ANOMALIX

idGenius Crucial Cloud

Total Public Cloud Protect

idGenius Crucial Cloud empowers you to manage identity and access in your extended cloud environment

PRODUCT DESCRIPTION

idGenius Crucial Cloud is a full-stack cloud protection platform that holistically secures your cloud assets. The cloud-native SaaS platform uses AI and machine learning to identify, correlate, monitor, and audit security and compliance activity across public cloud environments. Crucial Cloud helps enterprises reduce financial risk and costs resulting from security breaches and non-compliance.

KEY CHALLENGES IN SECURING THE CLOUD

Public cloud environments are subject to attacks on a daily basis. Microsoft alone detects a concerning, 1.5 million attacks per day targeting its Azure public cloud platform. The inherently dynamic nature of public cloud platforms presents high risk and costly challenges:

- The native security tools from cloud providers don't cater to enterprise security needs.
- Breaches can go undetected for months in complex cloud environments.
- Cloud migration reduces visibility, making access management more challenging.
- The cloud thins the line between security, DevOps, and resource boundaries.
- Nearly 70 percent of cloud security breaches are due to resource misconfiguration.
- New threat actors and malware are becoming more sophisticated.

Crucial Cloud's full-stack protection provides the guardrails to protect against cloud security challenges.

KEY PRODUCT HIGHLIGHTS

Manage identity and access to improve visibility

Most organizations struggle to create a holistic view of user access permissions and resource inventories in public clouds where IDs, accounts, policies, roles, and groups come from multiple, disparate sources.

Crucial Cloud protects the identity of consumers, employees, and that of accounts associated with applications, services, and connected assets across heterogeneous identity sources. The platform manages access to cloud resources such as:

- Servers, serverless apps, and containers (VMs, AWS IAM, EC2, S3 buckets, Lambda, RDS, Aurora)
- LDAP/Active Directory accounts and groups
- Customer defined applications and data

Not all access is equal. The identity and access control tools from cloud providers lack policies to map the minimum set of privileges to corresponding job responsibilities.
Crucial Cloud helps you detect high-value, high-risk resources, and accounts for managing role-based least-privilege access to these resources.

Resource configuration monitoring detects threats early

A Cloud Security Alliance (CSA) report cites misconfiguration and inadequate change controls as a top cloud security threat. In 2018-19, hackers exploited misconfigured S3 buckets most commonly to expose sensitive data that they either stole, leaked, or held as a hostage against a ransom. Crucial Cloud's smart monitoring proactively identifies misconfigurations. The platform creates an inventory of all resources in your AWS/Azure/GCP environment, such as – cloud accounts, VMs, AWS EC2, and S3 buckets, serverless and container-based resources, unused and underused resources. Crucial Cloud resource configuration monitoring features:

- Flag misconfigurations of cloud resources
- Instantly evaluate current configuration with best practices
- Identify dedicated connections, AWS VPC configurations, and public IPs that are accessing your resources
- Check port level configurations, for example, SSH exposure to the public internet
- Identify the ways to get access to your cloud resources
- Identify any direct account permission mapping to resources
- Check all security policies, IAM roles, and groups that have access to resources
- Check all active directory groups and accounts that have permission to cloud resources
- Limit root/admin accounts

Network security monitoring limits resource exposure

Misconfigured network ports aid malicious account access and data exfiltration. Crypto-jacking is another fallout of network exposure where hackers mine CPU-intensive cryptocurrency and blockchain algorithms by compromising your cloud servers.

Network security logging and monitoring are imperative as this provides visibility to unauthorized access attempts, access/permission usage, API call information, and configuration deployment events. Crucial Cloud creates a holistic view of who and what your resources communicate with. The platform helps you to:

- Identify/monitor all internal and external network activity
- Monitor for whitelist/blacklist IPs
- Monitor for new IP and Port connections
- Monitor for lateral movement across containers
- Determine who has access to what resources
- Manage outbound traffic, limit SSH connections

Crucial Cloud's network monitoring detects anomalies like unauthorized access and suspicious activities to thwart threats before they inflict any damage.

Compliance reporting minimizes compliance costs

Compliance is a business imperative. Violations have costly consequences that impact your market presence.

Crucial Cloud's continuous learning and monitoring provide organizations with a holistic view of their compliance posture in real-time. Crucial Cloud's compliance reporting helps you to:

- Identify all relevant standards (PCI, GDPR, HIPAA, NIST, SOC2, etc.)
- Identify compliance violations by standard
- Report the resources and activities being monitored, such as VMS, EC2, S3, Lamda, RDS, Aurora, etc., serverless apps and containers, network traffic
- Indicate overall security and compliance specific posture in a single report
- Break down best practice violations by resource or incident
- Recommend fixes by standards/best practices

Crucial Cloud automates compliance, monitors compliance in real-time, and reduces the cost of compliance for organizations.

KEY PRODUCT FEATURES

- **Visibility and inventory of cloud assets and resource utilization**
- **Identify "Who Has Access To What" across ALL cloud resources**
- **Identify and remediate high risk and inappropriate cloud access**
- **Identify and remediate inappropriate asset configurations**
- **Identify and remediate anomalous and suspicious network activity**
- **Continuous learning for security and compliance-related behavior**

THE UNIQUE POWER OF idGenius CRUCIAL CLOUD

idGenius Crucial Cloud overcomes the limitations of traditional tools and “point solutions” for cloud security. As a cloud-native full-stack solution, Crucial Cloud provides enterprises with deep visibility, cloud access management, network security governance, and compliance assurance across public clouds, including Amazon Web Services, Microsoft Azure, and Google Cloud Platform:

Reduced financial risk due to security breaches

Reduced cost of compliance reporting

Reduced security operations associated with manual and redundant activity

Reduced time and resources related to meeting compliance mandates such as KYC/AML, NIST, PCI, SOC 2, HIPAA, GDPR, CCPA

ABOUT ANOMALIX

Anomalix is a Gartner-recognized solutions and services company for Identity and Access Management. Anomalix leverages machine learning and AI to create cloud security solutions that allow organizations to establish an omnichannel view of identity and access information that improves sales and marketing campaigns, enhances cloud security administration, and simplifies governance compliance and reporting.

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144

ANOMALIX