

NEWS RELEASE

Stack Identity Announces Industry's Only Shadow Access Risk Assessment to Prioritize Cloud and Data Security Risks

10/3/2023

- Free daily scan and report of Shadow Access risks in your cloud environment
- Eliminates the need for piecemeal manual tools and processes
- Deployable in the most secure environments; no external credentials required

MENLO PARK, Calif.--(BUSINESS WIRE)-- **Stack Identity**, a Silicon Valley based company pioneering an identity security platform that champions a unified, consolidated and automated strategy to tackle Shadow Access, today announced its new Shadow Access Risk Assessment (SARA) — a free product that provides users with a daily report of Shadow Access risks in their environment.

Stack Identity Shadow Access

Risk Assessment Sample

(Graphic: Business Wire)

The rapid proliferation of large language models (LLMs), ChatGPT and other AI-driven applications have significantly expanded access to enterprise data, leading to a surge in entitlements and privileges granted to both human and non-human entities.

Shadow Access — or unauthorized, invisible, unmonitored and unintended access — has rapidly become one of the most pressing challenges for organizations safeguarding valuable data in the cloud. **Data** from Verizon states that 80% of all breaches involve existing credentials or identities in the system.

The complexity and scale of cloud identity, access and entitlements makes it extremely difficult for security practitioners to understand and quickly identify the most pertinent risks. An **IBM** report found that the average data breach took an alarming 212 days to detect and a whopping total of 287 days to contain entirely.

Cloud security practitioners are tasked with bridging the security gaps in a fragmented system. Practitioners need to ensure proper access for both human and non-human identities to the relevant data and systems, while maintaining crucial visibility into potentially weaponizable access pathways and entitlements.

Stack Identity recognized that few products on the market directly addressed the needs of overburdened security engineers who deal with constant alerts, false positives and an overwhelming amount of data spread across multiple tools and systems. To address this gap and eliminate the need for piecemeal manual tools and processes, Stack Identity invented SARA.

SARA deploys directly into a customer's cloud environment to comprehensively assess and analyze different cloud events and identify emerging Shadow Access risks. With SARA in place, customers receive a daily email recapping any new threats that have originated in the past 24 hours and a call to action so security practitioners can spend their precious time on remediating Shadow Access rather than detecting it.

"The fundamental law of cybersecurity is you can't protect what you don't know about, and this is especially important when you consider that identities provide the literal keys to the kingdom," says Jack Poller, senior analyst at Enterprise Strategy Group. "Understanding the dynamic and changing nature of which identities have access to sensitive data and critical resources is crucial for reducing organizational risk."

Since many security and compliance controls prohibit access to SaaS monitoring tools, SARA is deployed and runs locally within a customer's on-premise trust boundary. Due to its automated detection capabilities and daily summaries of contextualized risks, SARA dramatically reduces customers' MTTD (Mean Time to Detect) by 60% to 80%.

"We developed SARA to ease the burden of identity threat detection for security practitioners across industries," says Venkat Raghavan, founder and CEO of Stack Identity. "Rather than spending valuable time manually compiling data, SARA users receive a comprehensive, daily assessment of Shadow Access risks, allowing them to focus their time on eliminating security threats instead of uncovering them."

Shadow Access is difficult for organizations to detect and easy for hackers to exploit - and at a fundamental level Shadow Access breaks Zero Trust architectures. As organizations continue to share data in the cloud, their digital attack surface will continue to expand. This makes the need for advanced risk management capabilities greater now than ever before.

To run an assessment of Shadow Access vulnerabilities and find the IAM blindspots in your cloud environment, register here: www.stackidentity.com/Shadow-Access-Risk-Assessment.

About Stack Identity

Founded in the heart of Silicon Valley, Stack Identity is an identity security platform that brings a unified, consolidated, and automated approach to continuously detect, eliminate and govern Shadow Access. Through its patent-pending algorithm Breach Prediction Index (BPI), Stack Identity reveals ten different types of Shadow Access patterns that expose sensitive customer data, create audit and compliance violations, and break policies and governance. The platform delivers risk and impact-driven prioritization empowering operations and security teams to automate remediation. Stack Identity is backed by WestWave Capital and Benhamou Global Ventures. Visit us at www.stackidentity.com, and follow us on [LinkedIn](#).

Treble

Matt Grant

stackidentity@treblepr.com

Source: Stack Identity