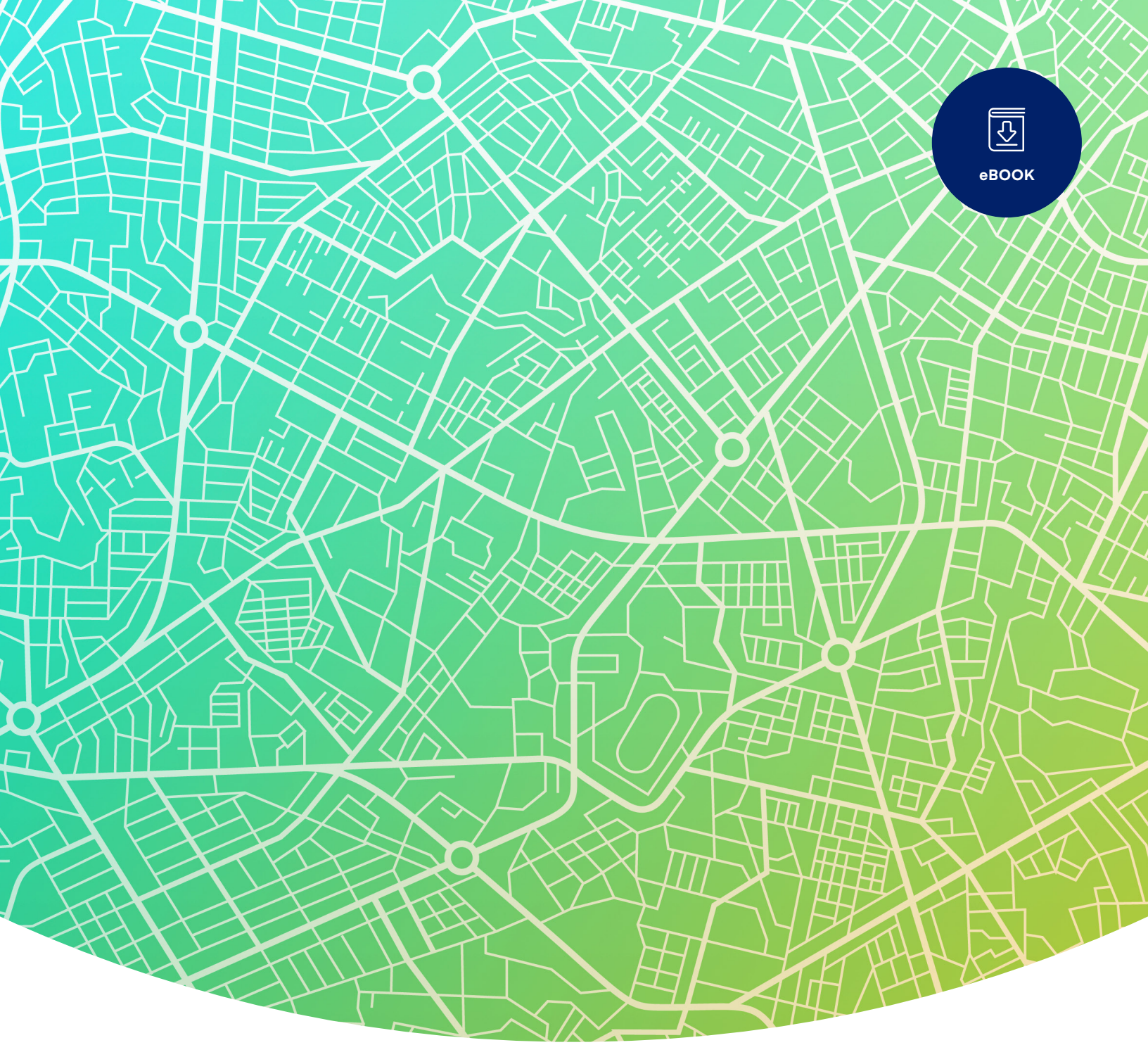

Identity in a **Zero Trust World**

SailPoint

We have a concept at SailPoint: identity at the center of security. While that may appear self-gratifying, when one digs a little deeper, they'll discover why it is accurate. Zero Trust has been the growing buzzword and theme for the last couple of years in security. At its core, it means we build our solutions to habitually question who someone is and what they want to do. We can no longer blindly trust a user that comes from a known location. We need to keep asking questions.

At the center of those questions is a critical concept: identity. Our solutions must continually validate the identity of the person accessing our applications and data. That includes authentication, authorization, and one that might not entirely be as obvious is administration. The identity becomes the Golden Key to ensuring that we can validate users. We need trusted sources that tell us who someone is and what access they should have. From there, we can form the foundation of our policies that determine how things are accessed.

While it all sounds great in theory, what does that mean in reality? What steps can you take to get there? What does that mean for your firewall?

Let's answer all of those questions.

First, what does it mean to have a Zero Trust model?

There is no such thing as an internal network. Whether a worker is accessing the network from their office desk, Starbucks coffee shop, or even Bangladesh, nothing changes as far as trust goes. There are no "if/then" rules that determine the strength of authentication that should be used based on whether the user is internal or external. As far as the application is concerned, all users are external. MFA is utilized across the board, for every user, every time, everywhere. We get smarter about authentication and ask a lot more questions of the user by including behavior patterns, and a more in-depth look at the user's attributes. Does the user know the password, and are they logging in from a device we've seen before with an IP address we've seen before and from a location we expect? That's a very different set of questions from a simple user authentication process that asks, "Does the user know the password and some random number?"

Second, embrace the concept of "question everything"

We've verified who the user is; now, we need to verify what they are doing or asking to do. Is the user trying to access payroll data during business hours from an IP address we see often? Including more context into authorization decisions enable you to base access decisions on what's happening right now rather than a set of static rules or policies that were established six months ago or longer. To support this effort, an identity solution should have the ability to build dynamic authorization policies that include information about the user and about what the user is trying to do. Also, it should provide user behavior patterns to understand what activity is considered normal and which are abnormal. In short, zero trust means being smarter and more in-depth the actions we take to verify a user.

Zero trust starts with identity

Everything that has been addressed centers around identity. Having a robust identity infrastructure gives organizations the ability to build more dynamic and identity-aware applications. Administration and governance is the first brick that is laid to develop a robust solution. It is what creates a solid foundation. A trusted source is required to pull attributes needed for authorization policy and deeper authentication. The process of feeding that source and ensuring that the attributes are accurate is where governance and administration come into play. This process allows organizations to control the lifecycle of new accounts and attributes and ensure they are aligned both from a quality perspective and policy perspective.

These concepts combine to create a "Zero Trust" architecture. However, one must remember that zero trust is not a solution. Zero Trust is a way of thinking, or perhaps even better stated, an approach. The entire concept should challenge organizations to think differently about how they build applications, networks, and security controls. They should start with the belief that no one can be trusted. They cannot depend on a single attribute to determine the level of trust; instead, they must continually build that trust with the user by asking questions: "Who are you", "where are you coming from", "what are you trying to do", "when are you trying to do it". The common component for all of these questions is establishing the person's identity - the more their identity is established, the more they can be trusted, and the more access they can be given.

SailPoint Predictive Identity™

Digital transformation has introduced the challenge of more users, apps, files, and cloud platforms to manage and protect. Using the power of AI and machine learning, organizations can now effectively take on their zero trust initiatives with confidence. SailPoint Predictive Identity speeds the process of creating access models and policies and helping keep them up-to-date as organizational changes occur. It provides peer group analysis to quickly identify risky outliers that possess excessive permissions and offers recommendations when determining if access should be granted or revoked; helping ensure everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically.

SAILPOINT: RETHINK IDENTITY

sailpoint.com

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning (ML) technologies, the SailPoint Predictive Identity™ platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world's most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers' dynamic business needs.

Stay up-to-date on SailPoint by following us on **Twitter** and **LinkedIn** and by subscribing to the **SailPoint blog**.

EB1343-2003