rubrik

'No One-Size-Fits-All' Solution to Resilience and Recovery

Rubrik's Mohan on Identity Resilience, Recovery and New Unknowns in Cyber

iSMG
INFORMATION SECURITY
MEDIA GROUP

As traditional remediation strategies fall short of identity-based cyberthreats, identity resilience is becoming as much a business imperative as recovery.

Hema Mohan, vice president of product management at Rubrik, said organizations now face a new reality where identity has become the fastest and most reliable way to bring a business down. Recent surges in non-human identities and the emergence of agentic artificial intelligence put even more emphasis on building resilience. Resilience is about restoring operations with minimal impact, even amid highly dynamic identity systems that change daily, Mohan said.

"We're dealing with massively complex, multi-cloud, hybrid, SaaS-heavy environments. There's also been non-human identity explosion, which has increased the surface area of attack. And now we've also reached an inflection point with agentic AI, which has become a new vector of compromise," Mohan said.

In this video interview with Information Security Media Group at Gartner Identity and Access Management Summit, Mohan also discussed:

- Distinct recovery paths organizations must prepare for;
- Why rolling forward changes is essential for dynamic identity systems;
- How Rubrik supports resilience across AD, Okta, Entra and their dependencies.

Mohan, who leads product management at Rubrik, is an experienced product leader with more than 20 years of experience in building, shipping and selling enterprise software. As a product leader with strong product instincts and a solid enterprise sales background, she uses customer feedback to make data-driven, actionable decisions and build SaaS and security products.

Identity Security vs. Identity Resilience

TOM FIELD: There has been significant focus on identity security and not enough on identity resilience. Why is there such a critical distinction?

HEMA MOHAN: Identity security focuses on stopping or at least trying to stop attacks. Identity resilience is focused on helping businesses recover or even survive these attacks. The critical distinction here is that security is all about preventing the attacks, and resilience assumes compromise and focuses on quickly recovering from these attacks with minimal impact.

Why Identity Resilience Is Urgent Today

FIELD: With so many identity-related attacks, why is there an urgency for identity resilience today?

MOHAN: The urgency for identity resilience primarily comes down to unfortunately one hard reality, which is identity has become the fastest and the most reliable way to bring a business down. The reason this is happening is, one, we are dealing with massively complex environments: multi-cloud, hybrid and SaaS-heavy environments. Second, there has also been NHI explosion, which has increased the surface area of attack. Now we've also reached an inflection point with agentic AI, which has become a new vector of compromise.

Key Trends in Identity Attacks

FIELD: What trends are you currently monitoring?

MOHAN: Rubrik has a research team called Zero Labs. Zero Labs releases a report every quarter, not based on what it finds fancy or important, but what customers think is the important trends for that quarter.

In November, we released a report which was focused on identity. Three main things that stood out from that report for me were, one, 90% of the organizations have reported a cyberattack in the last 12 months. Second, 79% of CrowdStrike's detections were malware-free. What this means is attackers are directly logging in - they're no longer deploying malware. Finally, about 90% of the IT and security leaders that we surveyed as a part of this research said identity-based attacks is the number one threat.

Recovering From Identity-Based Attacks

FIELD: When there is an identity-based attack, what does the recovery process look like?

MOHAN: Recovery looks very complex in a situation like this. First of all, we're assuming recovery begins after one of the threat detection and response tools have identified what the entry point was and contained the attack vector. Then recovery goes back to that point and finds the last known safe state, and then understands that there's no malware. You're not reintroducing any malware or any of the bad actors. You then go back and roll forward the changes.

The reason I say "roll forward" those changes is because identity systems are highly dynamic. On an average, organizations are making changes to it on a day-to-day basis. Organizations are adding new employees and new groups. They can lose all those changes if they go back 45 days. Organizations need to deem what was malicious and what was intentional change, and then roll

forward that change so there's minimum data loss. That's the complex action that runs in the background to ensure recovery.

Different Types of Identity Recovery

FIELD: Are there multiple types of recovery?

MOHAN: There's no one-size-fits-all; there are different types of recovery. One is the hard reset, where you bring back the identity systems. The second type involves bringing back the systems and rolling forward all the changes that are needed. There are also surgical changes that you want to roll back on a day-to-day basis when you find something malicious.

Rubrik's Approach to Identity Resilience

FIELD: How is Rubrik helping customers embrace the concept of identity resilience?

MOHAN: Rubrik has been helping customers with cyber resilience, and identity resilience has just been a natural extension to that. Rubrik is the only vendor that supports multiple identities. You no longer find an organization with just AD, just Entra or just Okta. These are massive, complex organizations with multiple identity systems, and we support all these three IDPs. We don't just protect AD, Entra or Okta, we also protect and recover all the downstream and upstream dependencies.

For example, AD and Entra, there is a unique orchestration happening between the two. When we bring back AD, we bring back Entra as well, along with all the downstream dependencies. We not just recover the system and the dependencies, but we also roll forward the changes to ensure that you've not lost any data. We are also constantly monitoring and alerting for any kind of malicious changes that happen on these identity systems, and we're rolling it back on a day-to-day basis. We have a complete, widespread gamut of options that customers can pick from, and that's how our customers are being serviced today.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

CIO.inc DeviceSecurity.io PaymentSecurity.io FraudToday.io

CYBER THEORY CyberEdBoard Xtra mile LIFECYCLE MARKETING GREYHEAD gh

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io