ditno.

ditno AWS API Integration

ditno unifies network governance across your Amazon Web Services (AWS) environment with AWS API Integration, ensuring consistent security governance across your hybrid, on-premises and cloud environments.

Protecting your digital transformation across hybrid environments

Your digital transformation is set to deliver agility and cost savings. However, as you move your workloads, apps, and data from on-premises to the cloud, your security controls won't necessarily align. This could change your risk posture and make your company vulnerable to cyber attacks. Protecting your business and your customers means you must protect your digital transformation across the cloud and on-premises.

Many organisations mistakenly believe that the cloud provider is solely responsible for security when, in fact, AWS mandates a shared responsibility model where the customer is responsible for managing data and assets, and applying appropriate access permissions.

ditno AWS API Integration lets you migrate from on-premises to AWS with native security while maintaining the same network governance and risk posture. It applies the same compliant security controls across your environment both on-premises and in the cloud. This approach lets you audit your security groups from a centralised management portal and move from an agent-based model to agentless.

AWS helps you build secure, high-performing, resilient and efficient infrastructure for your applications. ditno helps define key strategic governance policies to ensure the IT services are not exposed. This includes the ability to discover all security group rules and misconfiguration, and detect any current exposure and remediate it with real-time network governance.

You can onboard an AWS account within minutes to start your assessment.

Key benefits

- **Discover IT service relationships to understand the impact of changes**
- **Classify and govern network access in real time to strengthen security**
- **Define compliant application profiles and apply these across the network**
- **Ensure micro-segmentation to prevent unauthorised lateral movement within the network**
- **Assess individual workloads for security gaps**
- **Maintain consistent trust across hybrid environments during and after migration and transformation activities to protect your digital assets**
- **Visualise security group connectivity**
- **Automatically audit security group configuration to eliminate manual work and ensure consistent compliance**

Key Capabilities

ONBOARD AWS ACCOUNTS WITHIN MINUTES

With ditno AWS API Integration, you can easily onboard AWS accounts and start assessing security group controls within minutes. This lets you visualise application dependencies and highlight superfluous network controls so you can ensure micro-segmented network controls are implemented correctly.

REAL-TIME NETWORK GOVERNANCE

Rather than manually auditing network security controls, ditno automates this process with an always-on audit that aligns to your risk profile. This also means critical services are protected from exposure by ensuring appropriate access. ditno delivers consistent governance models across diverse workloads including Infrastructure-as-a-Service, Platform-as-a-Service, and microservices. Real-time network governance also ensures effective and efficient use of network security to ensure an organisation is deploying IT services securely (DevOps). This helps improve IT service exposures in a measurable and cost-effective way.

UNDERSTAND CURRENT EXPOSURE

Network governance models help identify risk and assist with regulatory requirements. ditno's solution assesses your network's current state and easily identifies non-compliant network configuration and exposure. This lets you prioritise security initiatives correctly, separating duties between risk and security operations. You can confidently report on the entire organisation's network exposure, then take appropriate risk mitigation steps.

ENSURE SECURITY IN THE CLOUD

As you move to the cloud, it's essential to use consistent security governance that lets you securely migrate services from on-premises to AWS. Transforming services securely means re-architecting from traditional servers to containers or microservices without adding network exposure. ditno AWS API Integration complements DevOps by ensuring automation is performed securely and by identifying non-compliant rules so DevOps can rectify any issues on the next deployment. This helps reduce the number of exploitable IT services and prevents attacks from moving freely throughout the network. This gives you the ongoing assurance of a micro-segmented network fully controlled and governed throughout your AWS accounts.

To find out more about how ditno AWS API Integration can help your business maintain consistent network security governance across on-premises and cloud networks, contact the team today.

About ditno

Developed by experienced network security engineers, ditno's cybersecurity software helps you to better manage and mitigate cyber risk. The ditno platform gives you more visibility and control over your network, ensuring your network controls align with your cybersecurity governance policies. The result is more comprehensive network control and a stronger cybersecurity posture that will give you the confidence to operate with greater agility.

ditno.com
(02) 8011 4860
info@ditno.com

ditno.