CJ Moses' Security Predictions for 2023 and Beyond

November 2022

CJ Moses
Chief Information Security Officer, AWS

Contents

Cloud services can be used almost anywhere on the planet and now we're headed to space - AWS currently serves customers from 27 Regions globally and, with Project Kuiper, we're sending a satellite constellation into orbit that will provide fast, affordable broadband to unserved and underserved communities worldwide. The broad use of the cloud means data is being stored in the cloud at an exponential rate. In 2020, people created 1.7 MB of data every second and some projections say that 463 exabytes of data **will be created in 2025**. Simultaneously, the burgeoning reliance on the cloud and data has placed a heavier demand on organizations to hire and invest in skilled people to help these organizations accelerate their cloud journey. As businesses push to innovate quickly, it is clear that securing this data will be critical to their continued growth and the evolution of the cloud.

With all these moving parts between technology and humans, we've entered a fascinating phase in which it will take the right mix of both to help define the future of cloud security. As we look to the future, we know that automation will be key to remove undifferentiated heavy lifting for our customers, so they can continue making the right decisions about how to stay secure in the cloud and respond faster to a possible security event.

At AWS, security is our top priority. We work each day to earn the trust of every one of our customers. A big part of my job is spending time on how to prepare for possible future security needs. This ebook is meant to provide you insight into our perspectives and provide predictions on where security is headed in 2023 and beyond.

PREDICTION 1

Security Will Be Integral to Everything Organizations Do

Increasing threats and risks will continue driving a shift to the cloud, where security will be built into everything organizations do. Organizations will shift to continuous security and compliance, creating an environment where it's easier to make the right security decisions early in their digital transformation, enabled by the proliferation of automated security services and tooling.

Every day, our customers share with us how they have taken the opportunity to make the move from self-managed, on-premises security techniques to a shared responsibility service model that will support and scale with their business transformation architecture. This is because they know security must be automated as much as possible to keep up with business scale and make it easier for organizations to secure themselves. The cloud provides exciting innovation to help secure data in ways that weren't possible on-premises, allowing organizations to maintain focus on business growth while simultaneously enhancing security. As a result, organizations are adopting a security culture, where embedding security into the way they operate helps to propel them safely forward.

This focus on security starts with core aspects of maintaining an effective security program, including managing identities and permissions, protecting networks and infrastructure, identifying and responding to threats, data protection, and demonstrating compliance. The cloud allows automation of mundane tasks associated with each of these areas, such as logging, monitoring, auditing, patching, and integration with an existing toolset, to name a few. Tools such as **AWS Identity and Access Management (IAM)**, **AWS CloudTrail**, **AWS Key Management Service (AWS KMS)**, **AWS WAF**, **Amazon GuardDuty**, and **AWS Security Hub** are some of the

essential tools that provide insights into where data is stored, who is accessing it and when, its encryption status, where it's moving, whether it's being acted upon suspiciously, and if it's susceptible to common exploits. In the coming years, accompanying the inevitable continued cloud adoption, we believe we are going to see exponential demand in furthering automation capabilities in these areas.

Organizations will move to continuous security and compliance. We've seen from our customers, partners, and builders internally who work on delivering and maintaining our security services, that rapid innovation in cloud security services is making it easier to integrate security into everything with continuous security improvement. This is largely due to the ease of use we're seeing with cloud security services and tooling, allowing customers to improve their speed of development and their security bar, which results in shipping securely. As just one example, using **Amazon Inspector** and **AWS Systems Manager** helps customers automate patching for infrastructure and applications, reducing the burden of manually patching, easing the process of patching multiple operating systems, and boosting customer productivity.

PREDICTION 2

Diversity Will Help Address the Continued Security Talent Gap

As the scale of the cloud grows, the need for security professionals will grow along with it. Diversity is a big part of the solution to this problem and we believe that organizations that prioritize hiring people with diverse educational and career backgrounds, people who are neurodiverse, people from different cultures, and so on, will outperform in security compared to those that don't.

As of 2021, there were 4.19 million cybersecurity professionals worldwide. However, there was still a need for 2.72 million more. Closing the security workforce gap is a crucial step to improving security everywhere. While security professionals keep joining the workforce, the need for security professionals outpaces the supply. Some ways organizations can help close the security workforce gap are to invest in diversity, equity, and inclusion (DE&I) initiatives, similar to **Amazon's affinity groups**, reevaluate hiring standards and practices, and invest in candidates with diverse backgrounds. Around half of security professionals got their start outside of IT and we think this should be encouraged. We believe organizations will be more secure and successful if they hire for attitude and aptitude, and train for technical skills. The prohibitive costs of a college education and many security certifications is one reason why minorities and people with diverse backgrounds may struggle to break into the industry. Organizations should look beyond specific technical degrees and certifications and instead try to hire people who have the aptitude or skills in other forms.

Diverse security professionals mean diverse perspectives on security, which means stronger defenses. For example, organizations such as GCHQ, the U.K.'s signals intelligence agency, **are leading the way** by actively hiring neurodiverse individuals for their unique ability to spot patterns in data. For us, diversity in security is about more than just equality; it is about optimizing defensive capabilities by having access to the widest possible range of problem-solving abilities.

Diverse hiring is a key part of our culture at AWS, and that can mean hiring people who do not have a background in security. There are many skills that make a person successful in the security space and we believe it's important to hire this talent and provide them with security training. It's also important to focus on the development and retention of existing staff. We have long believed that education is the key to helping people and organizations improve their security posture, so we offer **Amazon Security Awareness training** to everyone for free. Automation in cloud security operations may play a role in closing the talent gap, but this problem cannot be solved by technology alone - it must primarily be a human-focused effort. We need to encourage the development of future staff through mentorship programs and by connecting with the future generations of the workforce to promote STEM education.

PREDICTION 3

Automation Driven by AI/ML Will Enable Stronger Security

Machine learning and artificial intelligence will add a critical layer of automation to cloud security. AI/ML will help augment developers' workstreams, helping them create more reliable code and drive continuous security improvement.

Historically, security has been a binary, rules-based system in which things are either okay or not okay. And we've built complex systems that define "okay" based on a number of criteria. Cloud changed this model, and we can now dynamically build strong defenses and effective hedging strategies against known threats. As part of the next phase of cloud security evolution, it will become more common to apply human-level intelligence to threat detection and remediation. Over the next several years, we anticipate machine learning will play a major role in augmenting security engineers' capabilities, helping them to create more secure architectures and applications in the cloud.

The predictive capabilities of AI/ML can help customers develop a more proactive security stance in the face of our evolving threat landscape. This has become increasingly important over the past few years with the rise of work from home and hybrid working models, where there has been a dramatic shift in people working across a variety of networks, expanding the threat surface exponentially. Threat actors are taking advantage of this phenomenon introduced by remote work, using previously unseen malware to initiate common security incidents, such as ransomware, phishing, and social engineering.

In this hybrid, increasingly complex environment, AWS services like Amazon GuardDuty, **Amazon Detective**, **Amazon CodeGuru**, and **Amazon Macie** will continue to lay the groundwork for integration of security and machine learning, helping customers with intelligent recommendations, at scale. These, and other rapidly evolving machine learning cloud capabilities, are beneficial due to their ability to assess large amounts of data, pinpoint anomalies, and provide intelligent recommendations about security vulnerabilities, code quality, and potential threats. For example, Amazon GuardDuty launched **DNS reputation modeling**, taking the DNS requests from across AWS and feeding them into a model that allows AWS to categorize

previously unseen domains as likely to be malicious or benign based on their behavioral characteristics. In practice, AWS is seeing that these models often deliver high-fidelity threat detections, identifying malicious domains 7–14 days before they are identified and are available on commercial threat feeds.

Another use case where we'll continue to see AI/ML influence security is compliance. AI technologies, like automated reasoning, built into our services enable customers to better understand their compliance posture with regards to complex systems, automating the detection of anomalies posing compliance risk amidst global data sets. Traditionally, many security and compliance tasks were hampered by the need for human interaction to assess compliance status and permissions changes, and managing these areas was a reactive process. Cloud services such as **AWS Audit Manager** and **AWS Identity and Access Management Access Analyzer** help automate away human intervention, so customers can know more about their compliance posture and permissions levels before deploying changes to their IT infrastructure. Audit Manager can automate evidence collection for desired compliance frameworks (such as Payment Card Industry Data Security Standard, Center for Internet Security, and National Institute of Standards and Technology (NIST)) rather than having customers rely on point-in-time, manual assessments. This evidence collection is also continuous, allowing customers to pull a report on their compliance adherence to their desired framework anytime. IAM Access Analyzer allows customers to monitor their policies for overly broad access to their resources and data. Once the policy is written (which IAM Access Analyzer also helps with), IAM Access Analyzer monitors authorization without human intervention. In the coming years in security, this concept of continuous improvement will force multiply, with the entire ecosystem of cloud providers, partners, and cloud users further evolving automation capabilities that drive systematic advancements in cloud security around the world.

AI/ML-driven security innovation such as that described here is helping customers solve real-word daily challenges for security practitioners, such as reducing workload for SOC analysts and allowing security architects to spend more time on threat modelling instead of having to validate that an application closed firewalls and patched servers. We are just scratching the surface of AI/ML in cloud security. With the exponential growth of the cloud, security needs will grow equally quickly, fueling the need for automation and intelligence-driven security.

PREDICTION 4

People Will Drive Greater Data Protection Investment

Data protection continues to be top of mind for AWS customers and people around the globe, especially as the amount of data created continues to grow exponentially. With that level of growth, we expect to see more data protection legislation, greater investment in data protection and associated programs, and a shift toward automation.

The European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other localized laws are just the beginning of data protection regulations. **A 2019 Cisco survey** found that nearly half (47%) of respondents trust companies more if they comply with GDPR. As the data protection space matures, and the public desire for data protection laws continues to grow, we'll see more governments respond by implementing legislation and we will see more organizations meet those requirements. Gartner predicts that by the end of 2024, 75% of the world will have its personal data covered under regulations.

Over the next several years, we'll also see organizations increase their investment in data protection. Gartner predicts that large organizations' average annual budget for privacy **will exceed $2.5 million USD by 2024**. Some of this investment will go toward data protection programs that include ways to assess risks to data, perform ongoing administration and resource management tasks, and develop tools that reduce risks to data while remaining highly functional.

At AWS, earning our customers' trust is the foundation of our business. We will continue to monitor the evolving privacy regulatory and legislative landscape to identify changes and determine what tools our customers might need to help meet their compliance needs – this is our ongoing commitment. We make sure that customers can control their own data by using AWS services and tools such as AWS IAM, CloudTrail, Macie, and others to determine where data is stored, how it is secured, and who has access to it. We also implement privacy safeguards with services and features that let customers implement their own privacy controls, including advanced access, encryption, and logging features. Customers can choose to store their data in any one or more of our **AWS Regions** around the world. By using AWS services, our customers can be confident that their data stays in the selected AWS Region.

To learn more about data protection at AWS visit **Privacy Features of AWS Services**, **Data Protection at AWS**, and our **Data Privacy Center**.

PREDICTION 5

More Advanced Forms of Multi-Factor Authentication Will Become Pervasive

By moving toward more biometric and multimodal forms of authentication, the future of MFA will combine impregnable security with usability, ensuring that users have a frictionless experience while improving their security posture.

MFA is one of the simplest and most important protections customers can use, making it harder for malicious actors to gain access to the account if their passwords are leaked online or their employees are targeted by social engineering. Customers use MFA to strengthen the security of their accounts and their applications by requiring an additional factor (something they have, something they know, or something they are, like a biometric) in addition to passwords, which are usually weak and vulnerable to theft from data breaches.

MFA is continuing to become more widespread for both business and personal use, and we believe the next frontier lies in more pervasive use of multimodal biometric forms of authentication because of their convenience and improved security. Multifactor, meaning using two or more factors for the purpose of authentication, can include roaming (such as Yubikeys and Virtual Authenticators) and platform (on devices like Windows Hello and Apple FaceID). Multimodal refers to the use of multiple biometrics to gain access to systems. Biometric authentication is the field of study that relies on the unique biological characteristics of individuals to verify they are who they say they are, and typically includes a physical or behavioral characteristic. Increased reliance on biometrics will make MFA a more frictionless, natural experience for customers. In a multimodal biometric system, we will see a combination of a physical biometric factor (fingerprint, voice, iris, or facial recognition) combined with a behavioral factor (keystrokes, hand movements, grasp, and more).

MFA use will benefit from the increased priority governments and prominent security organizations have placed on security over the past few years. MFA is being pushed as a baseline online protection by entities, such as the FIDO Alliance, NIST, and the U.S. government, which recently issued a **statement** urging all companies to adopt MFA. The government, specifically the Cybersecurity & Infrastructure Security Agency

(CISA), has taken further measures to drive MFA awareness and adoption by launching the #MoreThanAPassword **campaign**.

We encourage our customers to continue to monitor anticipated advancements in MFA over the next several years to see how they may improve an existing capability or build new MFA capabilities into their organization's routine. We will continue to keep customers posted on advancements in MFA on AWS at our **MFA overview page**.

PREDICTION 6

Quantum Computing Will Benefit Security

Quantum computing may not be top-of-mind for everyone yet, but it is gradually advancing, and quantum-safe security is advancing with it in the form of cryptography. AWS is already at work, preparing for a post-quantum world. In the long run, we expect quantum computing to help make things more secure, but for now, organizations should make sure they're using the latest encryption methods to protect their data.

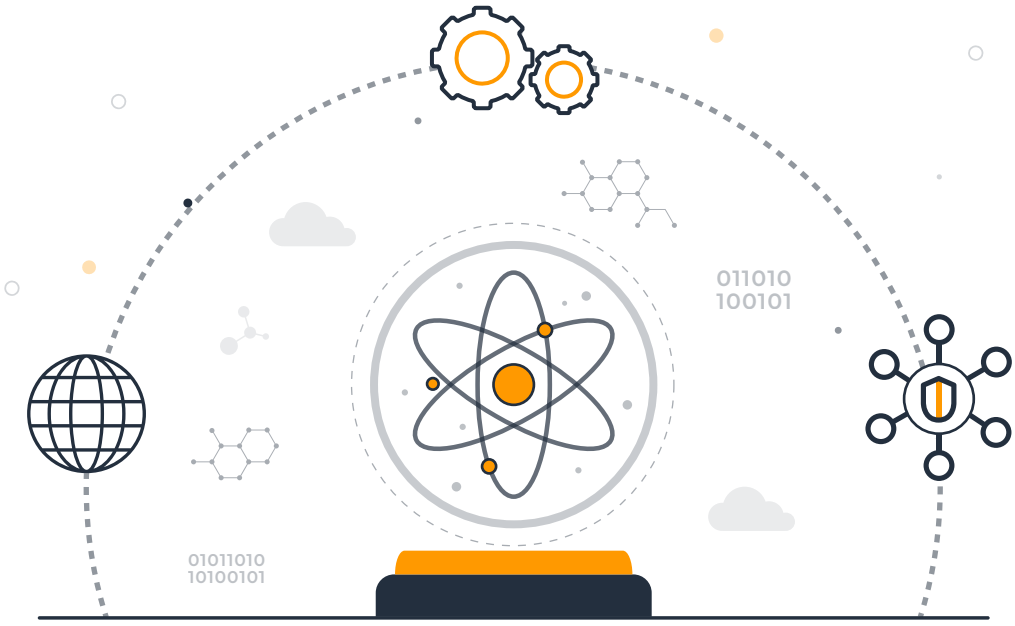
There's some evidence that quantum computing will become affordable and usable at some point in time — although it's unclear if that time is five or 50 years away. But when it comes, it is expected to weaken certain types of cryptography, including the kind we use for data-in-transit security protocols like HTTPS and TLS. The industry is currently working on what's called quantum-safe or post-quantum cryptography, in which different algorithms and different key sizes provide the same level of security that we have today, even against a quantum computer. As encryption algorithms and protocols evolve to address this potential future risk, we'll see a shift in the way our devices connect to each other. Our phones, our laptops, and our servers will adopt this new technology to ensure privacy in our communications.

In the long term, we expect that quantum computing will actually benefit cloud security. Once organizations work more closely with quantum computing and quantum algorithms, they'll begin to think about classical algorithms differently. Reconsidering classical algorithms in light of new quantum-inspired processes can inspire creative solutions to existing functions, developing new or evolving classical algorithms based on new ways of thinking about computing derived from quantum. For example, **a quantum researcher** was already able to find a way to have a classical computer potentially match the ability of a quantum computer to recommend products that users will like.

Cryptography standards will continue to evolve as the industry thinks about the risks of quantum computing. NIST is already working on this and aims to have new quantum-safe standards in place by 2024 that they are developing through a **post-quantum cryptography standardization effort** that spans several rounds of evaluation over multiple years. Large organizations, including AWS, are contributing to this effort. We submitted two options (BIKE and SIKE) and both made it past the first round of selection, which narrowed

82 original submissions down to 26 remaining proposals. NIST is likely to standardize more than one submission because the various approaches trade off different aspects of performance (such as faster computation but larger network messages).

AWS will work with others to implement future standards and continue to develop and implement post-quantum encryption. AWS KMS already supports some hybrid post-quantum key exchange algorithms for TLS 1.2. The Biden Administration included post-quantum encryption in a 2022 memorandum on improving the cybersecurity of U.S. agencies like the Department of Defense and we think we'll start to see more governments implementing post-quantum encryption.



As we've seen, further cloud expansion is inevitable as organizations become digital. We believe security will become the center of everything organizations do, creating a culture of security. In this culture, every employee becomes a security owner who can positively impact the security of the organization and the practice of security will be a collective, continuous pursuit fueled by technology innovation and diverse people. These factors will influence an overall perception shift about security for both organizations and individuals, where security will be viewed as a business and innovation driver, rather than seen as the department of "no" upholding a set of IT obligations. AWS and our customers continue to be at the forefront of a shifting cloud security landscape, providing the foundational innovation, use cases, and best practices to help position security as core to future innovation in both business and technology.