TRENDS REPORT

Getting Started With Zero Trust In The Cloud

Use ZT Principles To Anchor Security In Hybrid And Multicloud Environments

May 22, 2023

By Andras Cser, Heath Mullins with Merritt Maxim, Tracy Woo, David Holmes, Lee Sustar, Devin Dickerson, Andre Kindness, Hailey DiCicco

FORRESTER®

Summary

Cloud adoption has become so ubiquitous that some early cloud deployments are already legacy. But despite cloud's prevalence and the ongoing evolution toward cloud-native technologies, few firms have adapted their security strategy and architecture in response. Security leaders should apply Zero Trust security principles to today's hybrid and multicloud environments so their organization can protect data by monitoring, automating, and orchestrating security for workloads, networks, and identities regardless of hosting model, location, or device. This report details how to apply Zero Trust principles to secure the cloud.

Zero Trust Principles Anchor Cloud Security Strategy

Although security decision-makers in Forrester's Security Survey, 2022 indicated that their organization allocated 14% of its security budget to cloud security on average, a significant percentage still say that boosting their cloud security strategy is a top priority for the coming year (see Figure 1). A piecemeal approach to securing ubiquitous multicloud and hybrid deployments won't work; instead, it requires an architectural approach and capabilities appropriate to the unbounded nature of cloud workloads and data. This is where Forrester's Zero Trust Model for information security comes in; its core principles are a perfect fit for cloud environments where data proliferates across geographies and jurisdictions. Zero Trust also works well in environments where workloads scale automatically with demand and those developed with cloud-native technologies move between on-premises and cloud environments. Keeping Forrester's three principles of Zero Trust in mind, security leaders must:

- **Eliminate implicit trust.** All entities should be untrusted by default. You must explicitly define trust using device posture, workload type, and the identity context of every access session — and then continuously review it. For organizations that support anywhere work, the ability to directly connect employees to cloud workloads in a secure manner (without a VPN) from any device is vital to both employee productivity and cybersecurity.
- **Enforce least-privilege access.** Give human and machine identities, applications, and computing infrastructure the bare minimum of access needed to perform their function. There are several reasons that least-privilege access is especially relevant in the cloud. There are far more security policy types; Amazon Web Services (AWS) identity, session, resource, and access control list policies are but a few examples. Cloud infrastructure is ever-changing as providers add new compute and database services. And cloud workloads have far more administrators (e.g., developers, outsourcers) than legacy on-premises workloads.
- **Implement comprehensive security monitoring.** Cloud security monitoring involves aggregating infrastructure service logs; analyzing logs for changes in configuration, access rights, and data access patterns; and using security analytics and aggregation to ingest and analyze logs from on-premises and private cloud architecture to create a common repository. Cloud workloads' ephemeral elasticity makes log analysis more difficult: IP addresses and network traffic routing may change dynamically, making it harder to understand logs and detect threats. Cloud security analytics natively supports the controls needed to stop, remediate, isolate,

and remove detected threats. Cloud infrastructure service provider logging solutions like AWS CloudTrail and Microsoft Sentinel not only support infrastructure changes on their own platforms, but also process and analyze logs and events on others.

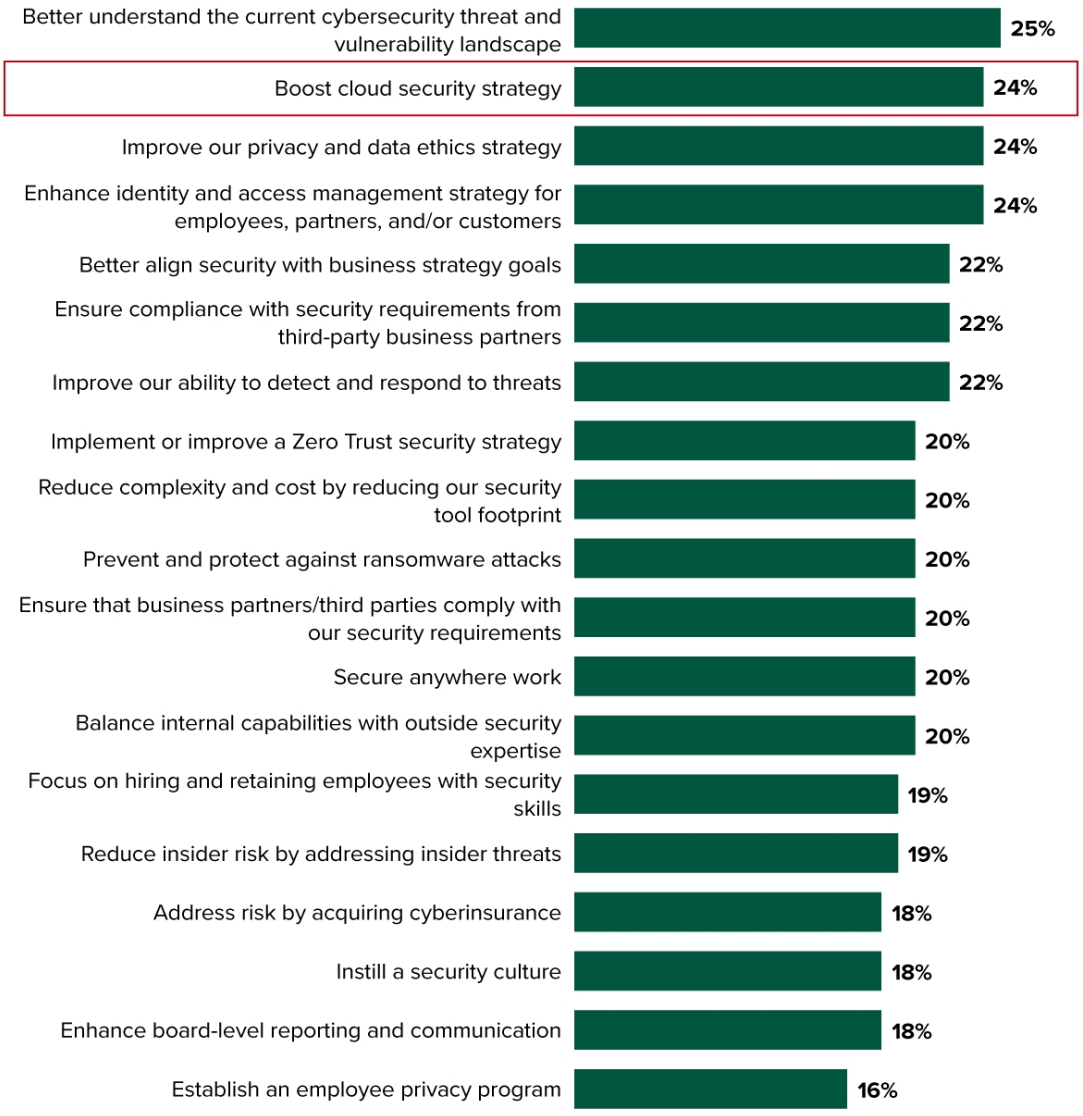
- **Attach cloud security to cloud management.** You can't separate cloud security from cloud management. Cloud security pros must work with their firm's cloud administrators and with cloud infrastructure engineers on the corporate cloud platform team to establish cloud workload instrumentation and cloud infrastructure configuration management processes. A French manufacturer told us that this transition required a significant time commitment and changes to attitudes and behaviors on the part of cloud management, IT security, and DevOps teams.
- **Harness cloud-native deployment, rearchitecture, and migration initiatives.** Cloud security should build on the firm's ongoing cloud deployment and rearchitecture projects. Imbuing cloud infrastructure with security at the infrastructure and workload planning and architecting phase is far simpler than bolting it on afterwards. New cloud-native design patterns like serverless and Kubernetes-based with built-in security features also help to establish Zero Trust from the start.

Figure 1

Cloud Security Remains An Important Security Priority

"Which of the following initiatives are likely to be your organization's top strategic Information/IT security priorities over the next 12 months?"

(Select up to five)



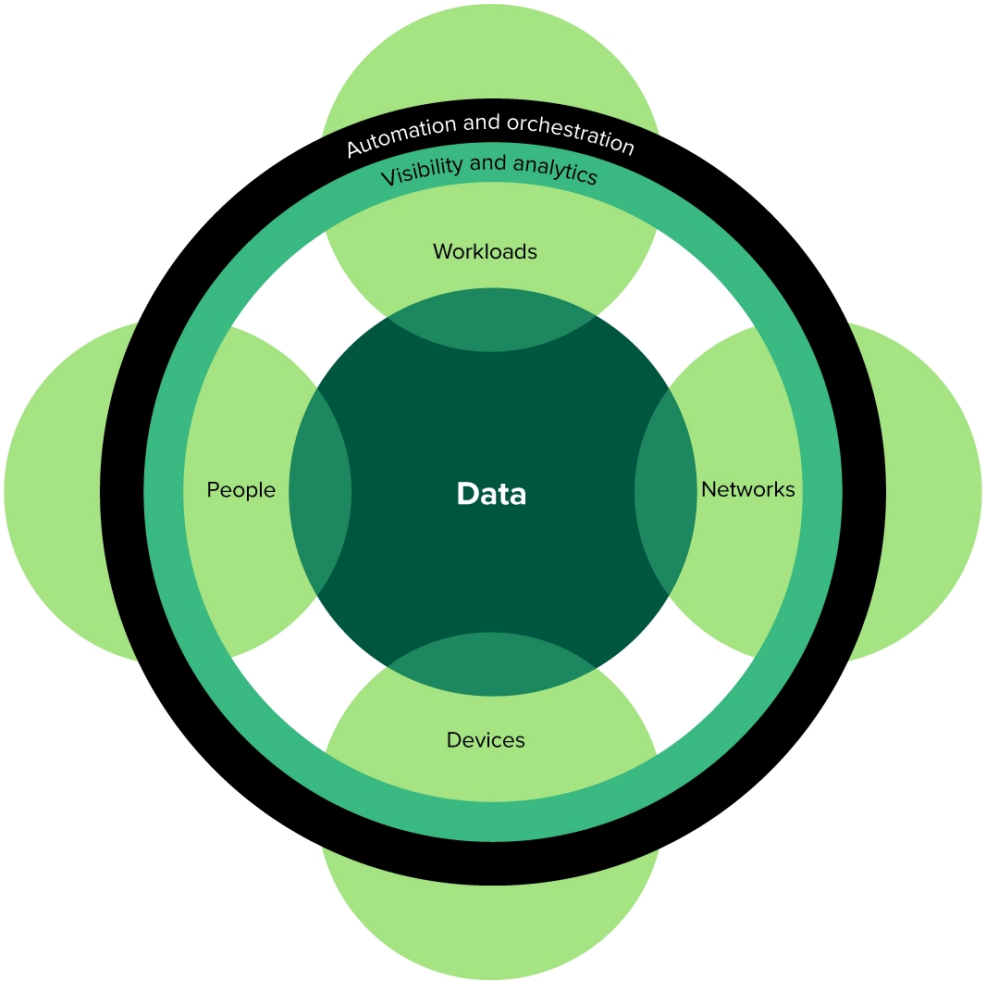
Base: 3,646 global security decision-makers

Source: Forrester's Security Survey, 2022

The Zero Trust Model Ensures Comprehensive Cloud Security Controls

To help organizations achieve Zero Trust, Forrester created a conceptual model for mapping the necessary strategy, capabilities, and technology (see Figure 2). Each pillar of the model has some key technology trends and requirements related to cloud security.

Figure 2
The Zero Trust Model



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Data: Discover, Prioritize, And Encrypt All Data

Without adequate cloud data protection, organizations cannot migrate on-premises data to the cloud. Zero Trust data protection in the cloud ensures that your firm's sensitive data and encryption keys do not fall into the wrong hands. It requires security professionals to:

- **Discover unencrypted and encrypted data and focus on cryptographic agility.** You can only effectively protect data that you've identified and prioritized according to the risk it carries. In addition to e-discovery solutions, you can use cloud-native security capabilities such as AWS Macie and Microsoft Purview to discover data in cloud workloads. You can also use dedicated data security platforms, which have the benefit of covering public cloud, private cloud, and on-premises. Data protection is critical because advances in quantum computing will render encryption algorithms like RSA and elliptical curve cryptography breakable and thus unusable. To ensure that your firm is ready to embrace post-quantum encryption algorithms quickly, upgrade your infrastructure, commercial off-the-shelf, and in-house developed software to enable easy replacement and maintenance of the cryptographic algorithms they use.
- **Choose cloud-native or third-party key management.** While cloud-native key management tools such as AWS Key Management System (AWS KMS) and Azure Key Vault may work well for platforms where keys will encrypt and decrypt data, large enterprises often prefer to keep keys in solutions such as on-premises hardware security modules (HSMs) by firms like Thales and Ultimaco. HSMs offer more resilient protection by allowing you to keep your keys instead of putting them in a cloud platform key store like AWS KMS. Keeping your keys adds hardware, software, and operating costs to cloud data protection — but it's often the only acceptable option for large, risk-averse organizations to separate key material and encrypted data storage.
- **Define role-based access control to keys.** Modern HSMs and KMSes all allow granular definition of access controls to the key store; ensure that only authorized administrator and machine identities can access it. Use time-based limits to key access, such as no key access outside business hours or no key access without business justification in a help desk ticket. A German bank told us that it had to switch HSM vendors because it needed much more granular HSM access rights management and prebuilt role-based access control at the HSM level.
- **Extend data protection to nonproduction environments.** Hackers don't stop at exfiltrating production data. If your infrastructure's other environments

(development, quality assurance, staging) contain unencrypted sensitive data, you can be sure that hackers will eventually find and steal it. Thus, you must use microsegmentation in cloud environments to clearly identify which software and infrastructure components belong to and access data in which environment; obfuscate or mask production data when transferring it to nonproduction environments; encrypt all nonproduction data; and use cloud security posture management (CSPM) and software-as-a-service (SaaS) security posture management (SSPM) solutions to monitor cloud infrastructure services and SaaS platforms for configuration changes. A US bank used SSPM provider AppOmni to cover data access rights by nonproduction Office 365 and Salesforce instances and detect excessive developer data access in these environments.

Network: Use Zero Trust Edge To Secure Your Cloud

Cloud networks are just that: networks. Zero Trust principles apply to networks regardless of location, deployment, dependencies, or connections. While cloud-first deployments are widespread, 38% of purchase influencers in Forrester's Buyers' Journey Survey, 2022 whose organizations are or will be purchasing network infrastructure and services say that their organization still relies on a hybrid deployment architecture. When developing a cloud Zero Trust strategy to protect networks, you should:

- **Know your network and redesign it for security and visibility if needed.** Without complete visibility into your network, assets, and application dependencies, your organization will struggle to apply security and access policies appropriately. To plan for monitoring and interception (SSL termination, firewalls), map the ingress into and egress from cloud workloads to the internet and from your legacy on-premises and private cloud infrastructure. This is important to ensure route sovereignty when network traffic containing sensitive data must not move out of jurisdiction. This often results in some infrastructure consolidation — which is good for network security.
- **Embrace software-defined networking and native cloud infrastructure security.** Cloud infrastructure services have rich capabilities for software-defined networks (SDNs), complete with classic network infrastructure and security features including subnets, regions, zones, switching, and firewalls. SDNs offer central visibility and security audit of network configuration and rapid threat response in case of a compromise — you needn't replug ethernet cables to isolate compromised compute instances. Each cloud infrastructure services platform has its own security and networking methods. Cloud infrastructure service providers offer native next-generation and web application firewalls that are on par with

third-party virtual appliances on cloud infrastructure services marketplaces such as Palo Alto.

- **Implement network analysis and visibility and eliminate VPNs.** Zero Trust network access (ZTNA) should replace VPN architecture across the enterprise. Deploying ZTNA technologies gives local and remote users access to on-premises, cloud-based, hybrid, and multicloud applications. Virtual private clouds (VPCs) and virtual networks (VNETs) enable granular access policy enforcement to virtual compute and network environments. Monitor network sessions across the network infrastructure of public cloud infrastructure service providers for insight into potential credential misuse and unusual data movements. Implement network analysis and visibility technologies to understand application and network dependencies, discover lateral movement, identify insecure cryptographic protocols, and find unencrypted traffic in the clear.
- **Encrypt all network traffic and automate SSL certificate lifecycle management.** Network traffic encryption isn't just for external connections. To harden the security posture for internal networks, encrypt all internal and external communication paths — everything from remote user connections to enterprise assets to applications and data stores regardless of location. Per the Office of Management and Budget's M-22-09 memorandum, US federal agencies must encrypt all DNS and HTTP traffic by the end of the 2024 fiscal year. Centralized SSL certificate lifecycle management solutions like those from DigiCert, Hashicorp, and Venafi automate the process of keeping SSL certificates up to date.
- **Use microsegmentation to apply fine-grained control to workload-level network traffic.** Many firms struggle to apply microsegmentation policies — and for good reason. A successful microsegmentation implementation depends on network infrastructure knowledge and requires integration with an identity provider. Identity providers supply workload identities, which are crucial to understanding and enforcing identity context in microsegmentation decisions that dictate how workloads can communicate with each other on the network. A US insurance firm deployed microsegmentation policies around each virtual compute instance (cloud-native hypervisor and container runtimes) to tightly control access and prevent lateral movement.
- **Treat virtual compute environments like remote offices.** Virtual compute environments like AWS EC2 instances and Azure Virtual Machines are accessible from the public internet by default. To protect these environments from hackers, treat them as isolated domains, similar to traffic in and out of remote sites. Apply the Zero Trust Edge model to each compute (hypervisor) instance individually and administer them as a cohesive environment in the form of SDNs, VNETs, and VPCs

that cover traffic to and from these compute (hypervisor) instances. Cloud infrastructure services' VNETs and VPCs implicitly deny network traffic by default — a great starting point for implementing Zero Trust.

Workload: Secure The Cloud Platform's Administrative Plane, Detect Unusual CPU Utilization

Hackers often exploit overprivileged compute hypervisors such as AWS EC2 instances, Azure Virtual Machines, and Google Compute Virtual Machines to access databases or hijack virtual machine (VM) resources for illicit cryptomining. To avoid this, regulate access to VM configuration at the cloud service provider's management console; carefully monitor VM firmware and boot configuration; and have deep visibility into VM resource (disk, network) allocation. You should:

- **Deploy trusted platform module encryption to protect in-memory data.** Hackers use malware to make unauthorized changes to CPU code and data in RAM. Trusted platform module (TPM) encryption like AWS Nitro and Intel's Software Guard Extensions and Trusted Domain Extensions protect against this. Each cloud infrastructure service provider offers native TPM encryption features for confidential computing. Cloud infrastructure service providers offer firmware integrity protection and signing. They also detect boot time anomalies, which occur when BIOS firmware is infected or hackers inject malicious kernel-level modules or device drivers into the boot sequence of the operating system (OS).
- **Detect excessive CPU and disk use to eliminate cryptomining.** Unauthorized cryptomining raises cloud operating costs and may disguise other hacking activity. An Asian public sector organization saw the CPU utilization of Azure VMs in production and other environments hit 80% in quiet periods like nights and weekends before it detected and cracked down on cryptomining. Cloud infrastructure services offer native hypervisor CPU, disk, and network activity monitoring that guest OS-level malware cannot turn off. Security pros also often use these capabilities to detect ransomware activity: Sustained high CPU and disk activity is a sure sign of unauthorized encryption on large data volumes.
- **Complement native Kubernetes security features with open source.** As a completely open container orchestration framework, Kubernetes (K8s) used to come without much security. Initial K8s security features, such as pod security policy for K8s container image admission control, proved too complex and were deprecated. In its place, the open policy agent OPA Gatekeeper is a promising open source project to help with container admission; it has been adopted by commercial container orchestrator security vendors such as Palo Alto Networks

and Red Hat. Multicluster K8s, a native infrastructure solution to improve availability and manageability, also offers single sign-on that allows a single treatment of users for authentication and role-based access control across multiple K8s clusters.

- **Mandate automatic instrumentation of cloud workloads.** Never create cloud workloads in any environment without proper monitoring, threat detection, and remediation instrumentation. This commonly means using build-out, continuous improvement/continuous delivery scripts like Ansible, Chef, Puppet, and Terraform to build out cloud infrastructure service environments, inject agent-based and agentless cloud workload protection solutions to protect workloads, and implement shift-left scanning in container registries.

People: Focus On Both Business And Admin Identity Management

Identity and access management (IAM) in the cloud has many facets: administrative user management for the cloud infrastructure service console, privileged identity management for workloads, and business user management. CSPM, SSPM, and cloud infrastructure entitlement management (CIEM) solutions solve many administrative user entitlement management problems in cloud infrastructure services and SaaS. You should:

- **Consolidate business user identity repositories.** Firms often use multiple user repositories to store human and machine user credentials and administrative and business user access rights in the cloud. They routinely mix on-premises Active Directory (AD) with user directories from identity-as-a-service solutions such as Azure AD, Okta, and Ping Identity. Storing different user populations in multiple repositories — for example, putting North American and European users in different AD forests — inevitably creates identity silos. Identity federation like SAML and Open ID Connect allows firms to provide cross-silo access — say, giving an administrator in Asia access to a North America-based workload — without duplicating identities. This tightens access rights controls, speeds threat remediation — in case of a compromise, you only have to reset a user's passwords or credentials in one place — and simplifies identity management and governance (IMG).
- **Perform identity attestation at least semiannually using the right tools.** A mix of users such as disgruntled employees, outsourcers, and users with no legitimate business need to access privileged and admin functions of cloud environments is a security disaster waiting to happen. While SSPM and CIEM solutions' vendors do plan to introduce full-scale reviews of attestation and access rights, this

functionality is missing from SaaS apps and cloud infrastructure services. We recommend using a traditional IMG solution to perform privileged user attestation at least semiannually and enforce separation of duties. Compliance mandates help justify the cost of IMG implementation. The SWIFT international payment network requires participants to conduct security attestation to reduce the threat surface — a serious motivator for financial institutions to implement IMG.

- **Use passwordless and multifactor authentication to consoles.** Phishing, network snooping, and cracking render password-only protection inadequate for all kinds of identities, especially privileged ones. At a minimum, mandate that all privileged human and machine identities use passwordless and multifactor authentication to access the cloud infrastructure service and SaaS consoles. Implement step-up authentication and just-in-time access policies; rigorously monitor all access and correlate it with actual human users or application instances. That enables you to track administrative account takeovers and unauthorized policy changes.

Devices: Steer Traffic To Proxies And Use Device Posture Management To Protect Data

Devices hold sensitive data. In the public cloud, where network controls such as VPNs are much less prevalent than on-premises or in private clouds, firms need to allow their workforce to securely access corporate applications and data from any device on any network without affecting user experiences. Applying Zero Trust to devices accessing cloud resources requires a three-pronged approach: inbound access security, device posture management, and device endpoint threat detection. You should:

- **Steer all inbound enterprise traffic to an access proxy.** Forcing all user traffic to traverse an inbound proxy enables single-point authentication, IAM-related self-service, traffic inspection, and inbound web threat detection and eliminates the need for a VPN concentrator. This architecture allows users to access corporate resources from any device that meets the firm's posture requirements. The access proxy can also perform device-based user authentication and authorization. These concepts are the architectural basis of Google's BeyondCorp proxy-based inbound access solution.
- **Use device posture management to detect and prevent on-device threats.** Because users can download sensitive corporate data to their desktop and mobile devices, you must ensure adequate protection for the data in these devices. Device-based data protection has two stages. First, it detects and protects the posture of workforce and customer devices to ensure that none are jailbroken or rooted or have malware or unencrypted storage. For the workforce, it uses unified

endpoint management solutions like Ivanti, Microsoft, and VMware to ensure that no one can steal corporate data from the device. Most enterprises that must protect business partner data mandate management of the devices of employees and even business partners.

- **Deploy agent-based threat detection to guard against malware.** Malware on a device may steal data and escalate process privileges, allowing hackers to use it for reconnaissance, lateral movement, and credential theft. An extended detection and response agent monitors a device's network traffic for anomalies; provides host-based network firewalls; checks for, quarantines, and eliminates malware on device storage and in device memory; and provides file integrity monitoring. Zero Trust Edge solutions such as cloud security gateways and firewalls integrate with these agents. Device-based agents of trusted network edge cloud security gateways, in concert with their egress forward or reverse proxy, enable the detection of shadow IT and anomalous data movement, interception to SaaS apps, and cloud data leak protection.

Visibility And Analytics: Control Configuration Drift At All Levels

Firms that can't see or analyze changes in the cloud can't implement effective Zero Trust there. Complicating the quest for visibility is that fact that cloud platform configurations are always in motion. New workloads are in a constant state of flux — creation, decommissioning, and frequent change — for cloud infrastructure services' hypervisors, storage, containers, and SaaS solutions. Configuration changes present significant challenges: Untested or overpermissive compute, storage, and network configurations expose data to hackers and threaten service availability and operational continuity. Zero Trust in the cloud is unimaginable without configuration management. Security pros should:

- **Use CSPM to protect cloud platform policies.** SaaS CSPM solutions from Lacework and Palo Alto Networks connect to the infrastructure service platform's policy management API and are part of a larger cloud workload security suite. While they typically connect in read-only mode, read/write mode is a must for automatic remediation. CSPM tools read and discover the infrastructure service platform's compute, storage, and network configuration; take a snapshot of a known good set of policies that offer sufficient security; and then poll the infrastructure services policy management API to detect drift (unauthorized changes) in infrastructure service policies. If CSPM tools detect drift, they notify security operations centers and raise help desk tickets for manual remediation. If the CSPM solution has read/write access to the cloud infrastructure services platform, it can automatically remediate and reset configurations.

- **Use CIEM to uncover hidden access paths between identities and resources.** CIEM (aka cloud identity governance) solutions from firms like Britive and Ermetic are great at painting a comprehensive picture of access rights resulting from the superposition of various policy types. On AWS, identity policies, access control lists, session policies, permission boundaries, resource policies, and service control policies all contribute to effective access rights between human and machine identities and resources like storage and network infrastructure. Zero Trust in the cloud requires that security pros fully understand and control these access rights to avoid inadvertent or unauthorized access to cloud compute, storage, and network resources.
- **Use SSPM to control SaaS configuration policies and admin access rights.** Each SaaS application has its own intricacies and access policies. Firms use at least 10 SaaS apps, and app policies are constantly evolving — so there's a storm brewing. SSPM tools work much like CSPM and CIEM tools, although they aim to manage not the infrastructure services platform but SaaS apps like Microsoft 365, Salesforce, and SAP. SSPM solutions are data-sensitive and understand ongoing patterns of data access in SaaS applications; they combine these with AI and machine learning policies to provide access risk scores and to detect and remediate SaaS configuration drift.
- **Use KSPM to detect misconfigurations.** Kubernetes has become an innovation platform: Its extensibility and adoption enables Audi to build easy-to-maintain applications on public clouds without provider lock-in. Kubernetes security posture management (KSPM) solutions from firms like Aqua Security and Sysdig allow firms to detect K8s pods that have excessive administrative access rights, lack multifactor administrator authentication, or lack image container admission control. KSPM solutions detect shortcomings and offer manual remediations like submitting a Jira or help desk ticket and automatic remediations such as changing K8s orchestration policy.

Automation And Orchestration: Guard Code And Design In Flexibility

Due to its scripted build-out and the large number of resources at all compute, storage, and network infrastructure levels, cloud is unsuitable for old-fashioned manual IT processes such as administration and security patching. Even the best visibility into cloud resources is useless if you can't proactively automate threat responses. To achieve Zero Trust in the cloud in automation and orchestration:

- **Guard the code used to build cloud environments with IaC scanning.** Infrastructure as code (IaC) platforms like Ansible, Jenkins, Puppet, and Terraform

allow DevOps and security pros to script the build-out and configuration of cloud platforms, container runtimes, and container orchestration infrastructure. IaC management and drift detection tools from Hashicorp, Snyk, and spacelift.io not only safeguard the build-out of traditional and containerized cloud environments but also automatically remediate drift.

- **Design in flexibility with orchestration.** AWS has always had an API-first design mandate, exposing its infrastructure formation and security policies via APIs. To varying degrees, this is also true for competing services such as Microsoft Azure and Google Cloud Platform (GCP). Orchestrator and IaC platforms call these APIs to build out cloud configurations. Public cloud providers' own tools permit orchestration: CloudFormation increasingly helps AWS users with AWS infrastructure build-out orchestration and multicloud orchestration tasks. Public cloud container platforms like Amazon Elastic Kubernetes Service and Google Kubernetes Engine also provide build-out automation and increasingly offer security checks.
- **Use identity orchestration to break authentication silos.** Representing and using identity information to authenticate and authorize users to large numbers of apps — both SaaS and apps built in house — requires identity orchestration. Identity orchestration programmatically defines the flow of and exposes APIs and SDKs to call business apps to implement joiner, mover, and leaver processes; perform authentication and session management; implement coarse-grained user authorization in applications; and provide user self-service such as forgotten credential recovery. BMW uses identity orchestration on the ForgeRock platform to implement its hybrid cloud IAM strategy.

Supplemental Material

Companies We Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Broadcom

Check Point

Illumio

Lacework

Palo Alto Networks

Rapid7

Sentinel One

Sophos

Sysdig

FORRESTER®

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

FOLLOW FORRESTER

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com