WHITE PAPER

avancer®
Simplified IT Security

WHY IS ZERO TRUST USING IAM IMPORTANT IN THE POST PANDEMIC WORLD?

EXECUTIVE SUMMARY

The new corporate mantra is to “Don’t’ trust anyone. Verify everyone.” Extending it to the IT security ecosystem, experts believe that implementing the zero trust model enables enterprises to protect data and keep their network secure. Such a concept has become more than necessary to be implemented in the post-pandemic era with organizations adopting an increased digital landscape to support remote working, mobile devices, third-party apps, cloud deployment and IoT devices, among others, for maintaining business continuity. Thus, networks and systems can now be accessed by anyone at any time, making them vulnerable to internal and external threats.

Perimeter-based security approach, therefore, is no longer relevant, and is gradually being replaced by the zero trust model, with focus on identity. Going beyond the set parameters of perimeter-based security, zero trust encompasses security architecture for including new users and IoT devices, helping in rapid adoption of cloud environment, and creating consumer engagement models. With COVID-19 compelling enterprises to undertake large-scale digital changes, the need of the hour is to rapidly adopt zero trust to secure the IT ecosystem.
At its core, the zero trust model works on the assumption that all the users accessing the system, technologies and network infrastructure within the organization are not trustworthy by default. It also rejects the hypothesis that any internal user or machine could be trusted automatically. Implementing such as model to identity and access management (IAM) framework enables businesses to grant access to users from anywhere, a core requirement of the ‘new normal’ of remote workforce, while ensuring a vigilant and centralized security policy

Even before granting a user access to the enterprise network, systems and data, including sensitive information, from any access point, the zero trust model focuses on establishing the identity of the user at the forefront itself. In the near future, zero trust strategies are expected to play a more pivotal role in the implementation of IAM technologies.

INTRODUCTION

Network security is being redefined with the expansion of remote workforce and adoption of cloud applications. This is challenging the traditional concept of perimeter-based security, wherein it was assumed that anything inside the corporate firewall could be labeled as safe. However, in the current digital landscape, enterprises need to relook at their strategy of trusting their corporate network inherently, and pivot towards the zero trust model to view all the users, whether internal or external, as untrustworthy.

Created by Forrester Research, the concept of zero trust, when implemented in IAM technology, helps companies to create a holistic security posture, without compromising on end-user experience. Here's how:

- Enabling security team to deploy greater integration for connecting identity data with data protection policies and networks.
- Maintaining identity records and linking them to user access rights as per data access privileges and access-certification.
- Alleviating the impact on security due to adoption of API-based microservices through the implementation of zero trust theory

Modern businesses need to ensure that along with providing a secure platform, they should also focus on seamless user experience. IAM requirements have in fact become increasingly complex as customers, partners, employees, and even bots are using unique identities with differing access privileges. The juxtaposition of IAM with zero trust model may help in achieving both the ends of continuous verification of users, along with providing them with a smooth access and experience. However, such an implementation is not simple. It requires major change in mindset and security technology methods. Developing a detailed roadmap to integrate zero trust strategy with IAM is pertinent for the success of such a model. Implementation of zero trust needs to be conducted in a gradual manner, with strategic planning, regular monitoring and updates, and cannot be a one-time deployment.

THE POST-PANDEMIC WORLD AND THE NEED FOR ZERO-TRUST

COVID-19 has dramatically changed the situations across enterprises and industries, with emphasis on digital transformation and remote working. This led to the attack area expanding drastically that exposed technological vulnerabilities, increasing risk and threatening security of an organization. Further, with the unexpected closing of monitoring centres, it crippled the condition further and many businesses came under direct threat of cyber-attacks.

Moreover, providing safe remote working environments for employees was seen as a critical shift for many organizations since the onset of the pandemic. While CIOs had a clear understanding on how the organizations will function in the 'new normal', they were still coping-up with the situation of safeguarding their perimeters – in terms of data. Enterprises across the world are facing multiple challenges, including ensuring business continuity while enabling technology transformation in the face of growing number of attacks on their network. Cyber-attackers have been quick to exploit the situation wherein large scale professionals moved to work-from-home, increased customer-facing networks issues and customers depending heavily on the use of online services.

For surviving during these unprecedented times, organizations need to become digital to the core, or digital-first companies. There are four fundamental areas which could be considered drivers for steady growth in the future – Remote operations to prevail even after pandemic, Protect the business environment against cybercriminals, Cost controlling and efficient use of the resources available and Protect the revenue avenues.

To become digital first, enterprises need to secure their systems as well as networks from cyber-attacks. They have to invest in an integrated identity management solution. New approaches have to be adopted that includes zero-trust networks, threat hunting, privacy-enhancing technologies, asset categorization and many others. These approaches are able to support new working model, which is scattered in nature. CISOs also need to reassess the present infrastructure as well as practices that include risk management. Constant resilience towards cyber threat is the newer way to survive in this business environment.

WHAT IS ZERO TRUST?

This framework of zero trust can be described as a strict approach towards cyber-security. In this environment, every individual or any device that attempts to access the private network, which might be located outside or inside the network - should be identified as well as authorized. Dissimilar to other security models that automatically trusts individuals or any devices that are within the corporate network - zero trust focuses on trusting no one at any point in time. This model was first discussed by John Kindervag, who was a principal analyst in 2010 at Forrester Research.

The theory acknowledges that IT security models that were used traditionally only protects network from the outside but are unable to secure threats from individuals or any devices that have already been logged into the network. This could enable a trust environment which could be misplaced. The attack could be from inside - from an employee or a device which could have been compromised from an outside attack.

Zero Trust states that inherently trusting every users or any devices that has been there in the network traditionally could result in compromising IT security models, which if remain unchecked could provide an opportunity to bad actors to move around freely inside the corporate network. They would be able to access corporate data and could raise the severity of a cyber-attack. Zero trust framework argues that the organizations should already assume that the network has been compromised. They should implement strategies or technologies for minimizing risk. Some of these strategies include:

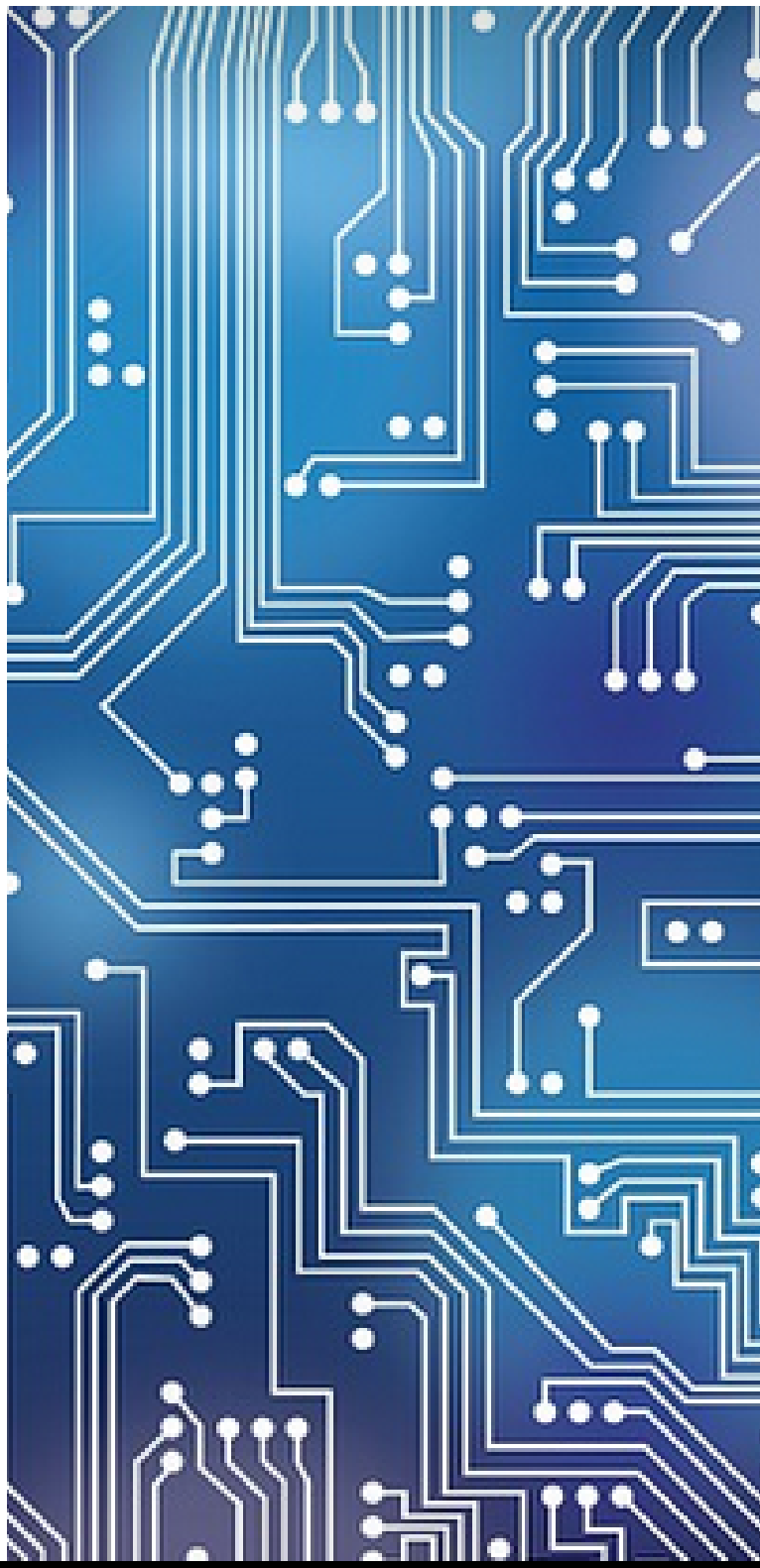
Segregation of Duties (SoD). This principle is also known as separation of duties. It states that the no singular individual or any device should be given full access to an organization's IT sources. If one individual or device is given the access to the entire information, a hacker may gain control and get unfettered access to corporate network by hacking into the account. Some of the examples to broad access include virtual private networks - VPNs- and network firewalls. Another dimension of SoD includes no individual should be given multiple roles that are critical.

Least privilege access. The separation of duties is achieved by providing user a role with least privilege access. This means that every user or any device which is there within the network is able to access only essential part of the resources that they need and nothing else. The benefit being, if the user's credentials or the device is compromised, the hacker would have access to device's environment only.

Microsegmentation. Zero Trust model inclines towards microsegmentation, which includes splitting up the IT environment in an organization into security zones. This would require an individual or device separate authorization for accessing each zone. The practice is able to limit the chance that a hacker is able to access the entire network.

Multifactor authentication (MFA). This is a principle which requires more than one method of authentication for verifying user credentials. For instance rather than relying on password, MFA would ask the user to enter a secret code which might be sent to an email address or phone number.

Auditing and tracking. An audit trail ensures that an up-to-date log of each connection with verified identity is maintained. With this, zero trust solution is able to offer session recordings for knowing exactly the actions taken in a session. This has been found useful for forensics as well as reporting in Security Information and Event Management (SIEM) systems.



ZERO TRUST IN IAM STRATEGY

In order to provide security at par with today's digital enterprise needs, it is essential to move beyond perimeter-centric security approach to zero trust model based on data and identity. The concept of zero trust, as explained above, focuses on more than network segmentation, and instead provides a holistic approach to security that encompasses people (users), workloads, networks, devices and data.

ZERO TRUST PEOPLE (USERS)

Zero trust strategy focuses on regulating and strictly enforcing user access, along with securing the users in the network. This includes technologies required to authenticate users and monitor and govern their privileges and accesses constantly. It also focuses on implementing technologies to safeguard interaction of users over solutions such as remote browsers and web gateways. Further, growth in biometric authentication has also resulted in expanding the zero trust perimeters. Here's how zero trust could be leveraged for authenticating and protecting users:

- **Resolving critical business or audit issues.** Adoption of zero trust in IAM enables enterprises to resolve the pressing challenges associated with user access. Addressing the requirement of an organization's digital transformation needs, implementation of IAM technologies such as MFA and single sign-on (SSO), based on the principal of zero trust, helps in proactively resolving any possible compliance, security or operations issues.
- **Applying least privilege policies.** The focus is on not providing users more access to data than needed, a core principle of zero trust. With users switching jobs or getting transferred to different departments or projects, it is imperative to reset or revoke their accesses accordingly. Creating over-privileged users may lead to data breaches. Further, such user accesses should be reviewed at least annually as per the changed scenario, and appropriate actions should be undertaken.
- **Moving beyond passwords.** Passwords are susceptible to hacking, due to its inherent vulnerability. Thus, moving beyond passwords to use passwordless authentication methods such as tokens, biometrics, tokens, Auth0-related solutions and keys decreases the possibility of hacking attacks. In order to retire passwords, enterprises may implement solutions provided by vendors such as Microsoft, Okta, Google, Secret Double Octopus, Ivanti and others.

ZERO TRUST NETWORKS

One of the important components of zero trust is the ability of isolate, segment and control networks. Enterprises are able to understand that isolation and segmentation provide holistic and secure networks, and have been investing in such solutions provided by vendors such as Cisco, Palo Alto Networks, Forcepoint, Akamai and VMware, among others. Here's how zero trust could be leveraged for securing networks:

- **Protecting networks and resources through boundaries/segmentation.** Segmentation policy focuses on defining the access parameters for each group with regards to another group. For instance, while the application tier can collaborate with middleware, which in turn can connect with the databases, the application tier is not provided direct access to the database. This ensures that the hackers are not able to exploit applications to access data, due to the presence of the middleware. However, it is imperative to review the segmentation policy for anomalies before enforcing it.
- **Achieving border security goals.** The focus should be on absolute control over accesses in the enterprise. Tracking user-generated traffic through web gateways enable enterprises to detect and block any risky activities, along with preventing malware. Solutions based on DNS, which are easier to deploy, can also help in achieving such border security goals of the enterprise.

- **Augmenting cloud security controls.** Through the use of next-generation firewall based on zero trust principle can help business to enhance security controls, even in the cloud environment. Such firewalls are now enhanced with crypto chips to inspect and decrypt all traffic moving through a boundary. In case of cloud, one could include a layer of autoscaling virtualized firewalls for inspecting application traffic.

ZERO TRUST DATA

An integral part of zero trust is data security, which focuses on managing and securing data, developing and categorizing data classification and encrypting data which is both in transit and at rest. Some of the vendors who focus on mapping zero trust strategies to secure data include Forcepoint, Microsoft, Micro Focus, Gemalto and Thales eSecurity, among others. Here's how zero trust could be leveraged for safeguarding data:

- **Defining which data set need to be protected, where and how.** In order to identify the location of data, and to especially find out sensitive data, it is imperative to build capacity to classify and discover data. Such capacities are found in technologies such as Titus, BigID, James and Microsoft Information Protection.
- **Understanding the data lifecycle and threats associated with it.** Find out about policies and controls and gain technological and business insights with data intelligence feature. This helps in understanding core features related to data such as – flow of the data, usage of data and for what purpose, requirement of creating the data by the enterprise, data collection process, lifecycle of the data, and impact of any data integrity compromise. In addition, understand the threats to your data collected from other security tools in your environment, such as DLP and EDR, to help guide decision-making.
- **Protecting data through technologies.** In order to protect data, enterprises need to control access, inspect patterns of data usage and dispose data in a secure manner. Some of the technologies that enable data security include encryption, such as database encryption and email encryption, which help in safeguarding data at rest, in use as well as in transit.

ZERO TRUST WORKLOADS

Workload is a standard used in infrastructure as well as operations management. This is an entire application stack from app layer through hypervisor – in other words self-contained components – which is used for processing that includes virtual machines and containers in the stack. Workloads are considered to be the frontend and back-end systems, which run the business. It also helps in winning, servicing and retaining a customer. In the area of zero trust, these connections, as well as components should be considered as threat vector and should have zero trust controls. One of the particular concerns regarding workloads is that it runs on the public clouds. AWS, Perimeter and Guardicore deliver solutions that help in securing workloads. Below are some of the pointers through which zero trust can be leveraged focusing towards workloads:

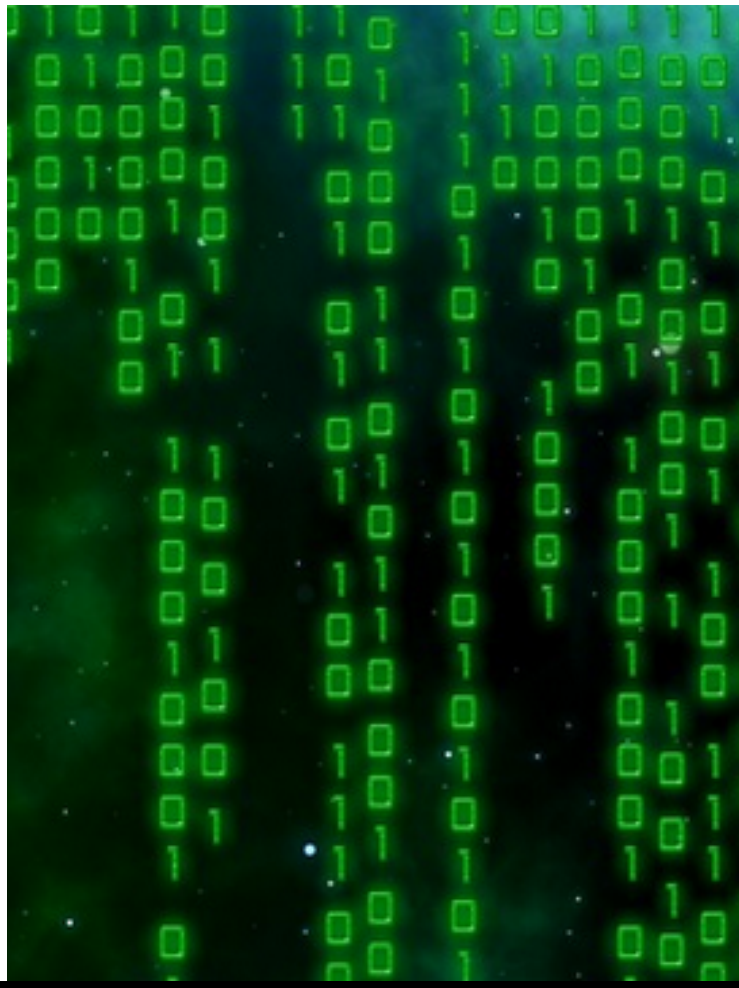
- **Establishing a holistic cloud governance process.** Building a repeatable process ensures governance becomes an ongoing benefit to security and it is not just a one-time effort. Process documentation and establishing formal organizational structure helps in ensuring two-fold benefits - a) Adequate scope and coverage - as organization might have different areas along with various infrastructure components that it might want to cover, including private, on-premises, and public clouds; and b) Cover cost optimization, regulatory compliance, budgets, and threat detection should be covered under cloud governance.
- **Monitoring workload configurations.** Since it is easy to create, cloud workloads are able to proliferate quickly, most times without any oversight or even formal governance of cloud platform credentials. Thus, cross-cloud workload security is required to ensure cloud security.
- **Focusing on cloud-native security.** Cloud washing as well as dumb lift together with shift of data workloads to cloud that does not have proper governance structure often times lead to data sprawl, high costs and data protection issues. Protection and configurations that are appropriate for on-premises workload are rarely suitable in a public cloud.

ZERO TRUST DEVICES

Network-enabled device technologies and IoT introduced a huge area of potential compromise for enterprises and networks. Mobile devices, smart TVs and even smart coffee makers are there in the market now and each of these items brings new avenues of assets and code that a security team must track as untrusted source in any infrastructure.

For moving towards zero trust strategy, security teams should be able to secure, isolate and control each device which is there on the network on a consistent basis. This might require endpoint security solutions which is a traditional approach. Newer network access control solutions are available with vendors such as MobileIron, Forescout, Trend Micro and Pulse Secure. Below are the places where zero trust can be leveraged focusing on devices:

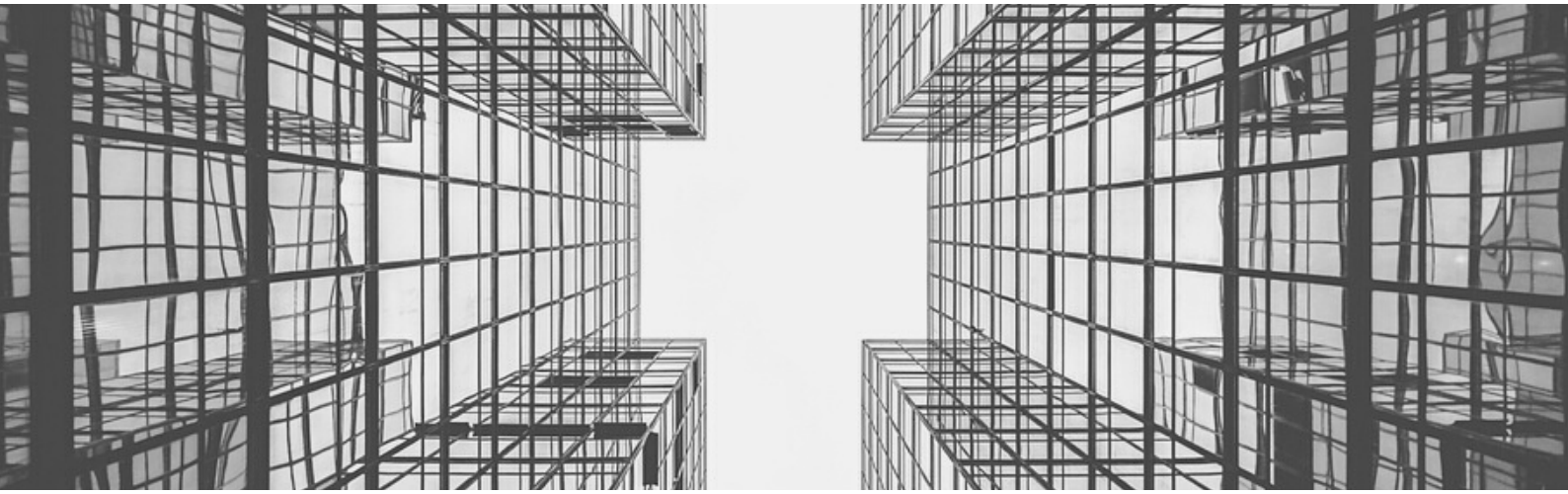
- **Applying zero trust to manage devices.** IoT network segmentation solutions are able to take an existing network of IoT devices and then create zones or microperimeters for helping isolate IoT devices from other networks or IT devices. This also includes the ability for quarantining compromised or potentially infected devices from further spreading malware. By segmenting user as well as device traffic from the rest of the network helps reduce risk of cybersecurity incidents significantly.



- **Hardening IoT devices.** Hardening solutions from IoT device enables IoT device as well as create data integrity that includes trusted execution environments obfuscation, secure firmware, or binary modification for minimizing risk of device or data tampering. Once it has been implemented, device hardening is able to support secure communications, secure patches, signed software delivery, and application updates. These categories would be able to include scenarios such as application sandboxing and device-based lockdown. In this space the vendors include Infineon, Cisco, Thales and Intel.

- **Curtailing user risks due to BYOD policies.** Endpoints should not be considered “yours”. BYOD as well as increasingly mobile workforce has eliminated control IT that is used over endpoints which connects enterprise networks. It also minimize issues by refuting overt threats that is presented by the endpoints, which includes malicious software infections, malware and ransomware events. By conducting health checks on endpoints before allowing them to connect over the system would be a good start point. Ivanti, Cisco (Duo), Unisys and Microsoft have device health checking which can be applied.

CONCLUSION



With pandemic disrupting businesses and driving them towards digital transformation, it is imperative to focus on a fool-proof security model. Looking beyond the traditional perimeter-based security approach, companies are now shifting towards a more robust zero trust approach, wherein the focus is not trusting anyone or anything, whether internal or external user, device, systems or networks. The only protocol to follow is to undertake authentication to establish validity of each access request.

Such as shift in security strategy is not easy to implement as it requires mindset change and often overwhelms the team. However, with technology changing rapidly and business environment being governed by dynamic socio-economic factors, it is important for enterprises to realize the importance of implementing zero trust strategy, in a gradual manner, to not only safeguard their organizations but also ensure sustainable growth over a period of time.

Further, implementation of zero trust may not need to be sudden. In fact, a well-thought out strategy should be formulated to deploy the approach with identity solution at its core. A roadmap to create the way ahead for such an implementation will help organizations reap the benefits at each phase in an easier manner.

Connect with our IAM experts to know how we can help in creating zero trust strategies and implement them with identity governance policies for your organization.

Sources:

- https://www.ssh.com/academy/iam/zero-trust-framework
- https://www.helpnetsecurity.com/2019/06/25/iam-zero-trust/
- https://blogs.manageengine.com/active-directory/ad360/2020/06/10/why-zero-trust-in-iam-is-the-new-way-forward.html
- A Practical Guide to A Zero Trust Implementation. Roadmap: The Zero Trust Security Playbook: Forrester report
- The Zero Trust eXtended (ZTX) Ecosystem. Forrester report

AVANCER'S EXPERTISE IN IAM

At Avancer, we understand that one of the compelling factors for organizations to bring in technical solutions is to adhere by existing compliances. However, there is so much more to technical solutions, and these add on benefits help in bringing efficiency, security and operational automation. We add an edge to solutions in Identity and Access Governance, IT Security and Big Data by closing any loopholes, and tailoring the solutions as per the needs of the business, industrial standards and regulatory considerations.

For more information on how we can make a difference in your organization, drop us a request here or directly contact our IT Security Leaders

RAJESH MITTAL, CTO| ARUN MEHTA, CEO|

Contact Us

Avancer Corporation
101 Interchange Plaza
Suite 201 Cranbury
NJ 08512, USA
Tel: +1 (609) 632-1285
Fax: +1 (877) 843-8594
Email: info@goavancer.com
Website: http://www.avancercorp.com/

To consult IAM Experts, click here.