Accenture Secure Cloud Express, powered by Palo Alto Networks

Kick-start your cloud security

Find and remediate cloud misconfigurations and shadow IT quickly

As enterprises continue to push to the cloud for speed and agility, many struggle with a lack of visibility into common cloud vulnerabilities that hackers are actively exploiting.

For example, all it takes is a credit card swipe for a development team to spin up a new cloud presence outside of organizational controls. Recent studies show that more than 60 percent of cloud apps are shadow IT operations that are running undetected.[1]

Meanwhile, misconfigured workloads are exposing sensitive data and apps to bad actors. Gartner Inc. predicts that by 2025, more than 99 percent of cloud breaches will be traced back to preventable misconfigurations or other mistakes.[2] In addition, The National Security Agency states, "Misconfiguration of cloud resources remains the most prevalent cloud vulnerability." [3]

Discover hidden vulnerabilities

Organizations can now get the visibility needed to uncover hidden vulnerabilities with Secure Cloud Express from Accenture. Using a diagnostic approach to find vulnerabilities and a prescriptive approach to remediation, Secure Cloud Express enables organizations to have a comprehensive understanding of their security posture in as little as one week.

Accenture partnered with Palo Alto Networks for the industry's leading visibility tools, including Prisma Cloud, which gives organizations visibility into what's running in the cloud to help them identify shadow IT workloads. Accenture combined that with Palo Alto Networks' Xpanse Cortex, which gives organizations the hacker's view of their cloud configurations, showing exactly where hackers can make their uninvited entrance.

At-a-glance

- Common risks like misconfigurations and shadow IT increase vulnerability to attack.
- By improving visibility into cloud resources and workloads, organizations can better understand their security posture.
- Accenture Secure Cloud Express provides the visibility to identify misconfigurations and shadow IT processes, and provide the tools and resources to quickly remediate vulnerabilities.
- Accenture Secure Cloud Express also accelerates the shift to DevSecOps, which will provide better security early in the development process.
- Within one week, Accenture Secure Cloud Express can provide visibility, recommendations, and a roadmap to remediation.

> **" "**
> Misconfiguration of cloud resources remains the
> most prevalent cloud vulnerability.
>
> - The National Security Agency[3]

A fast, 3-step process to better security

Secure Cloud Express is a unique blend of cloud security controls, deep industry knowledge, and the features of Prisma Cloud and Xpanse. The service is delivered in three easy and time-saving steps.

1. Rapid Requirements Baseline

Accenture works with you to develop baseline requirements based on your cybersecurity priorities across any combination of AWS, Azure, and Google Cloud. Accenture also incorporates regulatory and industry-specific security frameworks that are important to your business.

2. Rapid Fitness Appraisal

Accenture non-intrusively connects with your cloud provider accounts to create an inventory of resources and an evaluation of the security configurations of those resources. Suspected shadow IT accounts and potential public security risks are identified. The result is a diagnosis of your cloud security posture.

3. Rapid Prescription

Accenture provides practical tactical remediation advice by connecting the dots between the issues surfaced in the appraisal and the best approaches to addressing them. The result is a series of recommendations and a roadmap for risk mitigation and DevSecOps, tailored to your specific needs.

Benefits realized by customers:

• A large global manufacturing services company that recently utilized Secure Cloud Express found the automation capabilities enabled by Prisma Cloud significantly simplified the process for detecting cloud resource misconfigurations and reduced cycle time as well as risk of human error. Xpanse uncovered perimeter security blind spots for the leadership team allowing them to identify unsanctioned accounts across GCP, Alibaba, and other providers.

• By deploying Secure Cloud Express at a key hospital network in the United States, several high-risk findings were pinpointed & shared with the client along with the risk impact on the business. After recommendations were provided with a realistic roadmap for remediation, the client was able to easily prioritize their findings and engage in appropriate remediation activities.

Contact your Accenture or Palo Alto Networks representative today to learn how Secure Cloud Express can improve your security posture. You can also visit our website:

Learn more

Sources:
1. https://bit.ly/3NuD0WW
2. https://bit.ly/3NvrxX5
3. https://bit.ly/35lVNT9
4. https://bit.ly/3NuWieI
5. https://accntu.re/3iNfVAt