Deloitte.

Ransomware resilience on Amazon Web Services: Balancing security and recovery strategies

Contents

Introduction: Holding data for ransom 1

A two-pronged approach to resilience: Security and recovery 2

Security: AWS Security services help guard the business against ransomware 3

Recovery: Helping the business bounce back from an event 6

Conclusion 7

Introduction: Holding data for ransom

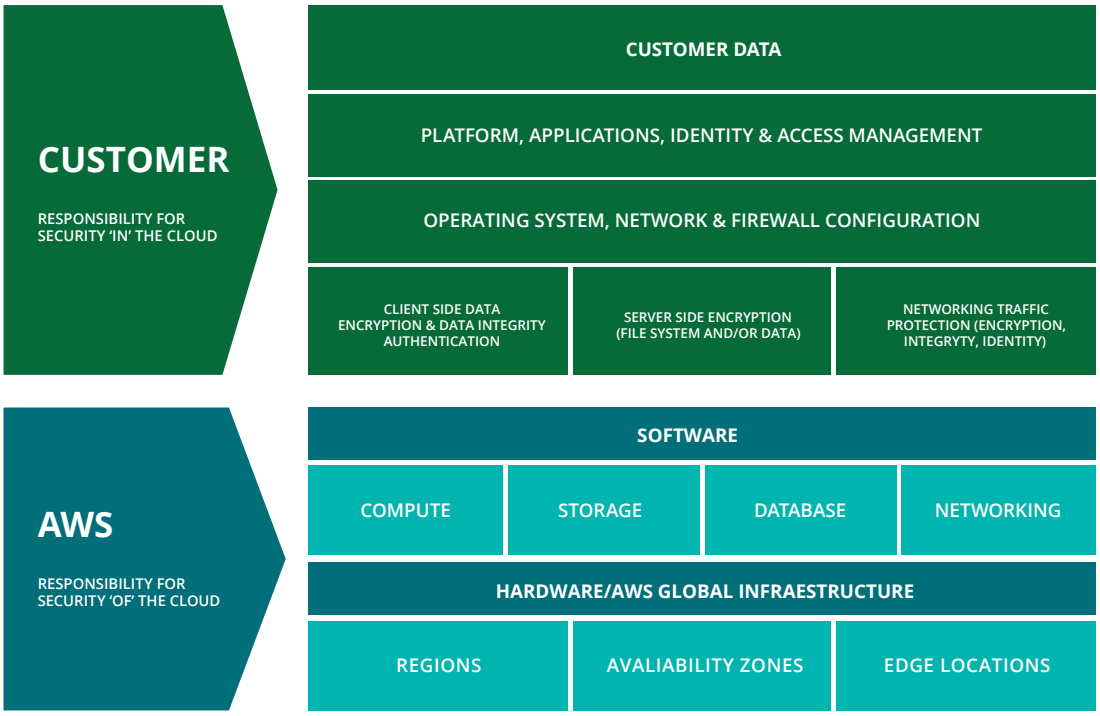
Every day, major corporations must contend with events that have the potential to interrupt normal business operations and, quite literally, hold computer files and operations for ransom. These events are becoming more sophisticated and increasingly common.

Implementing a secure architecture with the necessary controls to prevent ransomware events is critically important as they are not deployed during a single isolated event but in multiple stages and involve different parts of the organization. An outside party may attempt to penetrate a network, steal credentials, gain unauthorized access to the backup admin console, block access to the organization's data, and exfiltrate it.

Many leaders often feel uncertain about how to deal with such sophisticated, multipronged unauthorized access attempts. But organizations need to evolve to mitigate emerging risks, especially with the recent commoditization of ransomware, or availability of ransomware-as-a-service. To limit the impacts of painful financial costs, and other negative results brought about by such events, it is extremely important to assess and remediate any potential vulnerabilities and issues as soon as possible. These include dormant user accounts and credentials, preventing unintended network access, blocking phishing emails, and Remote Desktop Protocol compromises.

Deloitte and Amazon Web Services (AWS) can help you design your AWS environment with ransomware resilience. With the AWS shared responsibility model illustrated in figure 1, AWS is responsible for security of the cloud, while the customer is responsible for security in the cloud. This means that the customer assumes responsibility and management of the guest operating system (including updates and security patches) and other associated software, as well as the configuration of the AWS security groups. By leveraging a combination of AWS solutions, the AWS Well-Architected framework, and security leading practices, organizations can be better positioned to maintain a security posture that proactively limits the risk of unauthorized access to data and may help prevent attempted ransomware events from succeeding.

Figure 1. AWS shared responsibility model



A two-pronged approach to resilience: Security and recovery

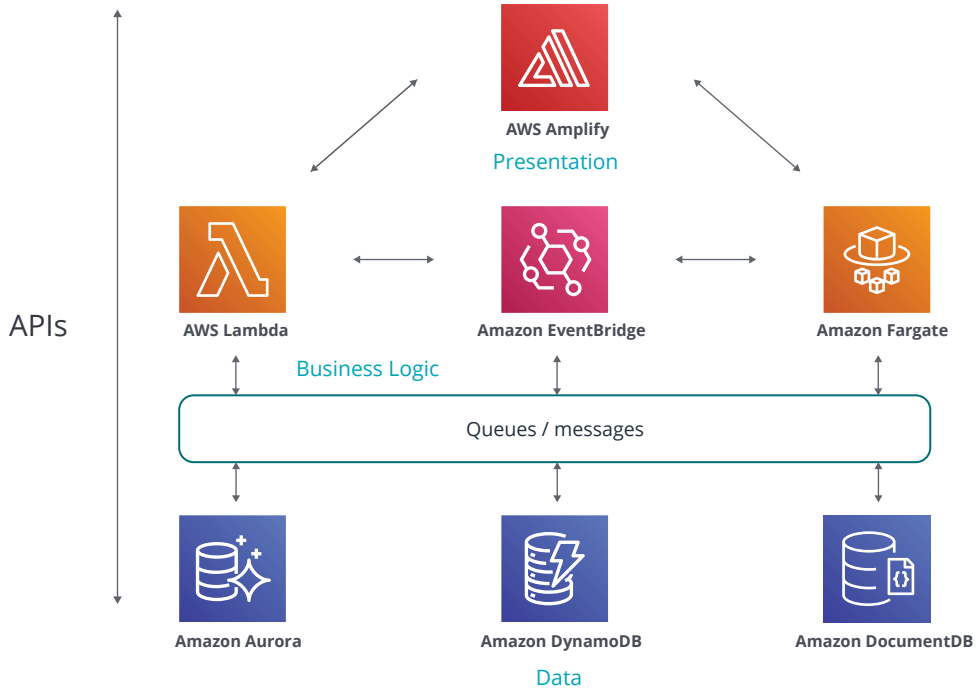
Resilience is a product of security and the ability to recover. In the information age, data comprises an ever-increasing share of your company's intangible value. Cybersecurity, then, is not only important, but potentially existential. As such, heading off a multisector event requires bigger thinking than a simple firewall. At any given moment, a chief information security officer may feel confident that an organization is adequately protected, but rapidly advancing technology and techniques could open new cracks even in a defense-in-depth strategy.

Older ransomware doesn't disappear: Traditional backups may leave undetected viruses intact and, if used for restorations, may introduce malware to the new environment. Modern security services and solutions can help streamline and bolster ransomware preparedness by detecting abnormal file activity, identifying specific user accounts, and blocking further hostile action. If an event occurs and a host becomes infected, these controls and processes can help isolate infected areas and accelerate a clean recovery. Such efforts help your business expedite a return to normal operations and can keep the business resilient.

AWS removes the undifferentiated heavy lifting by providing customers with the infrastructure and services they need to run workloads securely and reliably. This means leveraging AWS to create a modern architecture (figure 2) that spans AWS Regions and Availability Zones, allowing systems to be highly available and highly scalable with AWS Auto Scaling. Fault-tolerant, self-healing workloads employ a service-oriented architecture with decoupling via Amazon EventBridge and microservices running in AWS Lambda or AWS Fargate. A modern decoupled architecture limits the impact in the event of a failure or security event and also provides greater resiliency, scalability, and efficiency.

Additionally, AWS Security services such as Amazon GuardDuty help detect intrusions, and AWS Security Groups protect the company network via micro-segmentation to isolate network traffic and limit the scope of impact. Amazon S3 offers immutable storage providing both resilient data storage and tamper-proof backup policies that protect systems from external and internal events as well as administrative mistakes.

Figure 2. A modern architecture on AWS



Security: AWS Security services help guard the business against ransomware

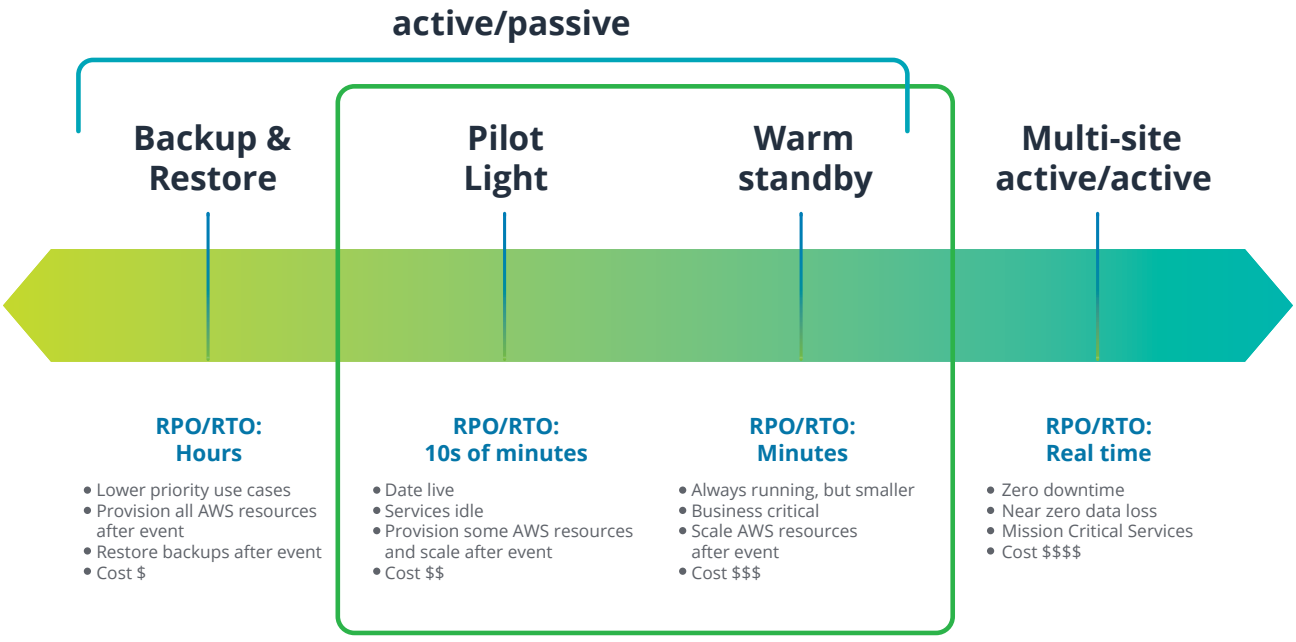
AWS Security services and features provide distinct advantages when defending against ransomware events. Identity and Access Management (IAM) is crucial given that ransomware aims to gain elevated privileges to exfiltrate data, corrupt backups, encrypt files, disturb operation and services, and gain broad access to the environment. For this reason, utilizing leading practices for IAM—along with patch management, network segmentation, firewalls, and security posture and monitoring—must remain as top priorities.

Using AWS IAM roles along with policy guardrails gives organizations greater control over which users have access to resources and data. Segmenting applications and workloads into AWS accounts is another way that customers can counter these events on AWS. AWS Organizations provides you with service control policies that can be used as guardrails and help enforce governance. This would further limit the scope of impact to resources if credentials from one account are compromised by preventing unauthorized users from accessing data and resources in other accounts.

Deploying applications to different geographically separated AWS Regions and multiple AWS Availability Zones is a critical part of resiliency. Amazon Virtual Private Cloud (VPC) provides a logically isolated virtual network in a region that can span each Availability Zone where you can deploy and run highly available systems. Deploying a reduced set of redundant resources as a warm standby (figure 3) in an alternate region can reduce recovery time significantly by having the infrastructure in place to handle requests in near real time, and then scaling out to satisfy the full production workload.

When the recovery time objective (RTO) allows, deploying infrastructure as code with AWS CloudFormation can help reduce the cost of recovery. This strategy is referred to as a Pilot Light (figure 3), and when utilizing this approach, it is critical that deployments are consistent and predictable. Using AWS CodeDeploy is a fully managed deployment service that eliminates the need for error-prone manual operations by automating software deployments to both primary and secondary sites.

Figure 3. Recovery strategies on AWS

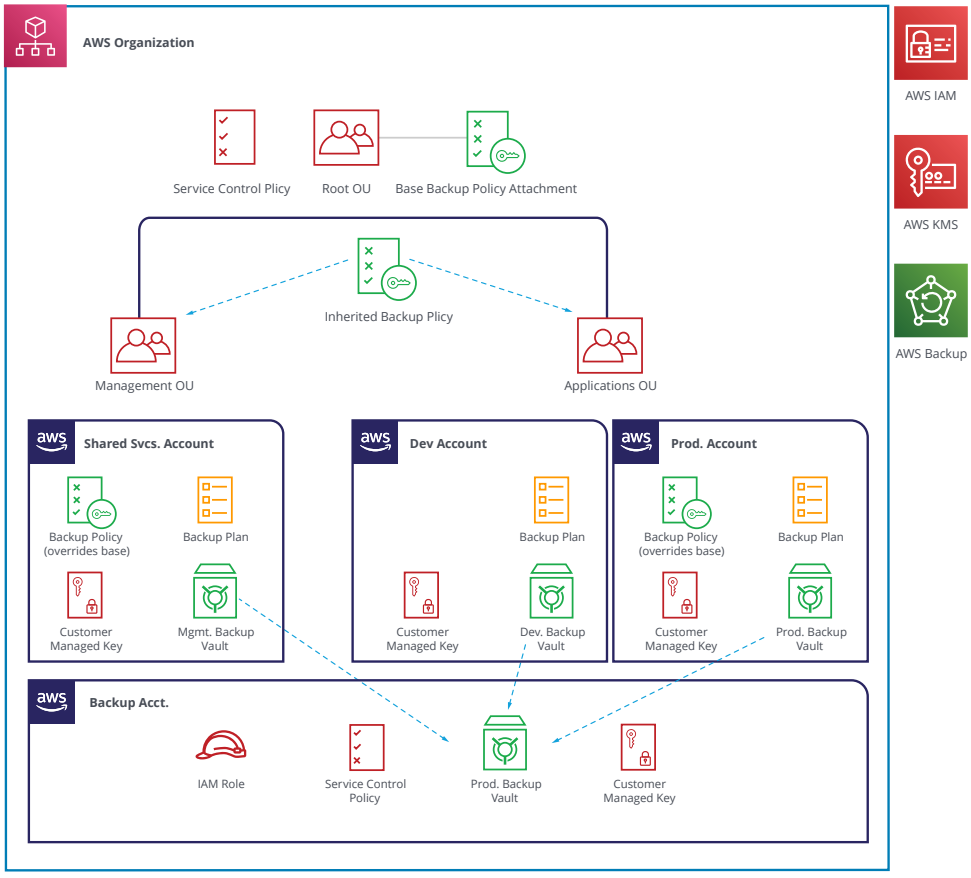


Data resiliency can be achieved with AWS Backup, as shown in figure 4, which provides you with centralized and automated data protection across your AWS availability zones and regions. When coupled with AWS Organizations, you can centrally deploy backup policies across your organization's AWS accounts and resources. AWS Key Management Service (KMS) is an important component of data protection, providing secure management of the keys that encrypt the data stored on your resources and the copies stored in your backup vault. To protect backups, organizations can leverage separate AWS accounts and allow read-only access to the archive using a different AWS IAM role. This provides additional barriers for an outside party to overcome.

A deep retention strategy can benefit from AWS S3 Lifecycle policies and Glacier archives that are kept "on ice" and can be configured via governance or compliance mode to make even the backup policies immutable. Of course, relying on the retrieval of data stored in an archive storage tier will mean a longer recovery time.

AWS Config enables you to continuously monitor, assess, and manage changes to your AWS resources. AWS Firewall Manager offers centralized management of firewalls across AWS accounts and applications. Then with AWS Security Hub, findings from AWS CloudTrail, AWS Config, AWS Firewall Manager, and other AWS and partner security services are aggregated and displayed in a single, comprehensive view (figure 5).

Figure 4. AWS Backup across AWS accounts with immutable vaults



AWS Systems Manager Patch Manager supports mass patching, and you can configure it to automatically patch your instances. Continuous assessments of vulnerabilities can be achieved through Amazon Inspector and AWS Config, and you can track the changes of your AWS resources. Maintaining compliant configurations is accomplished by using AWS Security Hub Automated Response and Remediation (SHARR). As findings come into Security Hub they trigger events that send out alerts and trigger automation to remediate non-compliant changes to AWS resource configurations (figure 6).

Other AWS logs can be stored in a central repository and apply additional enrichment to help advanced analysis and analytics. Using Amazon GuardDuty further helps organizations understand event vectors and patterns by intelligently monitoring your AWS account for malicious activity and providing detailed security findings and remediation.

Figure 5. AWS Security Hub aggregates findings for comprehensive view of security posture

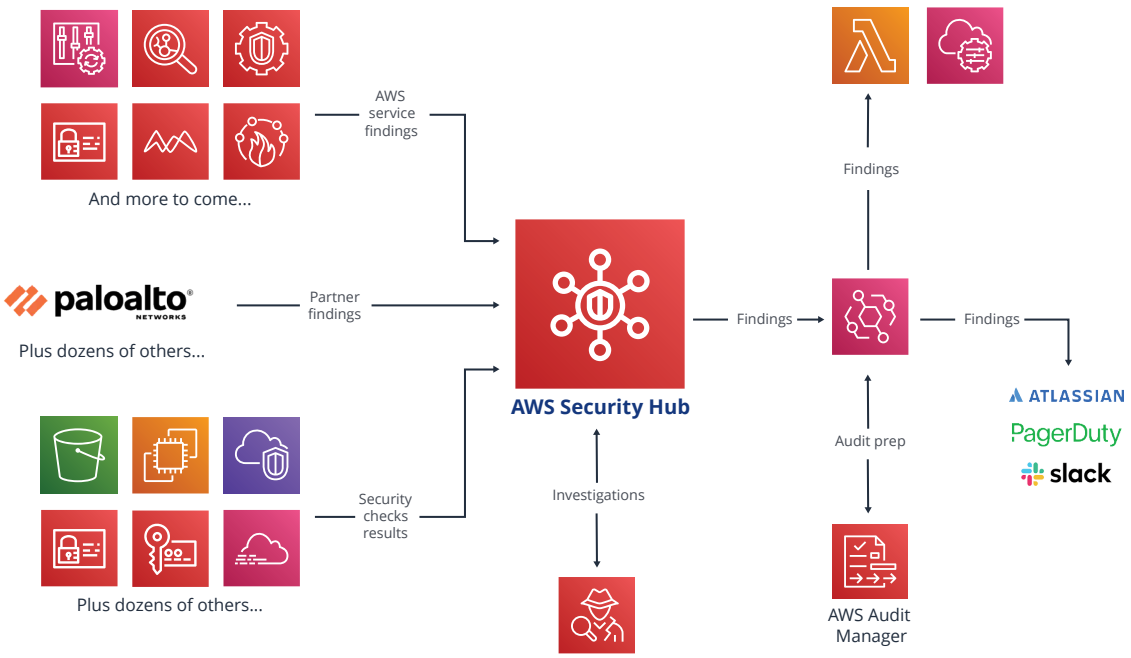
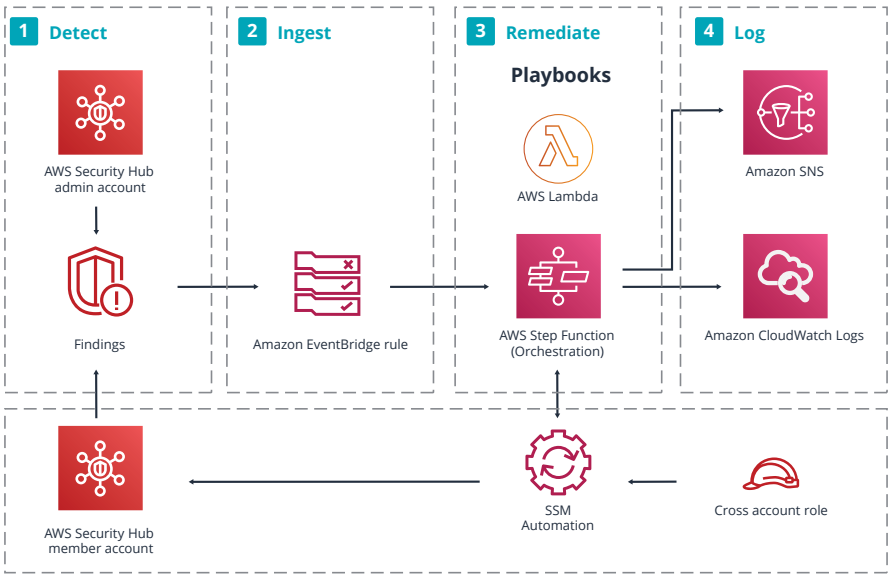


Figure 6. Security Hub Automated Response and Remediation (SHARR)



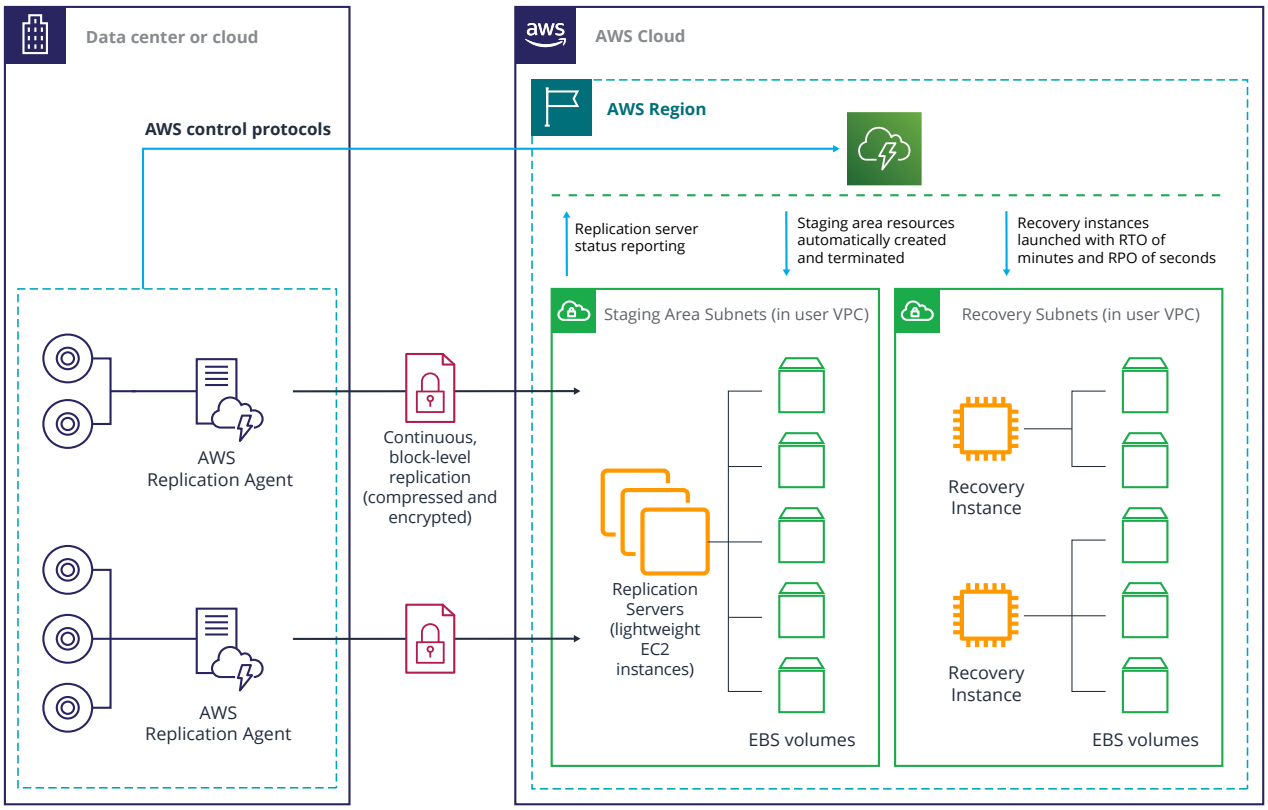
Recovery: Helping the business bounce back from an event

Defensive measures can be highly effective. Even so, it remains a challenge to stop sophisticated, highly motivated bad actors backed by organized crime syndicates, or even countries that are constantly upgrading their technology and techniques. Immutable backups and a risk-appropriate retention strategy are essential to prepare for the worst-case scenario from destructive malware. Surviving a ransomware event requires recoverability that includes planning and perseverance. Leveraging tools like AWS Elastic Disaster Recovery can provide the flexibility to recover compute instances and data from on-premises to AWS, between AWS regions, or even from other clouds to AWS (figure 7). It also allows companies to conduct non-disruptive DR tests; decrease downtime with fast, reliable recovery of on-premises and cloud-based applications; and reduce cost by removing idle recovery site resources until needed.

Having a strong cyber resilience and recovery program can mean the difference between mitigating damage and thriving uninterrupted. At the most basic level, AWS Backup allows clients to build automated backups of point-in-time snapshots at the object or bucket level. Taking things a step further, companies can use Amazon S3 Lifecycle policies to automate the retention strategy, and utilizing immutable (write-once-read-many, or WORM) storage—such as AWS Backup Vault Lock, S3 Object Lock, and Glacier Vault Lock—protects data from unauthorized changes.

You can streamline recovery by creating a data and system destruction recovery runbook to document and practice the process. It's possible to build confidence and muscle memory in this runbook by testing its effectiveness with simulation tools, such as an AWS GameDay.

Figure 7. AWS Elastic Disaster Recovery continuous replication of on-premises and cloud servers



Conclusion

Ransomware is driving organizational transformation across business continuity and cybersecurity, causing organizations to change the ways that they either operate or architect their environments. But leaders must adequately prepare for the transformation. In particular, they should strategically design, build, and protect ransomware-resilient solutions. These can help guard against ransomware and, ultimately, mitigate ransomware events and maintain business as usual.

Leaders need to evolve disaster recovery from a traditional approach to one that also prepares for cyber incidents—dynamically re-deploying infrastructure and applications for a quick, clean return. There is no substitute for preparedness. Proper planning for security and recovery can help limit the potential for a sudden shutdown, thereby enabling organizations to maintain business continuity.

The strength of the Deloitte/AWS relationship

With a global network, migration tools, and solution accelerators backed by leading industry and business innovation experience, Deloitte can help you guide your cloud transformation to see your possible and make it your actual.

Deloitte and AWS bring a holistic approach to our clients' business transformations. Before we design and orchestrate innovative solutions that leverage AWS technologies, our first step is to understand what our clients are confronting, along with the compliance, governance, data analytics, cyber risk, and regulatory issues that may be pertinent to not only meeting but exceeding customer expectations.

Our AWS-based business solutions, built on top of a scalable analytics platform, provide data-driven insights for our clients' leadership, help reinforce their key decisions on future opportunities, and identify actionable improvement areas to rapidly capture meaningful, measurable value for their businesses. That's why many organizations turn to Deloitte for help defining and executing cloud strategies on AWS.

Authors

Ammar Ahmed, PhD
Senior Manager
Cyber and Strategic Risk
Deloitte & Touche LLP

Jonathan Goldsberry
Senior Manager
Cyber and Strategic Risk
Deloitte & Touche LLP

Steve Bollers
Senior Partner Solutions Architect
Global Cybersecurity Leader
AWS

Deloitte.