Why is there an urgent need for secure remote access?

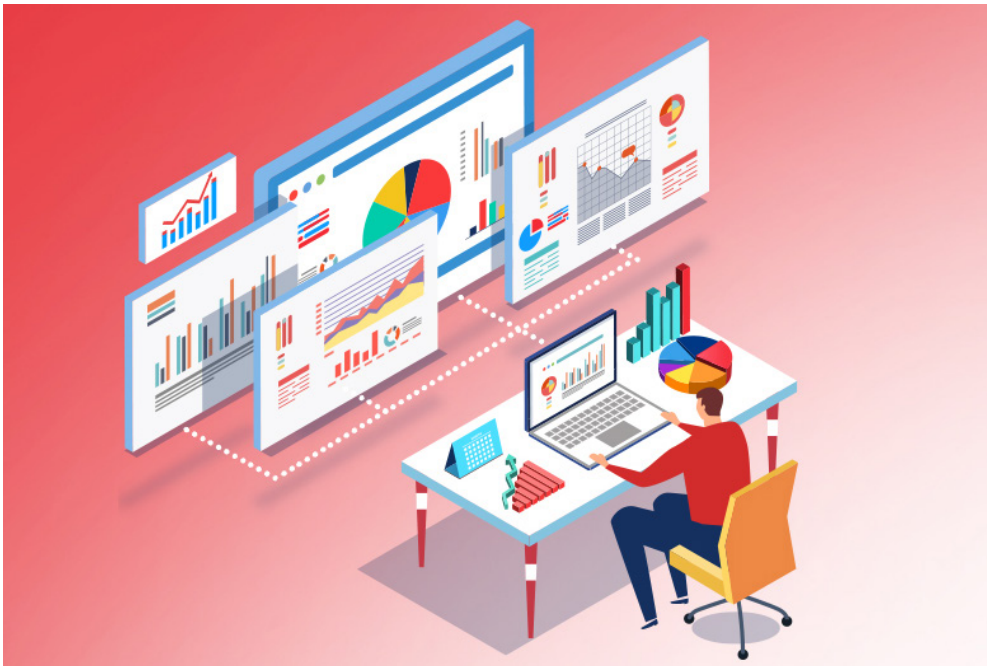


Table of content

Foreword

The novel Covid-19 disease has become a pandemic. With every passing day, businesses are facing increasing operational, administrative and financial pressure. Business Continuity Plans are at stake due to supply chain disruptions and workers absenteeism as Coronavirus has forced governments, businesses and individuals to self-isolate and maintain social distancing. In this critical juncture, companies across the world are compelled to ask their workforce to stay quarantined and work remotely.

However, if companies are not mindful of what the remote workforce is doing with confidential information/data that they are handling, the possibilities of serious IT crimes such as data breaches, credential abuse, and data exfiltration can go unnoticed. Therefore, learning and predicting risky user behavior patterns is central if your organization has to implement productive and secure work-from-home culture.

Don’t let your enterprise’s business continuity plans get disrupted

Scenario a: Work-from-home (WFH) directives in the backdrop of pandemic

The global lockdown as a result of the coronavirus pandemic has forced millions of employees to work-from-home. For an average medium sized firm, hundreds or thousands of remote users are accessing systems remotely. It sounds pleasing. WFH ensures business continuity whilst employees do not have to rush to offices, can do tasks with their Tee shirts and shorts on and favorite coffee in hand. However, this WFH initiative can become a nightmare, if systems to which employees interact are not monitored. Yes, indeed, even in these extraordinary circumstances, IT security cannot be taken for granted. Coronavirus could bring in more serious repercussions to an organization, if access to systems are not controlled and governed.

Scenario b: WFH culture for productivity enhancements in the normal course

Much before the forced WFH scenario came into the equation, employers were happy to implement it in the normal course given the productivity enhancements it may bring to an organization. Be it multinational corporations, start-ups and scale-ups, organizations of all shapes and sizes have been allowing WFH to implement a flexible work culture.

However, any malicious corporate insider or compromised third-party element can wreak-havoc on your organization if systems are accessed with no rule and role-based policies. It incentivizes corporate insiders and compromised third-parties with malicious intent to abuse credentials and make unauthorized access to systems.

Scenario c: Distributed and segmented digital identities

What threatens IT infrastructure of a modern-day enterprise is the distributed and segmented nature of digital identities. Day-to-day IT administrative tasks are conducted remotely and confidential information is accessed using Virtual Private Network (VPN) access or Demilitarized Zone (DMZ) instances. Consequently, the number of privileged tasks and privileged identities are multiplying so are the users, services and mobile workforce with privileged entitlements. Secondly, unmanaged machines and unmanaged users have increased manifold as organizations migrate IT workloads to managed services and cloud. Who is accessing confidential information? What has been accessed? Why has it been accessed? When was it accessed? -- are some of the critical questions that need to be answered if IT security and risk management wants to ensure a stable and secure IT ecosystem.

ARCON Remote Access : Enhance IT security and ensure Business Continuity

It is fairly evident from all of the scenarios mentioned above that organizations require a robust IT security mechanism to manage, control, monitor remote access. With WFH norm becoming universally accepted, IT risk management team will have to be more agile in establishing 'Trust' continuously. ARCON has a high-level of capability when it comes to configuring various tests to establish trust on the remote user. A host of features such as MFA, which includes Adaptive Authentication, granular level control, just-in-time privileges, and continuous assessment of trust using risk-based scores on risky behavior profile provides organizations with an added layer of security to protect confidential information.

ARCON ensures Secure Remote Access with these Robust functionalities

Unified Governance Framework:

ARCON provides a robust unified access control mechanism. The solution provides the IT security team with a centralized policy framework to authorize and govern the end users based on their roles and responsibilities. The solution offers rule and role based restricted access to target systems to ensure all access is made strictly on 'need-to-know' and 'need-to-do basis'. The solution enables the IT team to elevate privileges 'just-in-time'. It ensures security of all target systems whilst implementing the principle of 'least-privilege".

User Restriction and real-time monitoring:

Application Restriction and Elevation can be implemented to have better access control on end users working in different remote locations. Furthermore, Dash boarding can assist in investigating anomalous behavior of the users in real-time.

SSO access to elevate privileges:

Remote end-users can be granted elevated access rights to critical applications as and when required. The tool offers end users Single-Sign-On (SSO) access to privileged sessions. As a result, ADMINS don't have to share privileged credentials with end users or the IT staff thus helping to follow the basic principle of least privilege or just-in-time privileges.

Secure VPN-less connection:

ARCON offers secure gateway with network encryption or application streaming gateway approach to overcome network segmentation of digital identities.

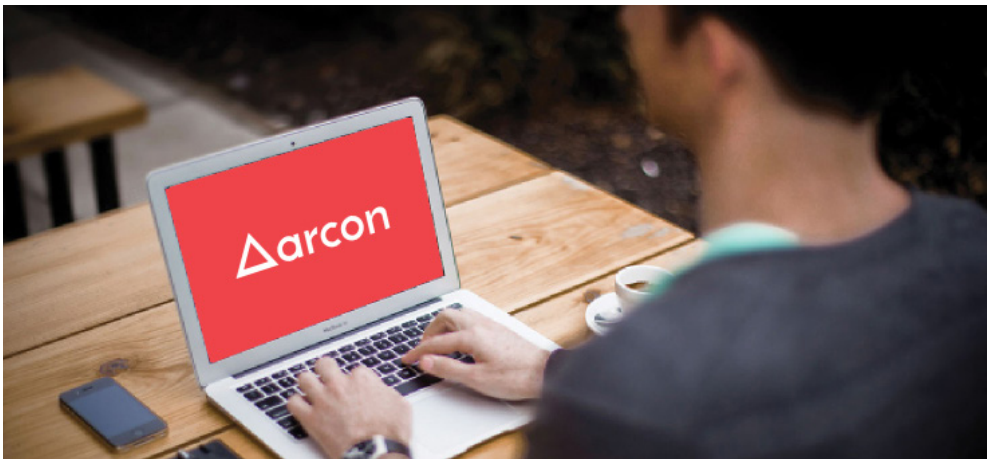
ARCON Knight Analytics:

Threat detection capabilities have been further enhanced by ARCON Knight Analytics. Access data is analyzed by this engine to detect, predict and display evolving threats, risky patterns, and suspicious remote behavior profiles.

Conclusion

The WFH model is widely adopted today by global organizations. Although it significantly improves employees' productivity, the threat to IT assets is expanding. Attacks on confidential information/data is imminent if organizations fail to keep a check on risky behavior profiles accessing systems remotely. ARCON provides a security and risk management team with a robust security mechanism to manage, control,and monitor remote IT users.

About ARCON



ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management

Connect with us