

# Identity is the Root of Establishing Zero Trust

(And Why You Might Be Closer to Achieving Zero Trust Than You Think)

Enterprises across the globe are fast-pacing zero trust initiatives as compliance regulations stiffen, government mandates are enforced, and advanced cyberattacks rise at an unprecedented rate.

Zero trust, a security model rooted in the guiding principle “*never trust, always verify*” who you are providing access to – both inside and outside your organization – requires verification for *everyone* trying to gain access to your organization’s resources. While the concept of zero trust may appear new, security technology and solution providers have long understood that gone are the days where a strong “perimeter” defense was enough to keep out bad actors and renewed their risk focus to a more granular level – Identity.

## THE CHALLENGE

**The implementation of zero trust architecture that supports establishing strong identity verification before access is granted may appear simple.** However, expanding network boundaries, increasingly diverse workforce, third-party vendors, and rapidly evolving compliance mandates have expanded the complexity of identifying users at a time when the threat landscape is more sophisticated than ever before.

Correctly identifying who has access to your assets and managing their identities is just the beginning in implementing your zero trust strategy. Executing zero trust correctly requires your organization to look beyond identity and access management to gauging the risk each identity poses to your organization.

Distinguishing the risk each user requesting access poses to your assets can be a daunting task. Swift, on-demand access, diversity in the types of users requesting access, and what assets they are accessing must all be considered without overcomplicating the user experience. Understandably, this is just a sampling of the large volume of information that must be processed to accurately gauge risk and a good demonstration of why manual identity processes have become archaic.



Manually managing identity and access is not only an extremely inefficient use of resources, but it’s costly, and often results in more human-related errors – increasing your risk of a breach. A strong zero trust strategy utilizes intelligent automation capable of orchestrating identity and access processes.

## THE SOLUTION

### Zero Trust Begins with SDG Identity & Access Governance.

SDG recognizes that reconstructing your security budget to achieve every new security approach or mandate that comes around is not always prudent or feasible when you are working hard to grow your organization’s revenue. However, we believe that the security benefits of implementing zero trust architecture are worth the investment and protection it affords your organization.

That is why we partner with you to drive value from the platforms you already have in place. We are experts in the field of navigating legacy environments and, when necessary, modernizing the environment to support zero trust and other standards. **The fact is, you might be closer to achieving zero trust than you think!** Our strong team of domain experts, architects, and developers are equipped to find out, they will advise you on how to turn zero trust into reality and, ultimately, transform your current environment into a more secure space.

## THERE'S MORE TO ZERO TRUST THAN WHICH TECHNOLOGY PLATFORM

Technology that supports zero trust, including automation and monitoring platforms, is necessary. However, there's more to achieving zero trust than which technology platforms you utilize. Achieving zero trust also requires a deep understanding of your unique risk tolerance and risk mitigation strategy. A thorough analysis of your existing technology, infrastructure, and strategy, combined with SDG's expertise on how they work together to support a more robust security process is the key to success.

Let SDG partner with you to advise, transform, and manage your identity and access governance to achieve your zero trust goals, better protect your assets, and achieve a sustainable, scalable, security solution that starts with where you are today. To learn more visit [SDGC.com](https://sdgc.com).

## ABOUT SDG

SDG is a global cybersecurity, identity governance, risk consulting, and advisory firm that advises and partners with clients to address their complex security, compliance, and technology needs and delivers on strategy, transformation, and long-term management of their cybersecurity and IAM programs.



■ 55 North Water Street  
Norwalk, CT 06854

■ 203.866.8886

■ [sdgc.com](https://sdgc.com)