ZERO TRUST PRIVILEGED ACCESS SECURITY REDEFINED WITH ARCON|PAM

Learn how ARCON|PAM adopts CARTA to help organisations build a secure framework around its most trusted privileged identities.
What’s common between the great empires and resilient IT ecosystems?

Great empires such as Roman and Greek survived and flourished for hundreds of years. Astute planning, resilient army and robust forts laid the foundation for some of the most mighty empires from ancient and Middle Ages. While at the helm, these empires more importantly observed strong internal controls and unambiguous state policies. However, it is said that most of these empires crumbled not because of a superior external force but because they failed to continuously assess and identify the internal threats (needless to say trust was always broken). A modern-day IT ecosystem is like any other empire. It will survive only when it has a security framework to defend both internal and external threats and the learning’s from the history should inspire us to continuously re-assess trust. Imagine the impact if at the center of the trust was the most important guard (like the guard of guards), which in the IT world are the privileged identities that hold the keys to the kingdom.

The one mistake that often leads to security disaster

The conventional security principles that once you are inside the fort you are trusted will be a colossal mistake in today’s IT environment. That all is well within the inner realm and the IT risks emanate only from outside the network is a misguided notion. The prime target of malicious actors, ‘privileged identities’, are like the holy grail of any organization. If compromised, attackers can reach the heart of the IT empire, DATA. The probability of data breach threat multiplies with every new privilege identity created in the IT ecosystem. With a vast number of database silos stored in servers and cloud resources, unprotected and unmonitored privileged identity can prove to be an organization’s nemesis. Unfortunately, organizations still maintain a conventional IT security approach. Much of the IT security investments are directed towards advanced network security solutions. Inside the perimeters, however, organizations seldom pay adequate attention to inculcate a practice of implementing robust security controls, especially around privileged identities.

If the user is trusted accesses are flat. Privileged passwords and privileged identities are shared, there is ambiguity over roles with regards to access, there is no fine-grained access control i.e. basic principle of security “need to know” and “need to do” basis is missing. The complexities are further high due to a large number of such digital or privilege identities.

It is now well established that protecting privileged identities is one of the most critical aspects of any security framework but to continuously assess the trust levels of such identities in today’s dynamic IT world is now a necessity considering these hold the keys to your DATA. Zero Trust frameworks have been a topic of discussion in the recent past i.e by default deny. In fact Zero Trust framework is the first step towards the more evolved Continuous Adaptive Risk & Trust Assessment (CARTA).

The Zero Trust Model is the initial step towards a roadmap to CARTA

Lately, there has been a lot of buzz around the Zero Trust security model. The Zero Trust is going mainstream with several banking and financial institutions, government organizations, among many other industries adopting it to mitigate data breach risks.

It is gaining wide-spread acceptability because it addresses one of the biggest IT challenges: identity security. Indeed, this model is a radical shift from a conventional perimeter-centric security approach to a unified data and identity-centric security approach. This is imperative in today’s context as enterprise data is widely dispersed across IT environments. To monitor which identity is accessing what, why and where is critical to assess the trust. A general framework of the Zero Trust model is that it never
assumes “trust” but continuously assesses it; this is echoed by CARTA, a new strategic approach for Information Security that assesses risk/trust continuously throughout the duration of the network interaction. Further, the Zero Trust model uses risk-based assessments by constructing micro-perimeters and micro-segmentations around dispersed identities. When this approach is applied, it provides greater visibility and analytics of identities present in every layer of IT infrastructure, ensuring better IT governance. It reinforces the inner realm of an organization.

**ARCON | PAM enables rapid deployment of CARTA framework around Privileged Identities**

One important factor why organizations trust ARCON to architect a Zero Trust and much evolved CARTA model is its raison d’etre, which is to unravel the difficulties arising out of managing a large number of privileged identities. We are here because we understand the pain-points of IT administrators and security professionals. By comprehending typical use cases arising out of privileged access control, ARCON has designed a best-in-class Privileged Access Management solution that assists an enterprise’s Zero Trust journey and more specifically the CARTA framework.

In order to move away from the practice of a large corporate perimeter security-centric approach which fails to define the limit of an identity, ARCON helps to build micro-perimeters around every identity. Each micro-perimeter is built with a set of unambiguous centrally built rules and roles, which defines the limits of an identity. This way, every identity in the IT ecosystem is granted access to systems, applications, data, and networks strictly on “need-to-know” and “need-to-do” basis -- a fundamental requirement to ensure robust IT governance. Secondly, for a Zero Trust journey to fructify, it must include a risk-predictive component within every micro-perimeter. A large number of suspicious identities go undetected for a long period of time if an IT ecosystem lacks security analytics and orchestration. ARCON | Privileged Access Management provides a proactive approach to mitigate the risk in real-time. Each and every identity underlying in the IT ecosystem is continuously assessed. Real-time alerts on risky behavior profiles ensure that risky identities are de-provisioned. It ensures the hygiene of the IT ecosystem.

Last but not least, securing data requires a well-established identity references for end-users accessing critical applications. In other words, to validate ‘what we know’ and ‘what we have’ is critical to protect the inner realm from unauthorized access.

**How does ARCON’s Predict | Protect | Prevent model enables the CARTA framework**

The CARTA framework echoes Zero Trust framework with an added focus on not just authenticating and authorizing access at the front gate, but continuously throughout the user’s experience through an adaptive, risk-based assessment to identify potential threats. One must follow Google’s BeyondCorp research which serves as the example of Zero Trust done right at a massive scale.

ARCON’s 2016 Predict | Protect | Prevent model was built on the premise that the detection and response model is way too expensive for organizations as the damage is already done. In several cases, organizations have not been able to recover from the massive damage done to the treasury or its reputation.

The key elements or foundation on which this model is based is to predict events before they happen so that we are able to respond or take adequate action in real-time. This model is heavily leveraged on the capabilities of AI/ML together with risk-based methodologies. It is on this model that our adaptive, risk-based continuous assessment of privilege identities is based on.

ARCON | PAM visualizes the Zero Trust/ CARTA framework through the following key enablers.
Continuous Adaptive Risk Assessment: This is an element that is embedded in every aspect of the solution. This is the ethos of ARCON’s Predict | Protect | Prevent Model. All enablers have an element of continuous risk assessment based on AI/ML technologies (Ver 8.5 U4)

**Enabler I: Establish TRUST**

Zero Trust, deny all until one is able to establish trust and trust cannot be established a longer by “what you know”. ARCON | PAM has high maturity when it comes to TRUST as one can configure various tests to be performed before Trust can be established. Establish trust not just on identity but various inputs like MFA, Adaptive Authentication, device, location and continuously monitor and assess the same using risk-based assessment methodologies.

A named user can’t access service until a sufficient level of trust is established (services are initially hidden from all users). Authenticate first, then connect.

The level of trust is established at connection time and is context-based including context such as device trust, user trust, location and time of day. The level of access granted is also context-based, granular (“precision access”) and configured for least privilege, typically to a specific application or service based on the user’s identity and role.

Some type of trust broker, controller or service validates the level of trust of the user and the device and communicates this to a gateway or agent that protects the service. At that point, an outbound connection is typically made from the gateway to the user (removing the need for inbound firewall rules, also significantly reducing the enterprise surface area for attack).
The basic principles of security are to provide access only on “need to know” and “need to do” basis. However, the world of technology, interconnected networks and the Internet were never designed with security in mind and one will not be surprised if these basic principles of security are not built into the systems or have not been configured. However, in this more complex world of distributed technologies, APIs and the advent of cloud technologies have further pushed us to consider the basics. Zero Trust Model echos these basic principles only with more rigour. Now if one were to look at the world of digital identities, privileged identities and machine identities these basic principles suddenly become the core foundations on which access will have to be governed. While the outer perimeter is vanishing one will now have to develop micro perimeters. Here is where ARCON | PAM offers a solution which is rapidly deployable.

If one were to apply the CARTA principles then the expectation is to ensure that while one is accessing the systems there is a constant monitoring of whether what is done is right. This is echoed by the ARCON Predict | Protect | Prevent Model, if the Knight Analytics is configured, it provides constant monitoring of who, when and what is being accessed as well as what activities are executed on the systems. This model leverages the neural and deep learning technologies and is able to highlight any alimony in real near time.
Enabler III: Secure Segmentation of Network

Secure Segmentation of Network/Micro-Perimeters, this is the most interesting and difficult task as privileged identities by their profile have direct and unlimited access. However, in today’s dynamic IT environment this too has to be limited considering resources and data face threats from various corners. What jeopardizes the data security in today’s IT environment is that organizations’ perimeters are turning segmented. They are no more static in the age of digitalization. Day-to-day administrative and critical tasks are conducted by “trusted identities” from outside of the traditional realm using DMZ instances, and/or VPN access. As a result, devices, users, services have multiplied in the wake of the rising number of mobile and remote workforce. Not only that, unmanaged machines and unmanaged users have proliferated as data workloads are migrated to managed service providers (MSPs) and cloud IaaS platforms. In the backdrop, where a good number of systems and services are accessed from outside of the conventional perimeter -- the old adage “inside means trusted” and “outside means untrusted” has become defunct. “Trusted identities” are probably more outside the network than within the network, thus, managing workloads from both within and outside the realm calls for a careful segmentation of “trusted identities”.

ARCON | PAM uses the network overlays, network encryption, software-defined Perimeter (SDP) and host-based agents to achieve network segmentation and micro-segmentation.

This is a secure gateway with network encryption or application streaming gateway approach to ensure network segmentation. The below diagram is a client-initiated ZTNA. The latest release of ARCON | PAM also enables a Service Initiated ZTNA (Zero Trust Network Access).

The SDP approach used to create micro-segmentation and is unique in the sense that multiple perimeters as well as combination of these are possible in as is seen in the diagram above. Access to IT kingdom is not only based on identity but also on other attributes and context such as IP address, device used, geographical location, time and date. The security model ensures better monitoring of identities and operational flexibility.
Opening applications and services to collaborative ecosystem members’ example: channels, suppliers, outsourced support, managed service providers and remote users in the cloud without requiring a VPN or DMZ. In the above case, access is tightly coupled with various unique elements including a combination and on the target side; this can be further based on unique elements such as Privilege Ids, Location and Devices or Systems.

**Enabler IV: Robust Detection and Response**

ARCON | PAM offers a robust detection capabilities in the form of session monitoring with textual context and commands executed on various systems. This is linked visually as who when and what. Sessions have HD quality screen grabs or videos and the text or commands are embedded in these sessions which can then be searched easily for monitoring, detection or forensic purposes. The solution offers capabilities of real-time alerts based on detection rules.

The detection capabilities have been further improved with the AI/ML based Knight Analytics which provides predictive capabilities and identifies early any anomalies or threats. A threat event can be easily monitored in real-time through the real-time session monitoring features which have added capabilities of offering a response such as warning, isolating the session by freezing the session or instant disconnection.

**Visibility & Automation**

One of the key outputs of the enablers is to increase visibility and enable automation in the life cycle of the digital or privilege-ids. ARCON believes real-time analytics using AI/ML and high automation will help Predict | Protect | Prevent targeted attacks and data threats.

**Conclusion**

The CARTA security model holds a lot of relevance today. As enterprise data is widely distributed in a shared, hosted and virtual environment, some of the most dreadful security vulnerabilities arise from a compromise of identities. Traditional security perimeters, built on the premise of “assumed trust” are no more adequate to manage and monitor identities. Instead, today it is imperative to have a process in place that provides continuous assessment of the trust. ARCON | Privileged Access Management provides security leaders with best practices that ‘defines’, ‘limits’ and ‘inspect’ identities continuously. The solution helps security leaders to build a resilient security framework around the most ‘trusted identities’.

Source: ARCON
About ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.

UBA: ARCON | User Behaviour Analytics (UBA) enables to monitor end-user activities in real time.

SCM: ARCON | Security Compliance Management (SCM) allows an enterprise to prioritize security and compliance efforts based on risk level. The tool enables continuous risk assessment for critical technology platforms and ensuring desired compliance levels.

PAM: ARCON | Privileged Access Management (PAM) is a highly effective solution that helps in managing, controlling and monitoring privileged user activities. The solution provides IT security team with a centralized policy framework to authorize privileges based on roles and responsibilities ensuring rule-based restricted access to target systems.

Corporate Headquarters
- 901/902, Kamla Executive Park,
- Off Andheri-Kurla Road, JB Nagar, Andheri (E),
- Mumbai - 400059
- Maharashtra, India

Email: info@arconnet.com

www.arconnet.com