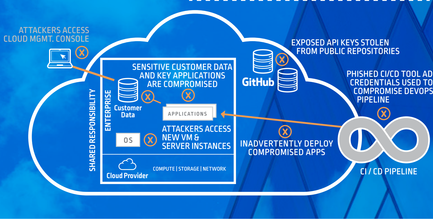
6 Security Checkpoints to Consider Along Your Organization's Cloud Journey

Whether you're on a journey to a public, private or hybrid cloud environment, relying on DevOps or leveraging SaaS applications, understanding cloud computing vulnerabilities is critical.

According to Microsoft, attacks on cloud-based accounts increased **300%** in 2017.[1]

Examples of Cloud Vulnerabilities That Expand the Cyber Attack Surface



The First Step of Protection Is to Know Your Specific Risks

Discovery tools can help you locate all cloud assets and uncover potential privileged accounts, access keys and other credential used throughout your enterprise's cloud environment.

Key Risk-Identification Actions

- **Discover all cloud and hybrid assets,** including privileged accounts, access keys, storage, and compute instances
- **Determine and assess risks and vulnerabilities** in cloud workloads and environments
- **Prioritize the highest risks** and focus on those first

According to Gartner
Through 2020, more than half of security failures associated with IaaS and PaaS will be attributable to significant security gaps caused by *failure to adopt Privileged Access Management* technology and processes.[2]

Cloud Vulnerabilities & Steps for Securing Them

1 The Management Console

- Apply privileged account protection practices to both human and script access
- Secure root account credentials in digital vaults
- Use multi-factor authentication
- Ensure API and automated access, scripts, etc. are secure
- Monitor active privileged sessions in real-time

2 The Organization's Cloud Infrastructure

- Secure privileged credentials associated with newly provisioned infrastructure
- Automate new server instance provisioning
- Use the principles of least privilege management
- Remove privileges when infrastructure is de-provisioned

3 API Access Keys

- Remove embedded API keys and secrets from scripts, automation tools, etc.
- Never provide human users direct access to API keys
- Secure all API keys in a secure digital vault
- Automate access to the digital vault to ensure the secure use of API access keys

4 DevOps Pipeline Admin Consoles and Tools

- Secure access to all tool admin accounts and consoles
- Rotate, monitor and record human and automated user actions
- Apply consistent security policies enterprise-wide to govern who/what uses and configures tools
- Perform audits to improve the organization's security posture

5 DevOps Pipeline Code

- Remove all secrets, keys & credentials from source code, configuration management, etc.
- Centralize access in a secure digital vault
- Monitor, control and rotate credentials according to enterprise security policies
- Automatically secure credentials when new instances are created
- Include security at the start of the dev process—don't retrofit as new code is going into production
- Audit everything to continually learn and improve

6 Admin Accounts for SaaS Applications

- Apply all principles of privileged access to SaaS application admin accounts
- Leverage AD groups for application provisioning /de-provisioning so access is automatically removed when employees leave
- Use session monitoring and recording for sensitive business applications such as payroll systems

Discover how CyberArk can assist you on your cloud journey—from securing your initial project to fully embracing the cloud and DevOps.

Visit http://www.cyberark.com/cloud *to download a copy of the ebook, 6 Key Use Cases for Securing Your Organization's Cloud Workloads or request additional information online.*

[1] Microsoft Security and Intelligence Report, 2017
[2] Gartner "Market Guide for Privileged Access Management" by Felix Gaehtgens, Anmol Singh, Dale Gardner, August 22, 2017

CYBERARK®