TCGi
TECHNOLOGY CONCEPTS GROUP INTERNATIONAL

CLOUDKNOX

Solution Brief

Combat the Expanding Threat Surface of Hybrid Cloud Infrastructure

The #1 risk to your hybrid infrastructure is a trusted identity with **excessive privileges**. When critical workloads can be deleted with a keystroke, **understanding and managing privileges for all identities across your clouds is critical.**

Cloud infrastructure has seen unprecedented and accelerating levels of automation over the past few years. This automation has given enterprises the ability to reach new heights in efficiency and scale. However, this newfound capacity comes with a price: increased risk of accidents, insider threats and compromised credentials"

In today's dynamic IT environment, one keystroke can create a data center or take it down in seconds. This is what happened to AWS in 2017 whereby one incorrect command knocked their S3 service offline, taking dozens of websites and applications offline, impacting hundreds of thousands of businesses and causing millions of dollars in lost revenue.

As organizations start embracing multiple cloud platforms – the probability of an incident such as the one AWS experienced is going to increase exponentially.

So, what can you do to protect your business from these types of risks?

Applying the Principal of Least Privilege (POLP) Across Clouds

At its core, POLP is about ensuring that every single identity that can touch your infrastructure only has the privileges necessary to perform its day-to-day job. Implementing the POLP is the number one security policy that every security organization must enforce in order to minimize risk. If you are not operating under least privilege you are running the risk of compromising every other security system, policy, and procedure in place.

While the concept of least privilege is simple to understand, it can be very complex to effectively implement. Consider some of the complicating variables:

- Diverse computing environments (e.g. virtual, private cloud, hybrid cloud, multi-cloud)
- Different types of workloads (e.g. servers, virtual machines, containers, serverless, etc.)
- Variety of services (compute, storage, networking etc.)
- Unique flavors of identities (e.g. employee, third party, bot, service account, API keys, resource, role, group)
- Number of privileges that increase daily across all cloud platforms

Know your organization's **risk profile** with a single metric based on your identities' **activities**.

Gain insights into your **identities'**, their **privileges**, **actions**, and **resources** impacted.

Apply **just enough** privileges (e.g. revoke high-risk privileges) **based on what your identities' need** to perform their jobs.

Current Model: Role-Based Access Controls (RBAC)

Implementing a solution that leverages RBAC will not work if you are trying to achieve the principal of least privilege. With RBAC, your identities belong to a static role (e.g. system administrator) and that role comes with a broad pre-determined set of privileges that will never completely be used by an identity.

The rigid nature of RBAC leads to a dangerous scenario in which identities acquire many more privileges than they actually need or use. The over-provisioning of identity privileges becomes even more serious in the cloud as the number of available actions that automate tasks exponentially grows.

For example – let's assume that Bob and Fred have been assigned a system administrator role which is tied to the enterprise's Active Directory. This role by default gives them the ability to perform thousands of tasks, 50% of which are high-risk, but Bob only uses 20 privileges in his day-to-day job and Fred only uses 10 different privileges to perform his day-to-day job.

Both Bob and Fred are over-privileged identities. They carry an unnecessary risk because they were both given a broader set of privileges intrinsic to the static role assigned to them.

Most trusted identities like Bob and Fred use less than 1% of their privileges to perform their day-to-day jobs. The other 99% of unused privileges represents avoidable exposure to risk from accidents, insider threats and compromised credentials. Any misuse of a high-risk privilege, accidental or malicious, can cause service degradation, service disruption, data leakage or a complete shutdown of your business. Moreover, a variety of non-human identities like service accounts; API keys, bots, applications, etc., exacerbate this risk.

Gain Access to a Unique Set of Capabilities

We deliver a single platform to implement Activity-based authorization across any private or public cloud infrastructure. The unique model offers a non-intrusive way to manage the entire identity privilege life cycle based on actual activity while avoiding any impact to productivity or trust.

Monitor and Measure Continuously

The platform continuously monitors the activity and behavior of all identities and provides a single metric, the Risk Score, to track the risk associated with each identity. This score is a function of unused high-risk privileges by each identity. An identity with many unused high-risk privileges will have a high-risk score.

Once you discover your risk score you can take action to reduce it. **Ensure that your risk remains low with our risk monitoring capability** which collects the privileges and activity details of all unique identities and updates the risk score continuously.

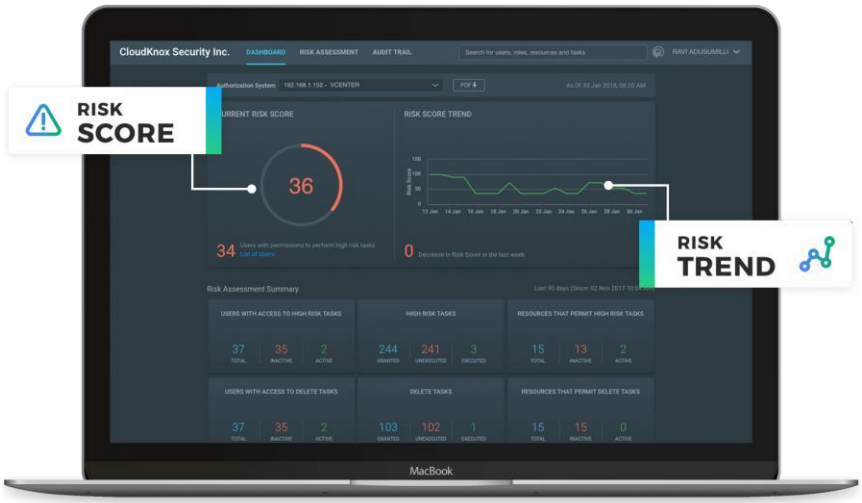
TCGi
TECHNOLOGY CONCEPTS GROUP INTERNATIONAL

CLOUDKNOX

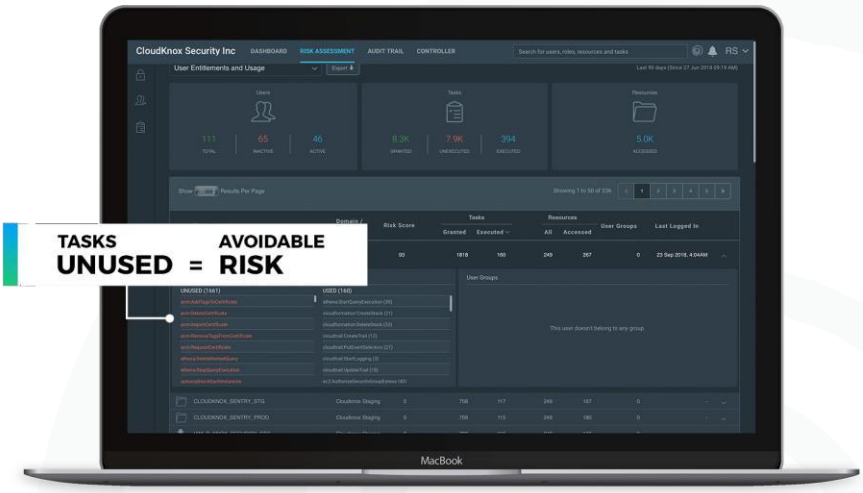
Solution Brief

Key Capabilities

- **Immediate visibility and insight** into identities, privileges, actions and resources across your cloud infrastructure
- **Activity-based authorization** for any identity that touches your infrastructure including service accounts, API keys, bots, third parties or employees
- **JEP (Just Enough Privileges) Controller** to automatically right size over-provisioned identity privileges and prevent privilege creep
- **Anomaly detection and identity activity analytics** across private and public cloud infrastructure
- **Forensic-quality activity data** for easy compliance reporting and a powerful query interface to investigate issues



Activity monitoring and proper accounting and attribution gives you granular insights into the privileges and activity that each identity is using or not using. With this level of visibility and insight, it becomes possible to accurately grant or revoke privileges for each identity with access to your infrastructure.



Activity-Based Authorization with the Click of a Button
JEP (Just Enough Privileges) Controller gives you the ability to automate and simplify the management of identity privileges across any of your private and public cloud platforms with the click of a button. It enables you to implement measures to improve your security posture against accidents, insider threats and compromised credentials without writing any scripts or understanding the different authorization models across those different clouds.

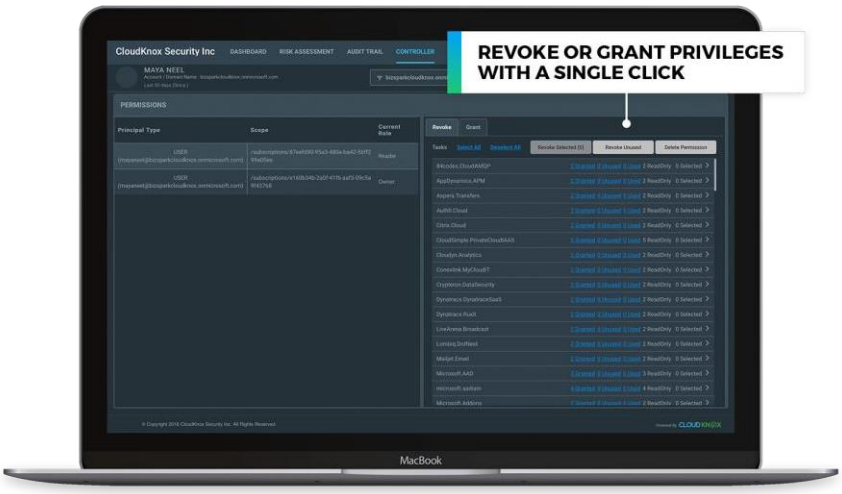
Proprietary JEP (Just Enough Privileges) Controller gives you the **ability to reduce your risk profile by revoking the unused high-risk privileges** for each identity with the click of a button across anycloud.

TCGi
TECHNOLOGY CONCEPTS GROUP INTERNATIONAL

CLOUDKNOX

Solution Brief

JEP Controller allows you to automate and simplify the management of identity privileges across any cloud platform**with the click of a button**.



Audit Trail, Reporting and Forensics
Creating or editing a report can be done with a few clicks through an intuitive dashboard without any scripting knowledge. Reports can be scheduled to run and distributed via email on a daily, weekly, monthly or custom basis and can be exported to .CSV or .PDF files.

Out-of-the-box, fully customizable reports, based on audit-quality logs, **make it easy to demonstrate compliance** to your auditors at any point in time.

How Does It Work

The platform is comprised of two components: FortSentry and Sentry Virtual Appliance.

FortSentry is a multi-tenant SaaS service hosted in the cloud. It is the central portal where it is administered.

Sentry Virtual Appliance is a Linux virtual machine with all the necessary software components pre-installed. It collects the privileges and activity data of any identity that can touch your infrastructure. Sentry uploads this data to the FortSentry system for ML algorithms to generate the necessary analytics. One Sentry is deployed for each platform (VMware vSphere, AWS, Azure, GCP etc.).

INSTALL VIRTUAL APPLIANCE	DATA COLLECTION	OPERATIONAL
< 30 mins	< 24 hrs	< 1 day

Solution Brief

With less than 30-minutes to install, organizations can operationalize the Cloud Security Platform **in less than a day**.

The FortSentry Cloud Security Platform helps enterprises **manage the entire identity privilege lifecycle** across any private and public cloud infrastructure.

About FortSentry Cloud Security

FortSentry Cloud Security is the only Cloud Security Platform built from the ground-up to support a hybrid-cloud environment. Through a single platform, its Identity Authorization Administration model helps enterprises manage the entire identity privilege lifecycle across any private and public cloud, thus enabling organizations to significantly reduce their risk against compromised credentials, accidents and insider threats and achieve the principle of least privilege.

TCGi is an asset management and procurement solutions provider, enabling corporations to increase the value of their spend and better achieve their strategic goals.

We also provide comprehensive cutting-edge cloud, security and network solutions through our distributor partners.

As a value-added reseller (VAR), TCGi has forged strategic alliances with key OEM partners in order to afford our customers the highest quality IT products.

Our software focus is to provide state-of-the-art cyber security architecture and solutions with enterprise-to-cloud protection.

Technology Concepts Group Intl (TCGi)

Authorized Reseller

285 Davidson Ave, Suite 501
Somerset, NJ 08873
732-659-6035
info@technologyconcepts.com
www.technologyconcepts.com