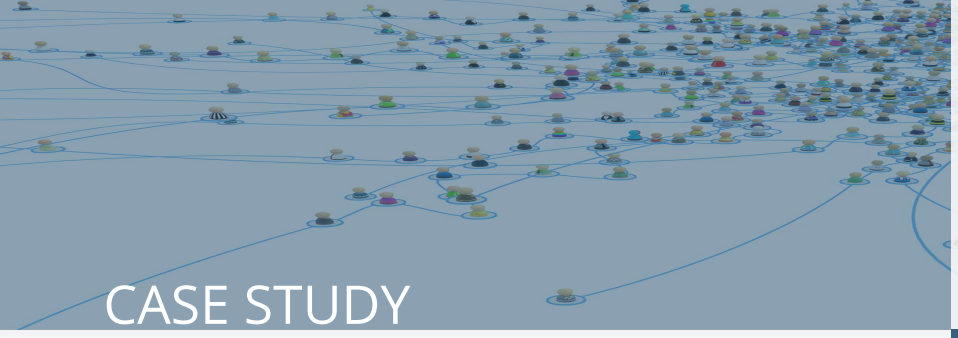

IDENTITY DEFINED
SECURITY ALLIANCE

# CASE STUDY

## LogRhythm's Journey to Identity-Centric Zero Trust

**Overview**
As a next-generation security information and event management (SIEM) company, LogRhythm is on the cutting edge of security, dedicated to helping organizations to reduce risk by rapidly detecting, investigating and neutralizing damaging cyberthreats. But just like every organization, they are also susceptible to a breach, and change in processes and policies — especially where it introduces friction — is a challenge. When James Carder, CISO and VP of LogRhythm Labs, joined the organization, he recognized he had an opportunity to not only improve the security of a security organization, but to also develop and implement an architecture based on Zero Trust that could be used as a model for organizations of similar size and IT characteristics.

Fortunately for the LogRhythm team, the existing IT environment was built with a cloud-first approach, reducing the complexity of their IT infrastructure, while enabling a distributed workforce. The transition to a Zero Trust architecture would need to prioritize scope and existing technology, allowing it to integrate with the current infrastructure in a way that available resources and budget could support.

**Solution**
James has been a supporter of Zero Trust since Forrester introduced the concept in 2009. The Zero Trust model lifts reliance on a single perimeter and moves it to every endpoint, user, application, and data element, with the user/identity context as the common thread. The sharing of identity context through integrated technologies is the basis of identity-centric security. The result focuses on two primary principles:

1. Don't inherently trust anything on or off your network, and
2. Apply appropriate security controls based on the data

LogRhythm approached the project in phases, starting in 2018, targeted to complete in 2020. This approach involves the following steps:

- Perform data identification and classification of toxic sensitive data
- Map out and identify locations of data flows and system architecture
- Implement identity and access management (IAM) and two-factor authentication (2FA), addressing role governance
- Integrate user and entity behavior (UEBA) analytics and trust inference for adaptive access
- Implement micro-segmentation and privileged access management
- Develop access control engine and inference pipeline

Once fully implemented, the team believes they will have the closest thing to a silver bullet to streamline the IT organization, improve security and reduce risk of a breach.

Industry
- Technology

Challenge
- Dissolve entity perimeter, including legacy technologies
- Eliminate complexity of identity governance
- Implement with limited disruption, change and friction
- Work within resource and budget constraints

Solution
- Deploy a Zero Trust approach to security using identity-centric principles
- Leverage existing identity and security technology investments
- Introduce automation and sole source of truth for streamlined IT

Lessons Learned
- Size and complexity of organization matters
- Bringing together vendors to meet the requirements is time consuming
- Identity-centric security implements Zero Trust concept

IDSA Framework
- Risk-based authentication

IDSA Member Technologies
- Okta
- LogRhythm

*Identity is at the heart of Zero Trust. The identities of your employees, the systems, the data they access, and their environmental context define the Zero Trust model. As a security software company, the last thing you need is a catastrophic security breach. We believe the Zero Trust model is the best approach to protect, detect, and respond to incidents before they become catastrophic breaches.*
*James Carder, CISO, LogRhythm*