

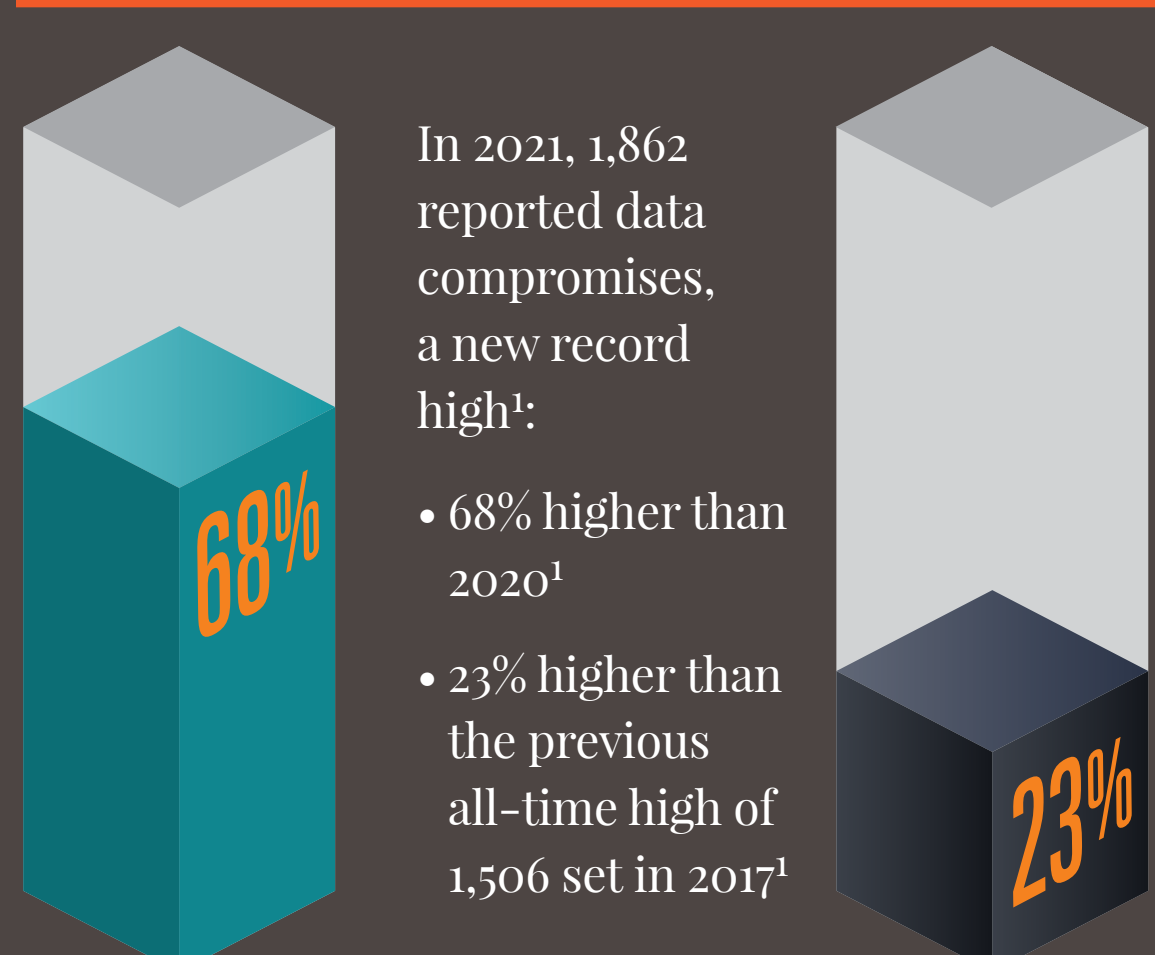
# A Salute to Public Sector Security: 3 Top Cloud Security Benefits

## WHY AWS?

Migrating to the cloud with AWS secures digital assets and protects systems from unauthorized access. Fed and SLED can benefit from AWS secure data centers and a network architected to protect information, identities, applications, and devices, including zero-trust components for network-level encryption and the Internet of Things (IoT). AWS helps defend against cyberattacks and provides many benefits, from fewer security incidents to exceptional compliance support and operational resiliency.

## WHY NOW?

With today's security threats on the rise, staying ahead of threat actors can be overwhelming. In 2021 and 2022, cybersecurity is at the top of the public sector agenda.



President Biden issued Executive Order 14028 in May 2021<sup>2</sup>:

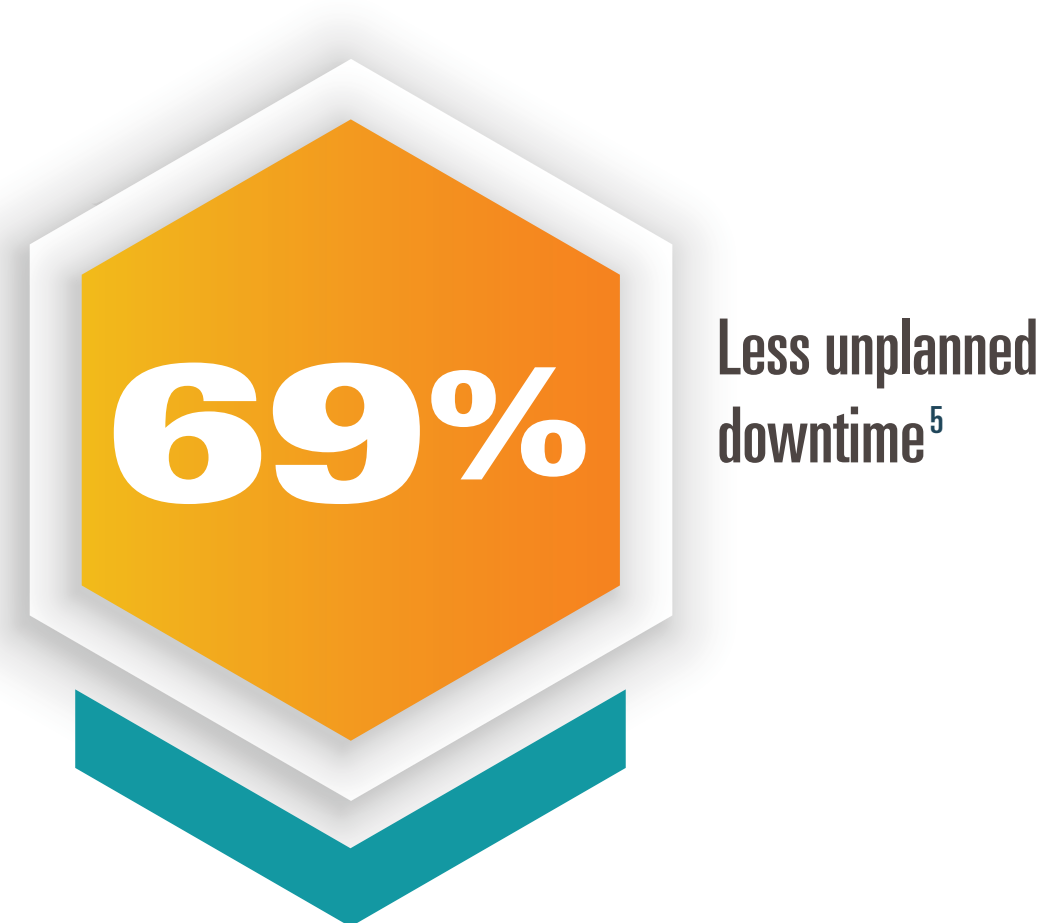
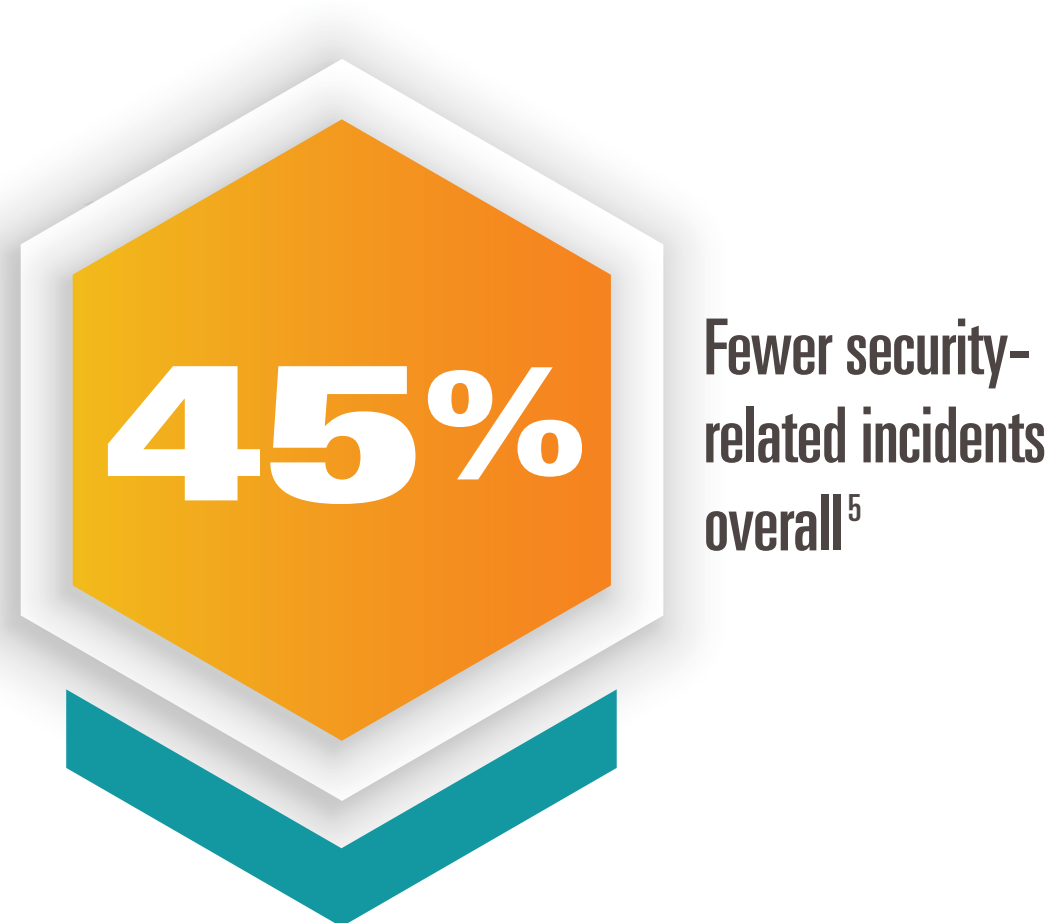
- Marked dramatic change in the federal government's cybersecurity philosophy
- Set prevention, detection, assessment, and remediation of cyber incidents as top national and economic security priorities
- Moved the government toward zero-trust cybersecurity principles

Existing security protocols require attention. For example, the Department of Commerce (DoC) Office of the Inspector General reported:

- 118 out of 256 (46%) of Special Access Programs (SAPs) security protocols were inadequately planned according to department requirements<sup>3</sup>
- 212 of the 256 systems (83%) Security System Plans (SSPs) were missing<sup>3</sup>

Office of Management and Budget Memorandum M-22-09, January 2022, and pursuant memos set goals for a federal zero-trust architecture strategy, requiring agencies to meet specific cybersecurity standards<sup>4</sup>

## BENEFIT #1: PREVENTING AND REDUCING THE IMPACT OF BREACHES



## BENEFIT #2: COMPLIANCE SUPPORT

AWS helps satisfy compliance requirements with more security standards and compliance certifications than any other offering, including:<sup>6</sup>

- SOC 2
- PCI-DSS
- HIPAA/HITECH
- FedRAMP
- GDPR
- FIPS 140-2
- NIST 800-171

Automatic data encryption across the AWS global network at the physical layer before it leaves secured facilities

**100+** AWS services with data encryption capabilities

Tools to help customers encrypt data in transit and at rest and ensure that only authorized users can access it, with control and visibility for compliance with regional and local data privacy and residency laws

## BENEFIT #3: INCREASED OPERATIONAL RESILIENCE

In case of cyberattacks or man-made or natural disasters, AWS enables delivery of mission-critical services when needed.

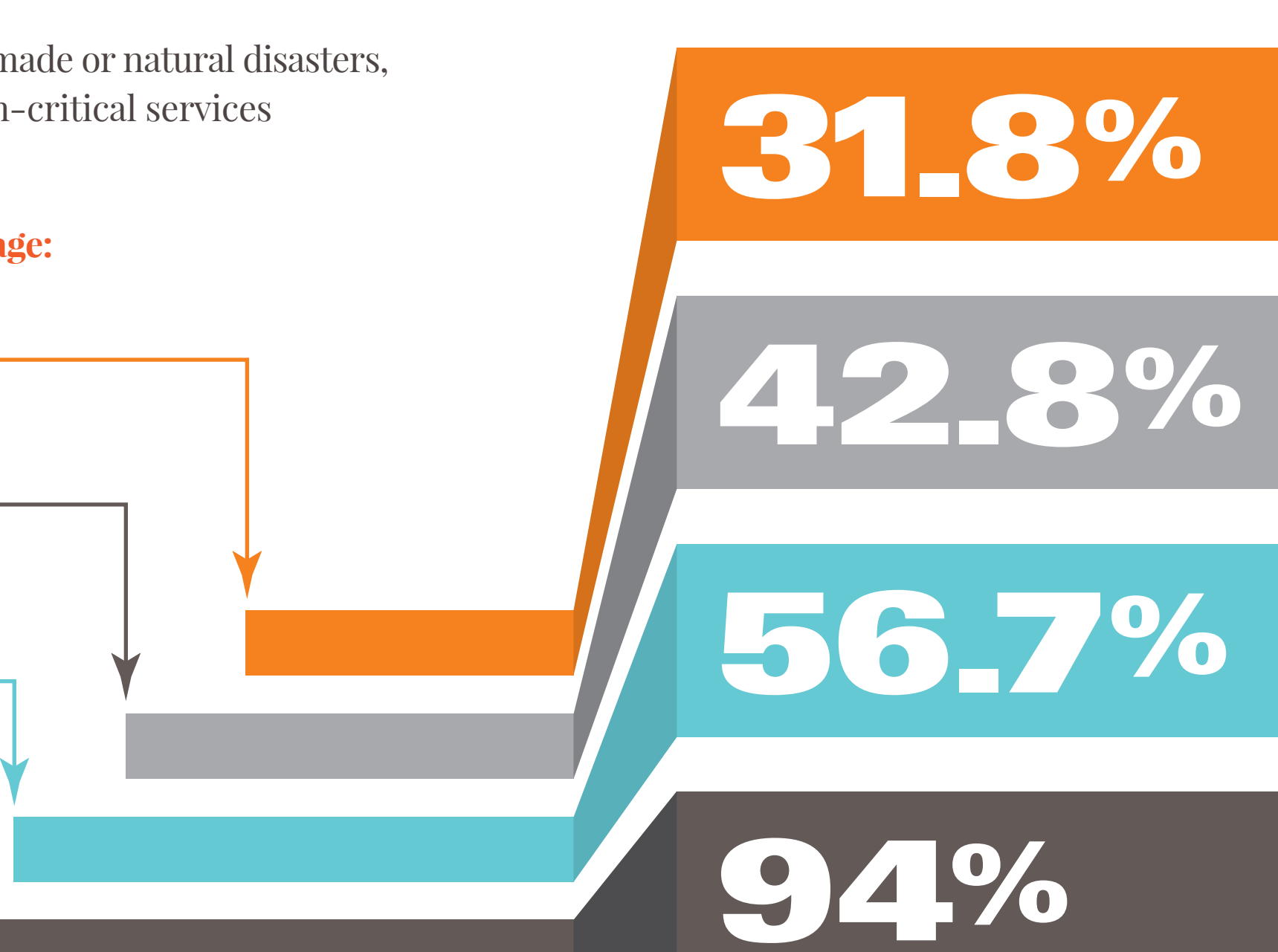
**AWS customers see, on average:**

Drop in P1/Po incidents<sup>7</sup>

Fewer critical incidents for apps with 1,000+ users<sup>7</sup>

Reduction in application downtime<sup>7</sup>

Less unplanned downtime<sup>7</sup>



1 <https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/>  
 2 <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>  
 3 <https://www.oig.doc.gov/OIGPublications/OIG-23-001.pdf>  
 4 <https://d1.awsstatic.com/psc-digital/2022/gc-mig/business-value-of-migration/Business-Value-of-Migration-Whitepaper-EN.pdf>  
 5 <https://pages.awscloud.com/rs/112-TZM-766/images/AWS-BV%20IDC%202018.pdf>  
 6 <https://aws.amazon.com/compliance/>  
 7 <https://pages.awscloud.com/rs/112-TZM-766/images/cloud-value-benchmarking-study-quantifies-cloud-adoption-benefits.pdf>

For more information on how AWS can help you improve cybersecurity practices that will benefit the government, public sector users, and the American public, contact us today.