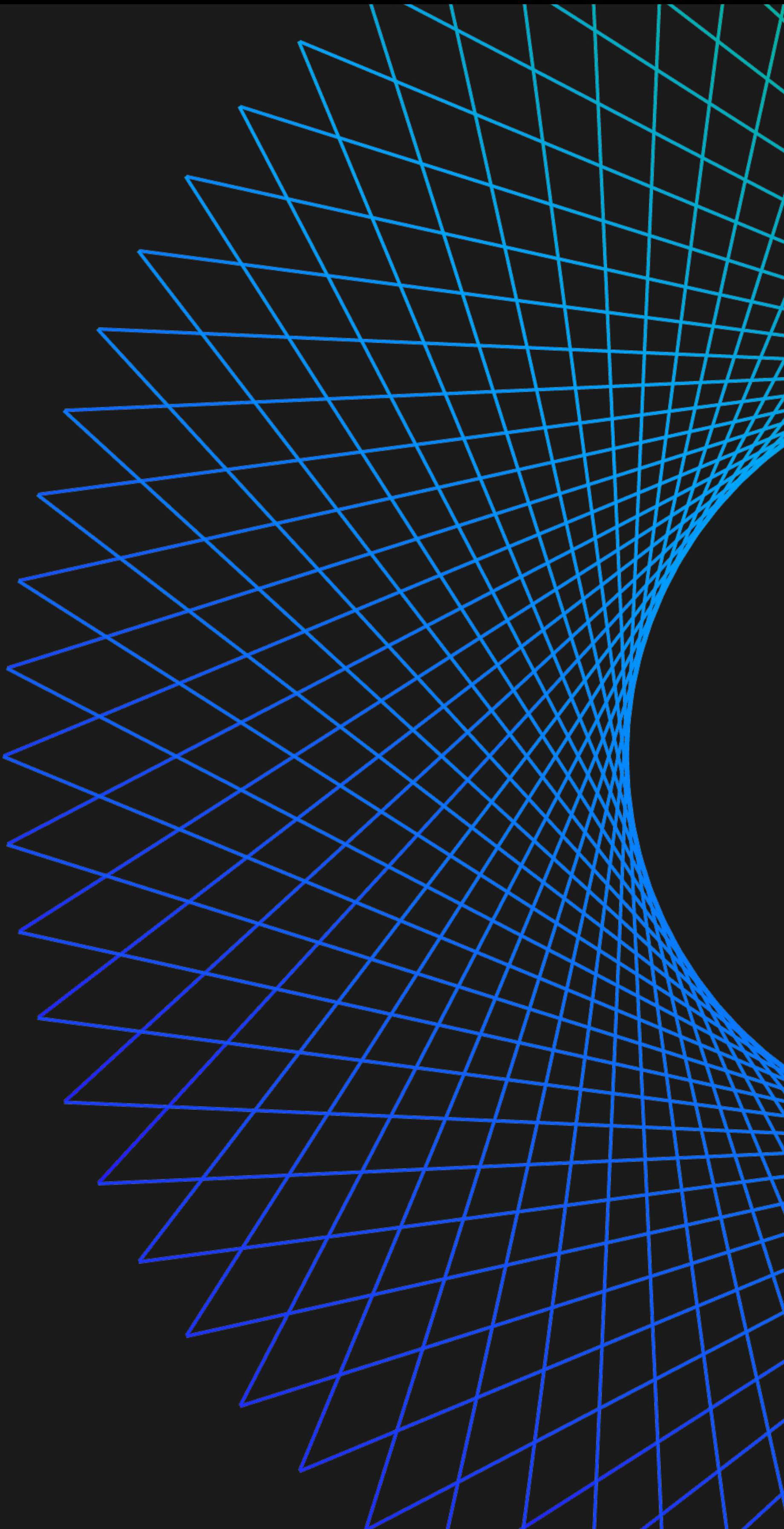
WHITEPAPER

Mitigating the ransomware threat with Trellix Cloudvisory on AWS

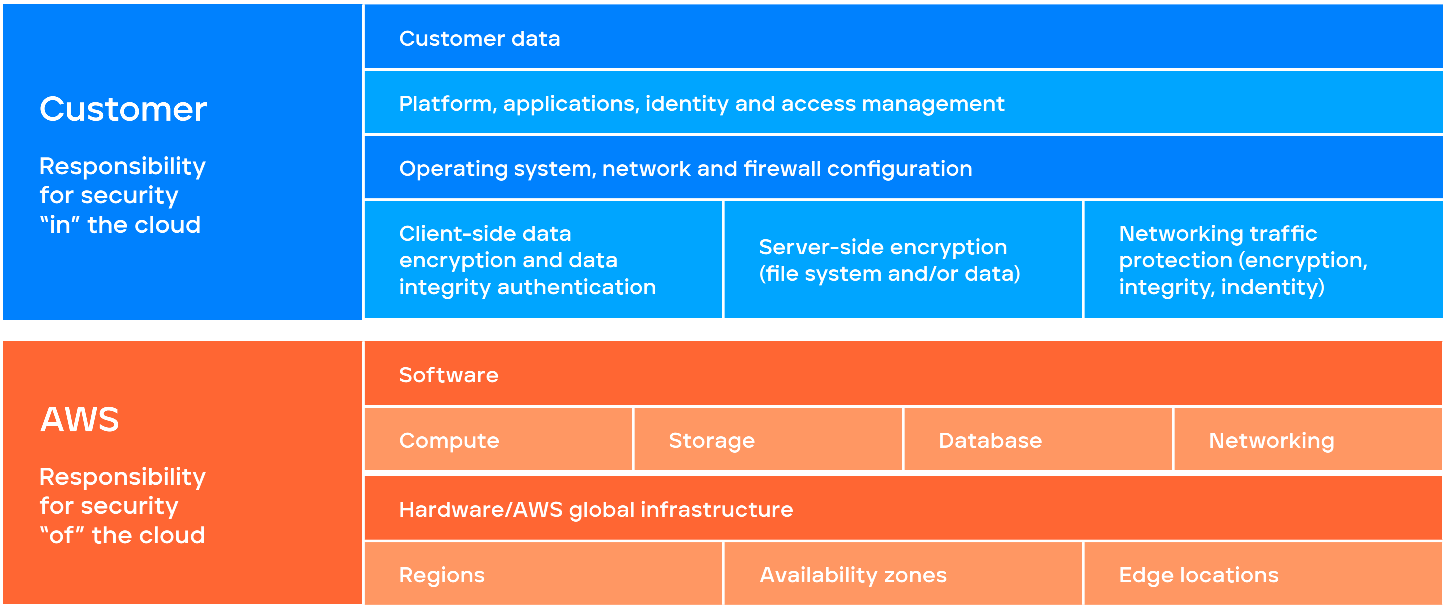
Misconfigurations can leave systems vulnerable to a cloud ransomware attack



Before migrating to the Amazon Web Services (AWS) Cloud, customers may have been responsible for the entire control set in their security compliance and auditing program. With a shared responsibility model, AWS shares the security responsibilities with you: AWS is responsible for the security "of" the cloud, while the customer is responsible for security "on" the cloud. Customers' cloud surfaces are dynamic, elastic, and on-demand. This means exposures can also be dynamic within the customers' part of the shared security model.

It is important to have a cloud security strategy that includes complete visibility, continuous compliance monitoring, management of misconfigurations, and microsegmentation. Additionally, organizations must be prepared for recovering data in the event of a ransomware attack or a natural disaster.

Many enterprises depend on self-service cloud infrastructure automation to allow the business to scale as needed. Unfortunately, this means unsecure policies and misconfigurations can be deployed at scale, at any time, with little oversight. Even knowledgeable and skilled cloud architects can find it difficult to make changes in cloud environments without making mistakes that violate the principle of zero trust and/or expose sensitive data.


Customer

Responsibility for security "in" the cloud

Customer data

Platform, applications, identity and access management

Operating system, network and firewall configuration

Client-side data encryption and data integrity authentication

Server-side encryption (file system and/or data)

Networking traffic protection (encryption, integrity, indentity)

AWS

Responsibility for security "of" the cloud

Software

Compute

Storage

Database

Networking

Hardware/AWS global infrastructure

Regions

Availability zones

Edge locations

Common sources of misconfiguration:

- DevOps teams may create unintended holes in the enterprise perimeter. For example, a developer opens network security controls such as network security group (or cloud firewall) rules to ensure their code works; however, they may have left the network exposed.
- DevOps teams typically lack the tools required to monitor the policies their tools deploy. DevOps people, processes, and technologies are all focused on ensuring the code works and applications are available. An automated policy that lets everything "just work" may also give unauthorized users broad access.
- An IT team opts to use an in-house team to deploy their cloud infrastructure, saving vendor budget. However, the internal team lacks the skills and knowledge required to securely deploy and manage infrastructure across all cloud accounts, regions, and services—leaving the enterprise vulnerable to inadvertent access and possible malicious attempts to encrypt that data to block access by legitimate users.
- A security team is formulating least-privilege security policies for modern cloud applications, but they lack the deeper knowledge of the application, cloud, and security context required to optimize security without breaking the app.
- A security team may lack the access to environments and tools required to discover cloud misconfigurations, and they may not be empowered to fix security holes due to risks of breaking production workloads

Without appropriate cloud visibility and continuous compliance monitoring, misconfigurations often go undetected until an audit or breach investigation identifies the issues. Shifting from constant intervention management to a consolidated, automated Cloud Native Application Protection Platform (CNAPP) reduces potential threats to the enterprise by ensuring immediate detection of misconfigurations and by orchestrating the response to the problem (before it becomes an incident).

Prevention is key.

Threat actors take advantage of misconfigured cloud environments with ransomware campaigns. Attackers are continually probing for an opening, such as a cloud service with overly broad permissions, to gain a foothold for spreading ransomware throughout the organization.

aws PARTNER

- Public Sector
- Marketplace Seller
- Authority to Operate
- Security Software Competency

How attackers use ransomware

The term "ransomware" refers to a type of malware that locks access to files, folders, or entire networks until a ransom is paid. (Payment is often requested through a digital currency such as Bitcoin.) It is disruptive, expensive, and affects all types of organizations—both large and small.

Once the ransomware breaches the network, the code will lock access to the network. More sophisticated attacks may encrypt specific files and folders. A successful ransomware deployment will involve both technical and non-technical challenges. The average network downtime following a ransomware attack is 19 days[1], resulting in lost income and productivity.

Ransomware by the numbers

- Average ransomware demand:
  $170,000
- Total ransom paid in 2020:
  $350 million
- Estimated per-incident cost:
  $761,000

Source: World Economic Forum, May 2021

[1] SafeAtLast blog:, https://safeatlast.co/blog/ransomware-statistics/#:~:text=The%20average%20downtime%20due%20to,a%20ransomware%20attack%20is%2019%20days

More attackers, more risks

Modern day attackers have developed advanced techniques that now require a holistic security risk mitigation strategy involving everyone from the board to practitioners. Organizations that rely exclusively on IT staff for security management, known as a "hands-on" approach, are more susceptible to accidental vulnerabilities.

When an organization folds network security management into the overall IT department duties, it places basic security maintenance in competition with other network maintenance, software updates, user requests, and issues that require immediate attention.

With this integrated IT/security scenario, the resources required to properly review, evaluate, and update network security could jeopardize the abilities and resources for the IT team.

As a result, security maintenance often falls down the list, potentially increasing risk of vulnerabilities. When maintenance teams complete updates and turn their attention elsewhere, the network can become vulnerable due to the actions of non-IT workers.

Closing security vulnerabilities through automation

Organizations like yours can reduce ransomware threats by replacing hands-on management with automation to adopt zero-trust security model and implementing security best practices as they adopt AWS.

An automated solution can address many of the core issues that can leave networks vulnerable to ransomware attacks. They provide ongoing, persistent network monitoring and resolution, significantly reducing risk to the organization while freeing staff for other tasks.

The role of microsegmentation

Microsegmentation is one of the principles of the zero-trust approach to security and is key to limiting lateral movement of any bad actor actions, including but not limited to ransomware attacks if the customer's portion of the shared security model is misconfigured. It is important to reduce a bad actor's ability to move undetected across the customer's AWS Cloud environments. With microsegmentation, bad actors can be limited in their scope if they breach an organization's defenses.

Additionally, it is important to restrict machine accounts and user access to resources leveraging a least-privilege model to further limit access to cloud resources and decrease ability to dynamically provision additional services that could be exploited.

The solution:

Trellix Cloudvisory with AWS

Trellix Cloudvisory is a cloud-native security solution for cloud environments built on AWS.

It provides unified control over cloud sprawl through centralized visibility, continuous compliance, and in-line enforcement of organization security policies.

The self-service tool provides a centralized view of an organization's cloud workloads and enables teams to manage environments using a single set of tools. With Cloudvisory, users can onboard a cloud provider, input credentials, and get actionable data in minutes—all without having to learn a new cloud system.

Additionally, Cloudvisory provides intuitive and scalable microsegmentation solutions, empowering organizations of any size to achieve microsegmentation for all cloud workloads by default. CloudVisory enables both "Contextual" Microsegmentation and "Golden State" Microsegmentation.

With "Contextual" Microsegmentation, Cloudvisory automatically discovers existing workloads across cloud providers to generate segmentation policies based on workload context. This enables organizations to build highly consistent and immutable security policies spanning complex hybrid- and multi-cloud environments. And it also enables them to gain operational agility to business DevOps and security teams by removing the complexity of managing microsegmentation rules at scale.

Cloudvisory enforces "Golden State" Microsegmentation rules based on static policies for IP addresses, providing recommendations for policy updates by leveraging machine learning correlations between actual network flows and current network policies. Cloudvisory is able to do this via:

- Automatic discovery and enforcement of existing network security policies (security groups)
- Learning desired state behavior through agentless collection and analysis of actual network flows
- Recommending network security policy improvements based on machine learning
- "Dry run" testing of the impact of such changes prior to implementation

Trellix Cloudvisory benefits

Go cloud-native

- Leverage AWS-native security controls.
- Protect all cloud workloads with an agentless approach.
- Deliver granular protections that "follow the workload" with microsegmentation using network policies.

Trust, but verify

- Preserve self-service efficiency while gaining central oversite of deployments.
- Establish sensible limits on self-service behavior with "compliance guardrails."
- Prevent users from accessing unauthorized materials.

Compliance

- Trust and verify with self-service provisioning that also has built-in security.
- Enforce a consistent organizational security policy across disparate cloud environments.

Detect and respond

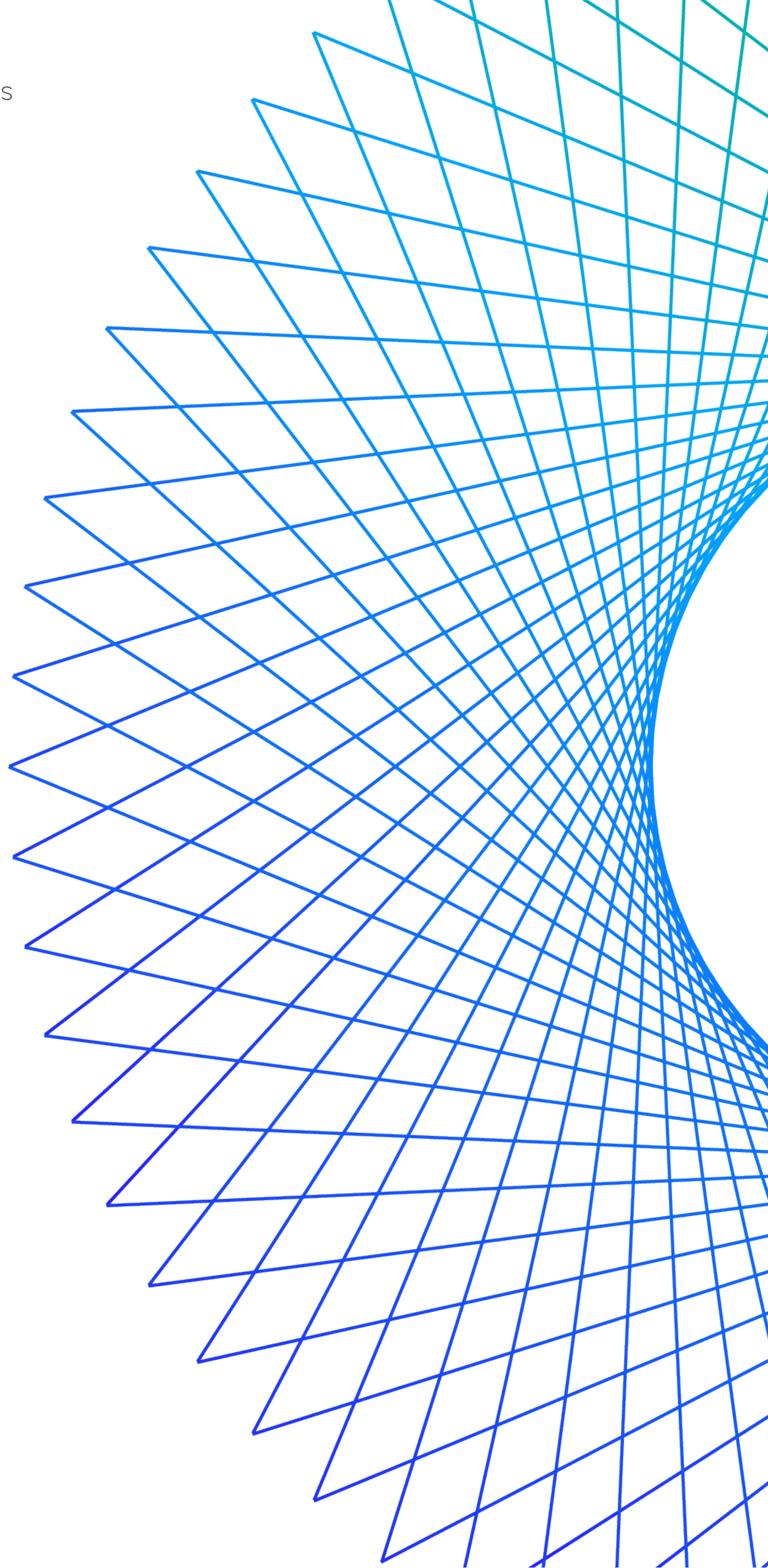
- Centralize security data to accelerate response and minimize impact of cloud-based security issues.
- Implement push-button and/or automated remediations for rapid incident response.

Simplify security operations

- Streamline security by consolidating security tools and processes.
- Reduce security staffing.
- Automatically discover and scan new resources, even in previously unused regions or services.

aws PARTNER

- Public Sector
- Marketplace Seller
- Authority to Operate
- Security Software Competency



Recovering from ransomware attacks

Organizations must have a strategy to recover from ransomware attacks or disasters. Backups are critical in mitigating the impact ransomware can have on your organization. The most effective deterrent to ransomware is to regularly back up and then verify your systems. AWS offers a number of native backup and storage services that can aid in this.

In conclusion

Ransomware remains a significant threat to all organizations, regardless of size or industry. Replacing traditional hands-on security maintenance with an automated solution helps protect your infrastructure against vulnerabilities to exploitation. In addition, organizations should have a strategy for mitigating the impact of ransomware attacks including microsegmentation, back up, and recovery. Trellix Cloudvisory offers a holistic approach to security with solutions that combine visibility, microsegmentation, protection, and a comprehensive range of services.

Learn more

Trellix

Trellix
888.847.8766
Trellix.com

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers. More at trellix.com

aws
PARTNER

- Public Sector
- Marketplace Seller
- Authority to Operate
- Security Software Competency