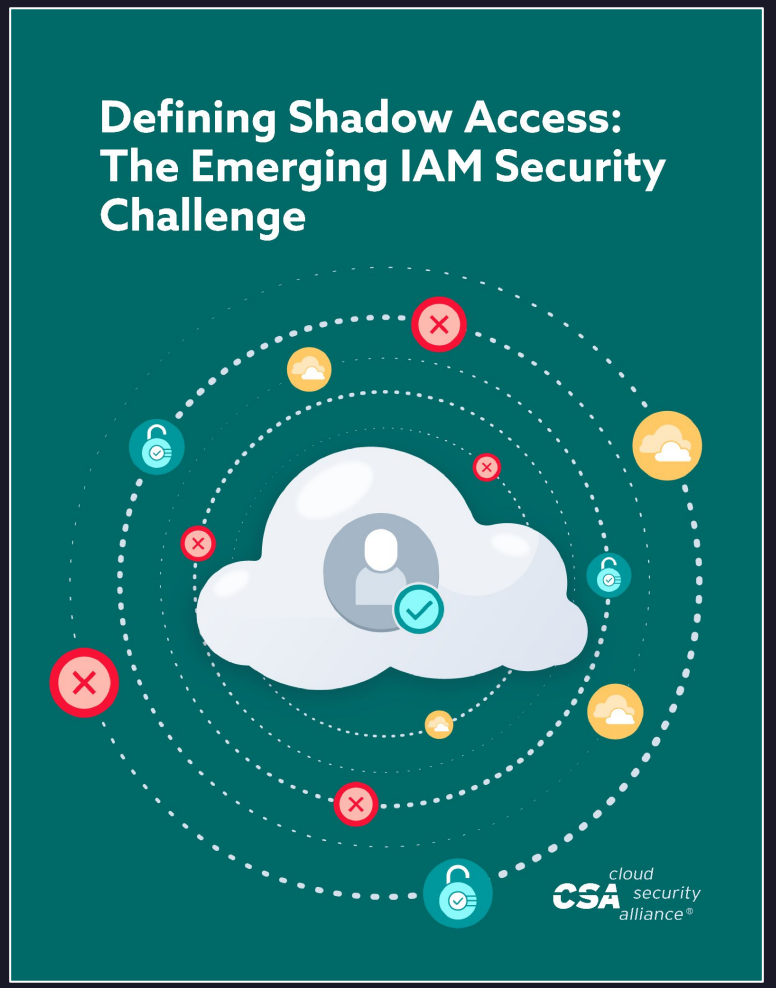
cloud security alliance®

Defining Shadow Access

The Emerging IAM Security Challenge

Release Date: 09/13/2023



IAM Working Group: Shadow Access Subgroup

Agenda

1. Shadow Access
2. Background
3. Causes
4. Impact
5. Conclusion
6. Acknowledgements

Shadow Access

- Shadow Access is the unintended and/or undesired access to resources, such as applications, networks and data.
- Shadow Access is increasingly a cloud issue, resulting from increased use of access and entitlements that connect cloud services together, coupled with automated infrastructure and software development, resulting in incorrectly or unexpectedly permissioned accounts and resources.
- The consequences of Shadow Access are potentially catastrophic and threaten to impact any organization that has an evolving cloud.
- This short presentation intends to summarize the background, causes, impact and path forward to regain the benefits of a dynamic and secure cloud environment.

Background

- Traditional Enterprise IAM (Identity and Access Management) systems have been deployed for decades, and are often built on popular services or protocols like LDAP and Active Directory.
- Many enterprises today operate Enterprise IAM (for on-premises hosted applications) in conjunction with or in tandem with a popular Cloud IDP like Okta, Azure AD, or Ping Identity.
- Cloud IAM is used to provision and control access and entitlements to resources, applications and data, residing inside public cloud ecosystems like AWS, Google Cloud, and Azure Cloud, as well as private clouds powered by Kubernetes.
- While similar at first glance, in reality, the concept is substantially different, and for that reason, we need to separately classify and examine these Cloud Identities.

Background Continued

- How are Cloud Identities different?
    - Everything you spin up in the Cloud has an identity with access to a critical cloud service, supply chain or data.
    - Inside the Cloud, every access requested is authenticated and authorized by before access is granted.
    - Cloud Identities can be human or non-human identities. Human identities are mostly end-users, Developers, DevOps, and Cloud Administrators. Non-Human Identities are the majority rest, composed of identities attached to Cloud Services, APIs, microservices, software supply chains, cloud data platforms, etc.
    - Modern cloud applications are really an assembly of many distributed services, driven from APIs, across providers and their ecosystem. As developers combine cloud services, these services create automated identities with access pathways to data.
- Cloud computing has created an identity-centric world and the differences surrounding them lead to the root causes of Shadow Access.

Causes

- The root causes of Shadow Access stem not just from having Cloud Identities, but also from the fundamental Complexity and Processes driven by the cloud.
- Complexity:
    - Data is no longer stored in a single data store.
    - Data stores are constantly evolving, expanding or contracting, new types appear with new or updated use by applications.
    - An application is not monolithic, but a dizzying combination of interconnected identity systems, cloud services and data.
    - The vast increase in the use of SaaS applications that connect with Cloud ecosystems.
    - Each cloud service has associated permissions and entitlements that give it authorization to sensitive data and operations.
    - The scale of permissions and entitlements are wildly more expansive and several orders of magnitude more complex compared to conventional on-prem environments.
    - Organizations use multi-cloud and a combination of public/private cloud environments.

Causes Continued

- Process Changes:
  - New identities and access are created centrally, often by the developers of those applications, using infrastructure-as-code.
  - The profile of a new identity is usually copied from a template that (at least at some time) hopefully had some central review for organizational standards.
  - New identities and access are being automatically created with little to no governance.
  - The applications that the identities access are constantly changing, without full system access reviews of the identities' access.
  - Application components are often re-used, copied, or used for multiple applications in order to get things done faster.
  - Increased use of SaaS and third-party applications with no formal review of the security posture of these applications.
  - The data stores the applications access are constantly changing.
  - There is no end-to-end review of the constantly evolving identity/application/data access combinations.

Impact

- Zettabytes of data are being stored in cloud platforms which is driving massive demand for access to this data.
- Among the impacts caused by Shadow Access are:
    - Existing tools are blind to the many cloud identities and access pathways.
    - Governance and visibility gaps make it very difficult to implement IAM Guard Rails.
    - Unknown pathways allow vulnerabilities to be exploited to breach cloud data.
    - Threat actors can weaponize programmable access to cause harm far beyond the breach of data.
    - Third-party and SaaS Applications that connect to cloud ecosystems introduce lateral movement risks.
    - Breaks cloud security, data security, governance, risk, and compliance.
- The true security state of an environment is never known, and the mechanisms and processes to derive that information are typically outdated before the analysis is complete.

Conclusion

- Shadow Access, as a new problem, impacts many process areas in cloud computing.
- A new generation of tools and processes needs to be established and instrumented to address the issue of Shadow Access, re-establish the intended state of access and data security, and allow the full benefits of the cloud to be achieved.
- The broader trends of automation, AI, and data creates a fertile environment for Shadow Access to thrive.

Acknowledgements

- Lead Authors
  - Venkat Raghavan
  - Sasi Murthy
  - Steven Schoenfeld
- Contributors
  - Michael Roza
  - Heinrich Smit
  - Shruti Kulkarni
  - Philip Griffiths
- Reviewers
  - Rajat Dubey
  - Ahmed Harris
  - Shraddha Patil
  - Senthilkumar Chandrasekaran
  - Ivan Djordjevic
  - Osama Salah
  - Alberto Radice
- CSA Analyst
  - Ryan Gifford