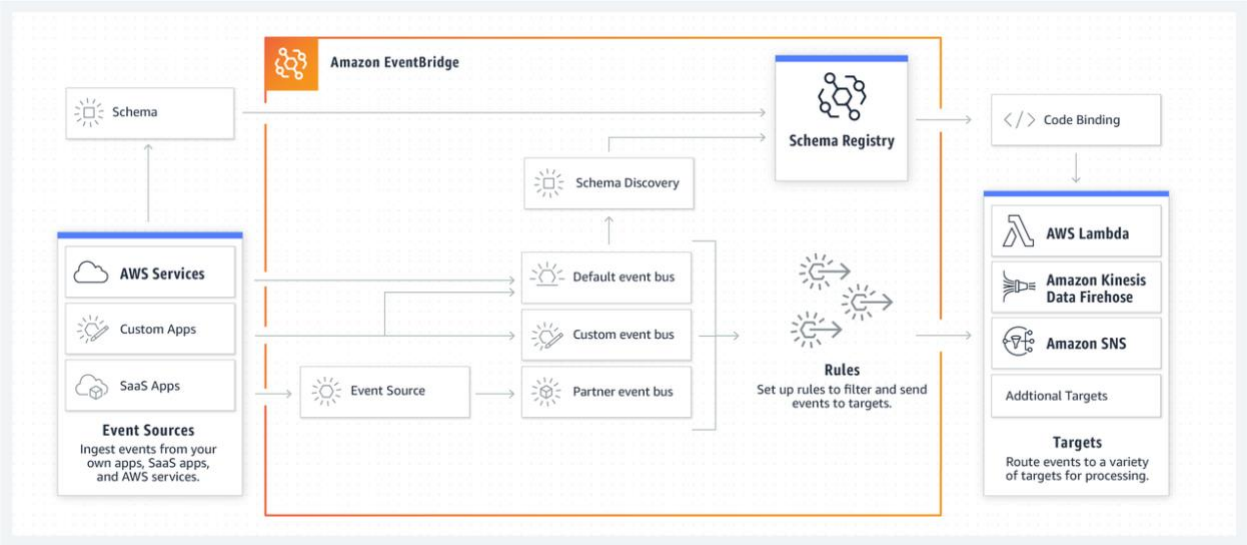

Figure 13 – Summary of Amazon EventBridge

AWS Lambda

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. With Lambda, you can run code for virtually any type of application or backend service—all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability. **The critical capability here for security response is that you can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.**

If or when a detection service like Amazon GuardDuty detects a threat and logs it as an Amazon CloudWatch Event, you can have a Lambda script triggered to take some action. For example, if GuardDuty logs an event where one of your EC2 instances is communicating with a known malicious botnet command and control (C2) server, then Lambda can trigger and block that suspicious activity at the AWS Web Application Firewall (AWS WAF) service, in the EC2 Security Group, in other third-party partner solutions, log the changes, and notify staff via email and SMS text messages all within seconds to minutes and without any human intervention. For more information, see AWS Lambda.

Figure 14 – Summary of AWS Lambda

AWS Config

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With AWS Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting. For more information, see AWS Config.

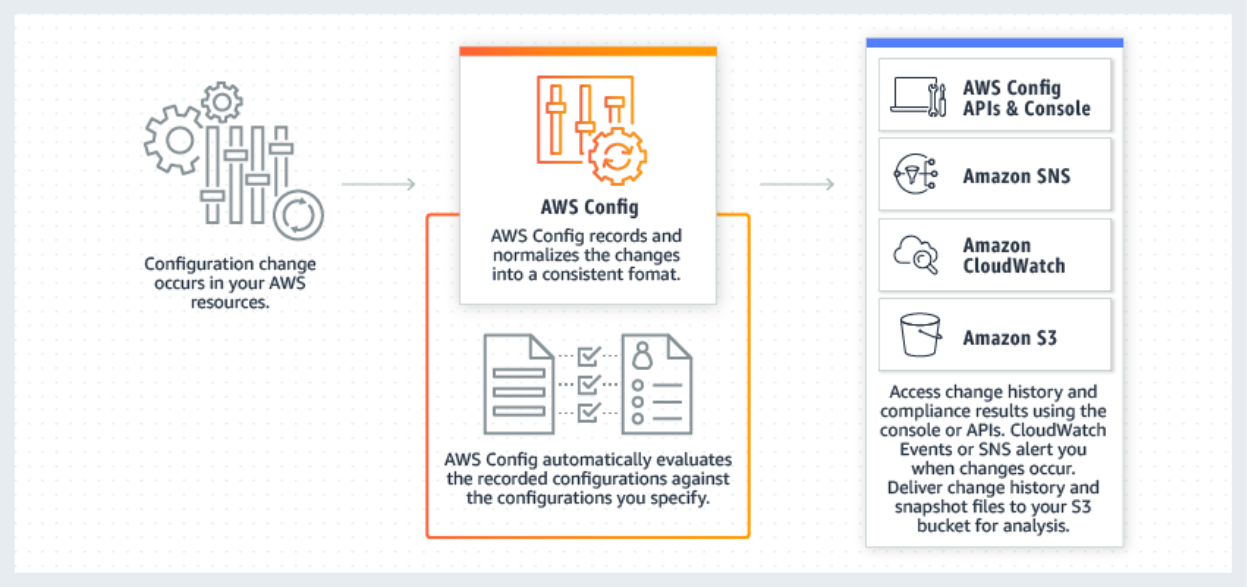

Figure 15 – Summary of AWS Config

AWS Auto Scaling

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to set up application scaling for multiple resources across multiple services in minutes.

The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas. AWS Auto Scaling makes scaling simple with recommendations that allow you to optimize performance, costs, or balance between them.

An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements to quickly identify when a server has failed and automatically replace it. When combined with one of the Elastic Load Balancing (ELB) services, the affected server's communications are shifted to other healthy servers until the replacement EC2 instance is brought online and checks in as healthy. For more information, see AWS Auto Scaling and Elastic Load Balancing.

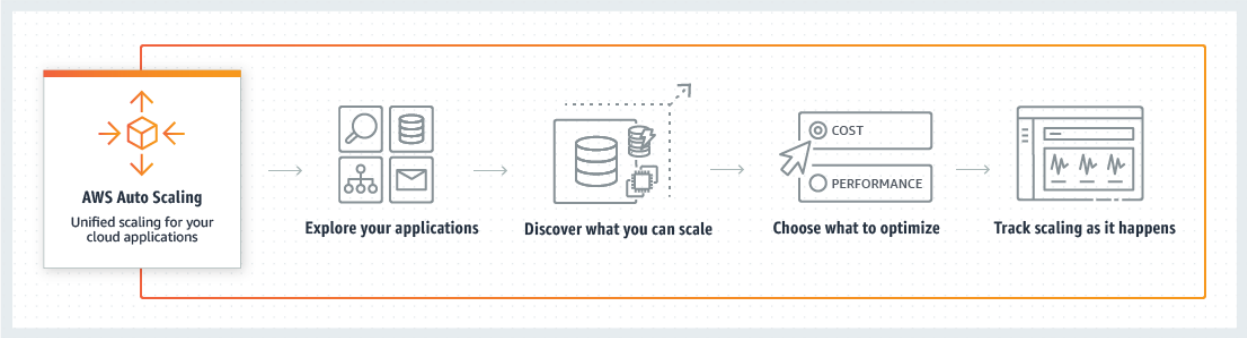

Figure 16 – Summary of AWS Auto Scaling

Recover

There is only a small window of time leading up to an election day, and the day itself, where the entire purpose of election systems exists. Every delay in recovering from an event and restoring the system functionality equals voters not registered, ballots not delivered, or votes not cast and can risk the entire democratic process.

There is only one CSF subcategory in the Recover Function where technology and automation can take the lead to reduce downtime and minimize the impact, and that is RC.RP-1 (Recovery plan is executed during or after a cybersecurity incident). The other subcategories are more manual and require people to lead the effort.

AWS brings the ability to build resilient architectures that are self-healing and that shift risk mitigation to the front of an event. The foundation for this is the AWS global infrastructure with 24 geographic Regions and 77 Availability Zones. For more information, see Regions and Availability Zones.

Region

For AWS, a Region is a physical location around the world where we cluster data centers. We group data centers within a Region into logical fault isolation zones called an Availability Zone. Each AWS Region consists of multiple, isolated, and physically separate Availability Zones within a geographic area.

Unlike other cloud providers, who often define a Region as a single data center, the multiple Availability Zone design of every AWS Region offers you many advantages. Each Availability Zone has independent power, cooling, and physical security and is connected by redundant, ultra-low-latency networks. AWS customers who are focused on high availability can design their applications to run in multiple Availability Zones to

achieve even greater fault-tolerance and resiliency. AWS infrastructure Regions meet the highest levels of security, compliance, and data protection.

Availability Zone

An Availability Zone is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. Availability Zones give customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible from a single data center.

All Availability Zones in an AWS Region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated metro fiber providing high-throughput, low-latency networking between Availability Zones. All traffic between Availability Zones is encrypted. The network performance is sufficient (<2ms latency) to accomplish synchronous replication between Availability Zones.

Availability Zones make it easy to partition applications for high availability. If an application is partitioned across Availability Zones, companies are better isolated and protected from issues such as power outages, lightning strikes, tornadoes, earthquakes, and more. Availability Zones are physically separated by a meaningful distance, many kilometers, from any other Availability Zone although all are within 100 km (60 miles) of each other.

So, what does this mean for elections technology solution providers or election officials? Traditionally, applications were built as a single server or server stack (a standard three-tier web application would include a database server, application server, and a web server) all housed in a single data center. If the data center had an outage due to any number of environmental events (for example, loss of power due to tornado) or if one of the servers failed, the application would be offline and customers would go unserved until everything could be restored. Recovery could take hours or days or even weeks to either rebuild a physical server and restore data from backups in an alternate data center, or to repair any facility damage to the current data center and restore utilities (for example, power, HVAC, or internet connectivity). This is simply unacceptable to the Election's mission.

If you move to AWS and refactor applications to decouple application processes and data, you can build an elections technology solution that would span multiple physical data centers within a specified geographic Region. This solution would replicate data synchronously, and be able to automatically respond to events so that there is no business impact. This would allow elections technology providers and elections officials

to ***shift from a reactive disaster recovery risk model to a proactive resiliency risk model***. This doesn't mean that risk can be reduced to zero. But much of the residual risk could be mitigated on the front end (before an event) rather than on the backend (after an event). Even so, we still recommend that a disaster recovery (DR) plan and capabilities be in place, which AWS can provide.

Security summary

AWS has the cloud infrastructure, services, and offerings to help you meet and possibly exceed the requirements and expectations for both elections technology providers and elections officials. The high degree of granular visibility and control of protective measures, advanced intelligent threat detection, automated responses, and resilient infrastructure provide an array of advanced capabilities and maturity that can help reduce risk and improve the probability of a successful election process.

Whether you use the NIST Cybersecurity Framework, the Privacy Framework, an international standard such as ISO, or have created your own unique organizational framework, we recommend using a programmatic model to organize and manage your cybersecurity program for both on-premises and in the cloud. This framework should allow you to adequately assess new and emerging technologies without bias. For more information about using the NIST CSF with AWS, see NIST Cybersecurity Framework (CSF) Aligning to the NIST CSF in the AWS Cloud.

We have also published our own AWS best practices guide as the AWS Well-Architected Framework, which consists of 5 pillars:

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimization

The Well-Architected Framework should be viewed as your guide to implementing a secure and resilient workload in AWS. We recommend that elections officials and elections technology partners request a free Well-Architected Review from your AWS account manager to assess where you are and provide recommendations for improvement.

The AWS Security Incident Response Guide contains best practices for you to conduct incident response within your AWS environment. We recommend that your security operations teams read this guide.

And if you're looking for on-hand support during a security event, AWS Professional Services also offers a statement of work (SOW) for Incident Response support with no upfront costs. You can design this SOW based on your unique needs and expertise with AWS services, tailoring the virtual and on-site response times. When activated, AWS resources will be dedicated to assist you in working through the incident response process from detection and analysis to containment, eradication, and recovery.

Conclusion

Elections administrators, campaigns, and civic engagement organizations face unique challenges while promoting fair and open elections for an increasingly dynamic electorate. During each election cycle, elections organizations need to address load demands on sensitive workloads with non-voting elections technology, such as online voter registration, electronic ballot delivery, election night reporting, and electronic poll books. Aligning election security and scalability in the AWS Cloud to the NIST Cybersecurity Framework and applying the CIS Foundations Benchmarks to non-voting technology hosted in the AWS Cloud are important best practices for elections organizations. In addition, elections organizations can modernize and optimize voter education, accessibility and elections management with artificial intelligence and machine learning (AI/ML) solutions, including omni-channel Alexa skills, question and answer chatbot, text messaging, and cloud call centers, with the support of AWS and its partners. Forward thinking elections officials, IT managers, Chief Information Security Officers (CISO), Chief Technology Officers (CTO), and other leaders in elections organizations can make a vital impact in strengthening election security, management, and voter services by leveraging AWS Cloud-based technologies.

Several technology providers and government officials operated elections workloads in AWS during the U.S. Presidential and state elections in November 2020, which was proven to be the most secure elections in U.S. history.[31] This success was due in large part to the diligence of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), state and local elections officials, and elections technology providers. AWS is proud of the work we did to support these customers in meeting their security objectives, and are ready to support elections for our global customers.

Document history

Date	Description
June 16, 2021	First publication

Contributors

The following individuals and organizations authored or contributed to this document (in alphabetical order):

- Stephen Alexander
- Mark Becker
- Spencer DeBrosse
- Michael Kaiser
- Jud Neer
- Tonya Rice
- Michael South

Notes

[1] https://www.eac.gov/payments-and-grants/election-security-funds

[2] https://editions.lib.umn.edu/electionacademy/2017/10/31/happy-belated-15th-birthday-hava/

[3] https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf; see also: https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html; https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections; https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016; https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

[4] https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections

[5] https://foreignpolicy.com/2020/03/20/russia-china-iran-coronavirus-disinformation/

[6] https://www.eac.gov/payments-and-grants/2020-cares-act-grants

[7] https://blog.aboutamazon.com/devices/alexa-tells-us-about-the-election

[8] https://blueprints.amazon.com/

[9] https://developer.amazon.com/en-US/alexa/alexa-skills-kit

[10] https://aws.amazon.com/lex/

[11] https://aws.amazon.com/blogs/machine-learning/creating-a-question-and-answer-bot-with-amazon-lex-and-amazon-alexa/

[12] https://docs.aws.amazon.com/lex/latest/dg/fb-bot-association.html#fb-bot-assoc-create-fb-app

[13] https://aws.amazon.com/connect/

[14] https://aws.amazon.com/solutions/case-studies/la-county/

[15] https://aws.amazon.com/blogs/contact-center/automating-outbound-calling-to-customers-using-amazon-connect/

[16] https://docs.aws.amazon.com/polly/latest/dg/voicelist.html

[17] https://aws.amazon.com/lex/

[18] https://aws.amazon.com/pinpoint/features/

[19] https://aws.amazon.com/comprehend/

[20] https://aws.amazon.com/solutions/implementations/ai-driven-social-media-dashboard/

[21] https://aws.amazon.com/lake-formation/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

[22] https://aws.amazon.com/quicksight/

[23] https://aws.amazon.com/products/customer-engagement/

[24] https://www.justice.gov/crt/language-minority-citizens

[25] https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections

[26] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[27] https://www.nist.gov/cyberframework

[28] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf#page=11.

[29] Privacy conscious cloud migrations: mapping the AWS Cloud Adoption Framework to the NIST Privacy Framework

[30] AWS Services and Customer Responsibility Matrix for Alignment to the CSF

[31] https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542

[31] https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election