451 Research | insight brief

EXECUTIVE BRIEF

CLOUD SECURITY CONTROLS – A NEW APPROACH

CLOUDVISORY

THIS EXECUTIVE BRIEF CONTAINS KEY INSIGHTS FROM THE WEBINAR:

Shifting Mindset on Cloud Security Controls

CLICK TO ACCESS THE WEBINAR

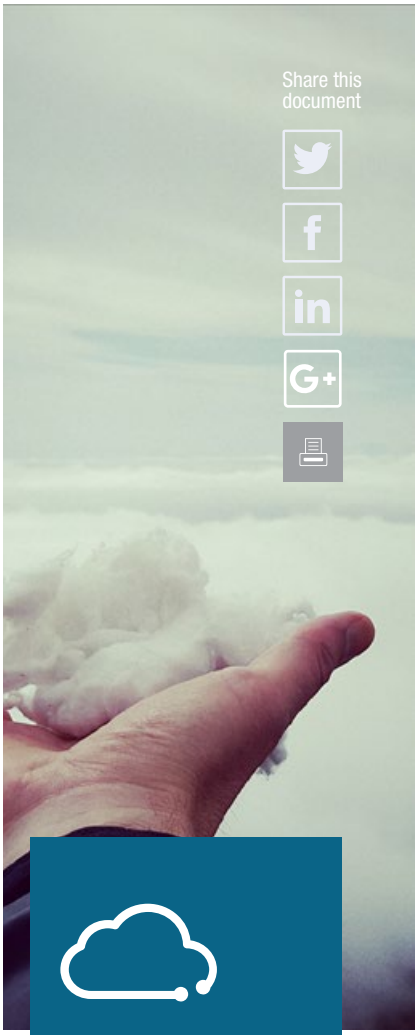
- In the webinar, 451 Research and Cloudvisory outline how organizations can successfully transition to optimal micro-segmentation and security orchestration in cloud, hybrid cloud, and multi-cloud environments. Executed correctly, this will speed up DevOps, greatly improve security and lower operational costs.

BACKGROUND

- Cloud transformations are accelerating. By 2019, it is anticipated that 60% of workloads will be deployed in the cloud. IaaS and SaaS environments to account for 37%.
- Typical places to deploy network security controls:
  - Perimeter
  - Host controls
  - Local network
  - Cloud Native Platform - Hypervisor / Security Group
- Benefits of different types of network security controls:
  - Perimeter - single point of control for the environment, additional deeper level inspection
  - Local network - a layered defense
  - Host - very elastic; deep host visibility
  - Cloud Native Platform - outside the attack zone; elastic and flexible
- Cloud architectures that support layered controls and micro-segmentation will strengthen security by minimizing the network's attack surface. Micro-segmenting provides granular separation of workload to workload communication policies and the ability to define least privilege access to harden security and halt East/West threat.

KEY POINTS

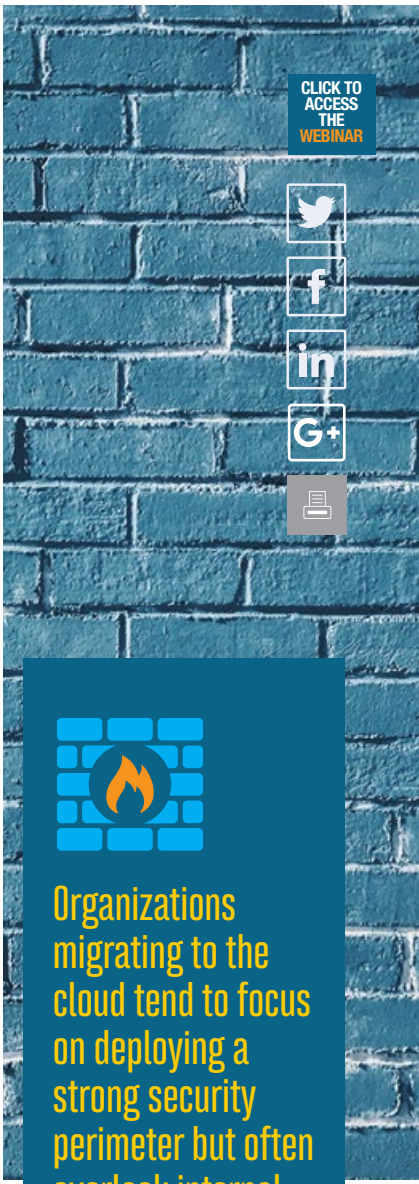
- Benefits of micro-segmentation include:
  - Granular control, on a workload-by-workload basis for accurate/fast provisioning of Policy
  - Visualization of infrastructure making it easier to identify violations
  - Regulation of internal threats
  - Minimizes attack surface of the network
  - Flexibility in moving workloads around for rapid change management
  - Monitoring and Enforcement of policy violations in real-time, avoiding threats and halting application outages.
- The six common migration paths organizations follow according to AWS:
  - Rehost - 'lift-and-shift' to the cloud
  - Replatform - lift and reshape with adjustments
  - Repurchase - moving to a different product
  - Refactor - re-imagining how applications are conceived and developed
  - Retain - migrating only what's needed
  - Retire - getting rid of unnecessary applications



Cloud transformations are accelerating. By 2019, it is anticipated that 60% of workloads will be deployed in the cloud. IaaS and SaaS environments to account for 37%.

KEY POINTS (cont.)

- Cloud transformation requires planning, particularly regarding security control. For example, if not careful, deploying hybrid or multiple cloud environments using a lift-and-shift migration strategy may result in suboptimal control, leaving the organization vulnerable to unnecessary risk.
- Empirical evidence from public cloud providers suggests organizations using a lift and shift migration strategy should do so in conjunction with cloud-native controls such as AWS or Azure network security groups. This provides the ability to realize workload level micro-segmentation, which decreases the attack surface, thwarting any risk and threat.
- Cloud providers use different terms to describe cloud-native controls:
  - AWS - security groups
  - Azure - network security groups
  - Google Cloud Platform - Compute Engine firewall rules
  - OpenStack - security groups
- Organizations migrating to the cloud tend to focus on deploying a strong security perimeter but often overlook internal firewalls. The consequences can be far-reaching; intruders have unhindered lateral movement and can go undetected for months.
- Tips for moving to the cloud, securely:
  - Understand the impact on existing security practices, before making any decisions
  - Think through the security policies for cloud workloads
  - Evaluate the pros and cons of cloud-native Vs. third-party security controls
- Compared to third-party controls, cloud-native security controls are:
  - Less Intrusive - supported by the cloud service provider; so no retrofitting required
  - Cost effective - no charge; included with existing cloud deployments
  - Configurable – allows for configuring granular *least privilege* security control
  - More secure – controls are outside the attack zone of the workload, where security decisions are made before the traffic gets to the workload. Separating policy enforcement from the workload itself, increases and thwarts the efforts of the hacker and any respective malware
- Cloud security is no longer the sole domain of one team. Security information should be agreed and aligned between development, operations and security teams - essential as workloads move through the DevOps pipeline.
- Cloud is changing traditional security practices. The new approach includes:
  - Security embedded in DevOps pipeline
  - API integration
  - Data science
  - Automated tasks
  - Scale and agility
- Challenges with cloud-native security controls: (why security automation controls are needed in conjunction with Cloud-Native)
  - Lack of visibility - black box deployment
  - Erroneous security settings - time-consuming to flush out
  - Mistakes - misconfiguration & mismanagement
  - Breaches - takes too long to identify threat



Organizations migrating to the cloud tend to focus on deploying a strong security perimeter but often overlook internal firewalls The consequences can be far-reaching; intruders have unhindered lateral movement and can go undetected for months.

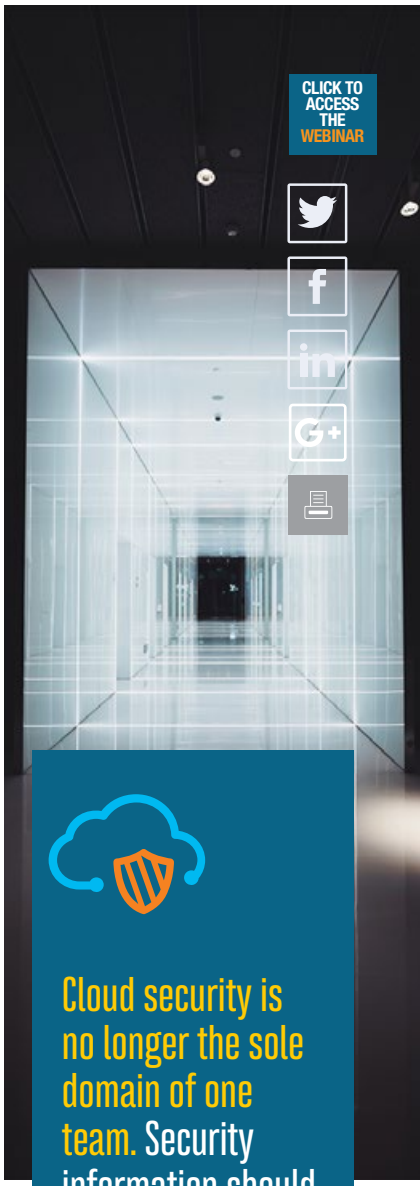
CLOUDVISORY'S OFFERING

(Key points on company offering made by Cloudvisory in the webinar)

- Through 2020, 80% of cloud breaches are predicted to be due to misconfiguration and mismanagement of cloud-native security controls, not provider vulnerabilities. Dealing with multi-cloud security controls is at the heart of this problem. The Cloudvisory Security Platform de-risks and manages this issue for organizations.
- Cloudvisory Security Platform (CSP) helps facilitate, manage and automate existing cloud- native security controls via native API, without imposing additional controls. CSP works across AWS, Azure, OpenStack, Kubernetes, and Google Cloud Platform as well as hybrid cloud and multi-cloud environments.
- The Cloudvisory Security Platform monitors:
  - Network security group policies, at the workload level
  - Real-time data flows and communication between workloads – and how these compare with deployed policies
  - The policies themselves and any attempts to change them
- The Cloudvisory Security Platform comes with the following key benefits:
  - Actionable Audit - Discover, Visualize & Audit to uncover existing risks and threats in minutes
  - Compliance Assurance - Cloud-native policy guardrails that identify, alert on and remediate risk in hybrid, multi-cloud deployments
  - Automated Micro-Segmentation - Cloud-native micro-segmentation, policy orchestration and automated enforcement to guarantee immutable security
- The Cloudvisory Security Platform provides dynamic visualizations of the entire hybrid/multi-cloud environment, including VMs, containers, microservices, security policies and associated real-time network data flows. The interactive maps created help identify malicious and non-compliant activity in real-time.

TAKEAWAYS

- With increasing number of workloads migrating to the cloud, a rethink of traditional security is a prerequisite. The choice between cloud-native security controls and third-party tools should be carefully considered.
- For cloud-native security controls, efficient management is essential when overseeing large numbers of servers in cloud, hybrid cloud or multi-cloud environments. Automation - made easier with platforms like CSP can help reduce operating costs, boost organizational agility and accelerate deployments.



Cloud security is no longer the sole domain of one team. Security information should be agreed and aligned between development, operations and security teams - essential as workloads move through the DevOps pipeline.

Click or scan to access the webinar:

CLICK TO ACCESS THE WEBINAR

Share this document

ABOUT CLOUDVISORY

CLOUDVISORY

Used by Security, DevOps and Business teams, the Cloudvisory Security Platform (CSP), was developed for cloud, hybrid and multi-cloud environments. It was built to deliver the most powerful, centralized cloud security management, audit, compliance, micro-segmentation and security orchestration solution available. The only complete Cloud Security and Compliance platform that leverages cloud-native controls of various providers, CSP works across AWS, Azure, Kubernetes, OpenStack, VMWare and bare metal environments, helping large enterprises to speed up business, reduce risk and thwart today's most dangerous hackers.

www.cloudvisory.com

The objective content from 451 Research is brought to you through the lens of InsightBrief, a publisher of technology and business information.

ABOUT 451 RESEARCH

451 Research

With a core focus on technology innovation and market disruption, 451 Research provides essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. 451 Research and its customers benefit from the combined assets and talent of The 451 Group and its two divisions: 451 Research and Uptime Institute.

www.451research.com

ABOUT INSIGHTBRIEF

insight brief

InsightBrief is dedicated to simplifying access to knowledge in a wide range of technology and business related topics, by developing, publishing and amplifying short-format content that helps busy professionals get key information, faster. The team vet and qualify the source content for relevancy and value to its intended audience before creating an InsightBrief asset. The editorial team is independent from the originator of the source material, ensuring that the insights exclude sales or vendor centric messaging, thereby creating real value for time-poor professionals.

www.insightbrief.net