Cloud Infrastructure Resilience: CloudIBN's VAPT Services for US Data Centres

CloudIBN boosts cloud infrastructure resilience for US data centers with expert VAPT services, ensuring robust threat protection.

MAIMI, FL, UNITED STATES, June 27, 2025 /EINPresswire.com/ -- With US businesses increasingly reliant on cloud-based systems and data centres to deliver critical services, the resilience of their cloud infrastructure is more vital than ever. CloudIBN, a recognised leader in cybersecurity, is proud to launch its specialized Cloud Infrastructure Vulnerability Assessment and Penetration Testing (VA&PT) Services, designed to help US organizations detect and eliminate infrastructure-level risks before attackers can exploit them.

CloudIBN - VAPT Services

Through expert-driven VAPT Services, CloudIBN enables enterprises to harden their cloud environments, ensuring business continuity, regulatory compliance, and defence against escalating cyber threats.

The Strategic Importance of Cloud Infrastructure Resilience
Modern digital businesses rely on complex infrastructure stacks hosted in public, private, and hybrid cloud environments. While cloud platforms offer flexibility and scalability, they also create potential entry points for threat actors due to:
1. Improper configuration of compute, storage, and network services
2. Unpatched virtual machines and container vulnerabilities
3. Weak IAM policies and over-privileged roles
4. API exposure and security mismanagement
5. Lack of continuous monitoring across dynamic workloads

What Is Cloud Infrastructure VA&PT?
Cloud Infrastructure Vulnerability Assessment and Penetration Testing (VA&PT) is a specialized service that simulates real-world attacks to evaluate the resilience of your cloud systems, services, and supporting components.
1. CloudIBN's VAPT Security Services for cloud infrastructure focus on:
2. Infrastructure-as-a-Service (IaaS) Security Testing – Scanning virtual machines, VPCs, firewalls, and IAM roles.
3. Container & Kubernetes Security – Detecting vulnerabilities in Docker images, misconfigured clusters, and API access.
4. Storage & Database Exposure – Identifying misconfigured cloud storage and exposed databases.
5. Privilege Escalation Testing – Assessing IAM configurations and role chaining risks.
6. Penetration Testing & Exploitation – Manual testing to uncover complex, business-impacting vulnerabilities.
7. Cloud Compliance Assessment – Evaluating infrastructure against NIST, PCI DSS, ISO 27001, HIPAA, and more.

Want to test the resilience of your cloud infrastructure?
Schedule your infrastructure VAPT consultation today: https://www.cloudibn.com/contact/

CloudIBN's Comprehensive Cloud Infrastructure VAPT Methodology
1. Asset Discovery & Scoping
Inventory of cloud workloads, services, and exposure points.
2. Infrastructure Configuration Review
Analysis of firewall rules, network segmentation, storage permissions, and encryption status.
3. Automated Vulnerability Scanning
Using best-in-class tools (e.g., Nessus, Qualys) to identify known weaknesses.
4. Manual Penetration Testing
Simulated attacks to test infrastructure resilience under real-world threat scenarios.
5. Risk Assessment & Prioritisation
Mapping vulnerabilities to business impact using CVSS and threat intelligence.
6. Reporting & Remediation Roadmap
Detailed findings with practical remediation advice and post-fix retesting.

Why CloudIBN Is the Go-To Choice for Cloud Infrastructure VAPT in the US
1. Cloud-Native Expertise: Extensive experience with AWS, Azure, Google Cloud, and hybrid setups.
2. Certified Security Team: OSCP, CISSP, and AWS Security-certified professionals.
3. Compliance-Focused: VAPT designed to support regulatory and audit requirements.
4. Real-World Testing: Go beyond scanning with simulated attacks tailored to your environment.

5. Actionable Reporting: Clear, prioritized remediation steps to strengthen defenses.

Stop guessing—know your cloud infrastructure's real vulnerabilities. Get in touch with us now: https://www.cloudibn.com/lp/pr-vapt-services-in-usa/

Threat Landscape: Cloud Infrastructure Under Siege
1. Cloud ransomware campaigns now target misconfigured services and backups.
2. Container escape attacks are on the rise in Kubernetes environments.
3. Serverless functions can be abused when proper role boundaries are missing.
4. Credential theft through poorly protected secrets and API keys is increasingly common.
A single oversight in infrastructure setup can result in a breach, downtime, or costly regulatory penalties.

Build a Resilient Cloud Infrastructure with CloudIBN
The future of business is in the cloud—but only secure and resilient cloud infrastructure will thrive. CloudIBN's Cloud Infrastructure VAPT Audit Services deliver visibility, insights, and expert remediation guidance US businesses need to secure their environments, achieve compliance, and stay competitive. Make your cloud infrastructure a security strength—not a liability.

Related Services : Cybersecurity Services - https://www.cloudibn.com/cybersecurity-services/

About CloudIBN
Founded in 1999, CloudIBN is an ISO 27001:2013, ISO 9001:2015 certified IT and Cybersecurity services provider. As a Microsoft Cloud Managed Services Partner, IBN specialises in VAPT, SIEM-SOAR consulting and deployment, cloud security, and compliance consulting. With a team of experienced lead auditors and cybersecurity specialists, IBN is committed to securing digital infrastructures worldwide

Surendra Bairagi
Cloud IBN
+1 2815440740
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X

in today's world. Please see our Editorial Guidelines for more information.