Best Practices for Endpoint Security and Management

Enterprise Risk Management pros faced a stiff challenge to ensure business continuity following the disruptions caused by the pandemic. Moreover, Information Security vulnerability increased as businesses altered their IT operations and administrative tasks to adjust to the new normal. Among many challenges, remote access posed all sorts of risks associated with data security and privacy. Therefore, Endpoint Security and Management became a pivotal point in the overall enterprise access control framework. In this whitepaper, ARCON discusses best practices to mitigate threats arising from unmonitored and unmanaged endpoints.

Table of content

Overview

There is an increased need to protect endpoints from security vulnerabilities. In the midst of digital transformation, the enterprise IT infrastructure is getting bigger. The workforce constantly requires access to files, applications, databases, and servers that could be located anywhere--on-cloud or on-premises.

Therein lies the security challenge. Endpoint represents the weakest link in IT infrastructure security. Whether a malicious insider or advanced cyber-criminals; they all look to target vulnerable endpoints to enter the network and execute attacks.

Consequently, against the backdrop for increasing number of endpoints and remote access use-case instances along with growing BYOD/BYOPC culture, endpoint security demands utmost planning and preparedness.

The threats of endpoint privileges misuse, application abuse, data exfiltration, ransomware execution among other forms of IT incidents can be mitigated with proper monitoring and management of endpoints.

The Changing Endpoint Security Landscape

Earlier organizations used to typically bank on antivirus software and firewalls to mitigate endpoint threats in their infrastructure. Nevertheless, in the wake of more organized endpoint attacks, these tools are no more adequate from a security perspective.

Today's organizations have to gear up against advanced cyber threats that include social engineering, insider threats and ransomware. Consequently, more and more organizations are adopting highly advanced automated hunting, detection and remediation tools to monitor and collect log data from endpoints (EDR) and (XDR), for collecting data beyond endpoints such as network devices.

However, endpoint access control management continues to be a largely unattended area. If any unauthorized end-user tries to access critical business data, organizations can suffer breaches if they do not have any foolproof solution that could scrutinize who is doing what with the endpoints.

Endpoint Access Control and Management

A robust Privileged Access Management (PAM) and Identity & Access Management (IAM) solution helps organizations to govern, control and audit every access to critical systems. The objective of these practices is to monitor and manage every digital identity's interaction with critical systems such as databases and servers.

However, there could be applications running in the IT environment that are not aligned to the role and rule-based policy. Endpoints in such cases provide easy access to mission-critical applications. Those endpoints, in turn, could lead to IT catastrophe if accessed by unauthorized or malicious end-users.

Endpoint Access just like Privileged Access or Identity Governance and Management demands careful organization around people, roles and responsibilities. The endpoint security vulnerability could be mitigated significantly when organizations define end-user access policies, adopt a unified endpoint access control framework and implements endpoint privileges on-demand.

Likewise, end-user behaviour analytics has become a crucial component of endpoint security. Many IT frauds, zero-day threats including insider attacks happen when organizations fail to act on malicious end-users in a timely manner. A robust User Behaviour Analytics solution leverages AI/ML capability to identify risky behaviour profiles that deviate from configured/mandated baseline activities. Potential risks could be mitigated in a timely manner when behavior analytics solution provides alerts on suspicious end-user profiles.

All in all, endpoint access control and management help to reinforce the overall Identity Governance and Management framework.

Best Practices in Endpoint Security and Management

IT Risk Management teams would find merit in implementing the best practices in Endpoint Security and Management as it significantly reduces endpoint attack surface. In the table below, 10 time-tested best practices have been discussed.

Security Approach	Benefits	Solution
Unified Endpoint Access and Governance Framework	This approach enforces a centralized policy to govern all end-users. A unified engine defines usage policy. It ensures compliance and data security as Unified Endpoint Access Framework fosters rule and role-based access to endpoints.	ARCON | EPM offers centralized engine to govern the end-users by role-based access control and rule-based endpoint access
Prioritized Profiling	This approach enables IT security staff to systemically grant access to end-user based on the job profiles of end-users. Access Priority is determined/set by IT admins	ARCON | EPM offers priority-wise profiling-keeping data assets safe and secure
Application Security	Very often, malicious applications run in the IT environment. These applications pose serious threat to data integrity. Application Security enables IT security staff to blacklist harmful applications	ARCON |EPM has the ability to enforce application blacklisting
User Behaviour Analytics	Leverages AI/ML to solve a range of distinct use-cases related to end-user behaviour monitoring and data exfiltration	ARCON |UBA detects end-user behaviour anomalies and profiles that deviate from configured baseline activities The solution helps to set mandates for end-user baseline activities from IT productivity enhancements perspective as well The solution also offers facial recognition capability for strengthening the authentication mechanism and mitigate IT frauds

Security Approach	Benefits	Solution
Endpoint Privilege Elevation on-demand	It enforces the least privileged principle and ensures privileged elevation on-demand to business-critical applications	ARCON |EPM provides privileged elevation on-demand to protect the endpoints and data The solution ensures controlled endpoint privileged elevation in remote and work-from-home environments as well
Fine-grained End-point Access Control	It helps to regulate end-users access to critical applications based on time, day, duration etc.	ARCON | EPM enforces time-based, day-based, duration-based access among other parameters to ensure endpoint granular access control
Dashboarding, reporting and audit trails	Investigating abnormal incidents and timely response to threats get simplified with immediate alerts on Live Dashboards along with all-encompassing reporting mechanism and audit trails along	ARCON | UBA enables to keep control over operations, governance and compliance requirements ARCON | UBA's dynamic report allows management to keep a real-time track on technical observables such as unusual working hours, misuse of privileged access, anomalous network service usage, printing activity and so forth ARCON | EPM ensures that audit trails are maintained of each and every endpoint privileged activity and the reports are generated for the audit purpose and confirms compliance with the IT standards
Data Loss Prevention (DLP)	DLP ensures that no compromised end-user can use any removable storage device like USB port or external hard drive to misuse or exfiltrate the confidential business data	ARCON | UBA offers USB restriction capability to prevent compromise of sensitive data UBA ensures copying of any sort of information/file from the endpoint to USB/ external hard drive and (vice versa) is restricted

Security Approach	Benefits	Solution
Just-in-time Privileges	It ensures that only the right end-user has access to right endpoint at the right time	ARCON |EPM enforces just-in-time privileges—keeping customers' data protected It fosters the practice of granting access based on 'need-to-know' and 'need-to-do' principle
Enhanced Admin and User Experience	Ensures IT efficiency and end-user productivity	Both ARCON | UBA and EPM provides a very enhanced end-user UI dashboard ARCON Remote Assist is an effective IT solution that enables administrators to manage any on-boarded desktop either remotely or in the network. Remote Assist enables IT admins to troubleshoot any machine within and outside the network

Conclusion

Implementing the best practices in endpoint security and management ensures:

1. Reduced threats from compromised insiders, data exfiltration and credentials abuse
2. Compliance to IT standards and regulatory mandates
3. Organizations around end-users, processes and policies
4. Enhanced IT efficiency and end-user productivity
5. Unified governance framework

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.

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.

UBA: ARCON | User Behaviour Analytics (UBA) is a highly effective risk predictive & analytics tool built for daily enterprise use cases. It breaks the traditional approach of 'restrictive' access and is capable of crunching large lakes of enterprise data, spot anomalous activity and trigger alerts 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.

Connect with us