Admin By Request EPM: 20 Key Points Of Difference Over Other EPM Solutions.

Admin By Request

WHAT SPECIFIC CHARACTERISTICS AND FEATURES GIVE ADMIN BY REQUEST EPM A CLEAR ADVANTAGE OVER OTHER SOLUTIONS?

The following features and capabilities are valuable to consider when presenting Admin By Request EPM to customers exploring various EPM solutions.

Admin By Request stands as the only product currently available that includes ALL of these features and functionalities, even in its FREE PLAN.

PORTAL SECURITY STANDARDS & COMPLIANCE

PORTAL SECURITY STANDARDS & COMPLIANCE

Admin By Request meets the very highest international data security standards for data storage:

- ISO/IEC 27001
- SOC 1, SOC 2, and SOC 3 (Service Organization Controls)
- HIPAA/HITECH
- FedRAMP (Federal Risk and Authorization Management Program)
- PCI DSS (Payment Card Industry Data Security Standard)
- ISO/IEC 27018, GDPR (General Data Protection Regulation)
- CSA STAR (Cloud Security Alliance Security Trust & Assurance Registry)
- ISO/IEC 22301, ISO/IEC 27701
- NIST 800-53
- CIS Benchmarks
- HITRUST CSF
- EU Model Clauses (Standard Contractual Clauses) Facilitates secure data transfers outside the EU.
- IRAP (Information Security Registered Assessors Program)

FURTHER DETAILS:

Admin By Request is built on Microsoft Azure SQL, the most compliant and secure implementation of MS SQL Serer available. Evidence available here https://learn.microsoft.com/en-us/azure/azure-sql/database/security-controls-policy?view=azuresql

PASSWORD-LESS APPROACH

PASSWORD-LESS APPROACH

Admin By Request EPM does not store or handle ANY user passwords.

FURTHER DETAILS:

Admin By Request does not store or handle any AD/Entra ID user passwords, either on the endpoint agent or in the portal.

Admin By Request
ZERO TRUST PLATFORM

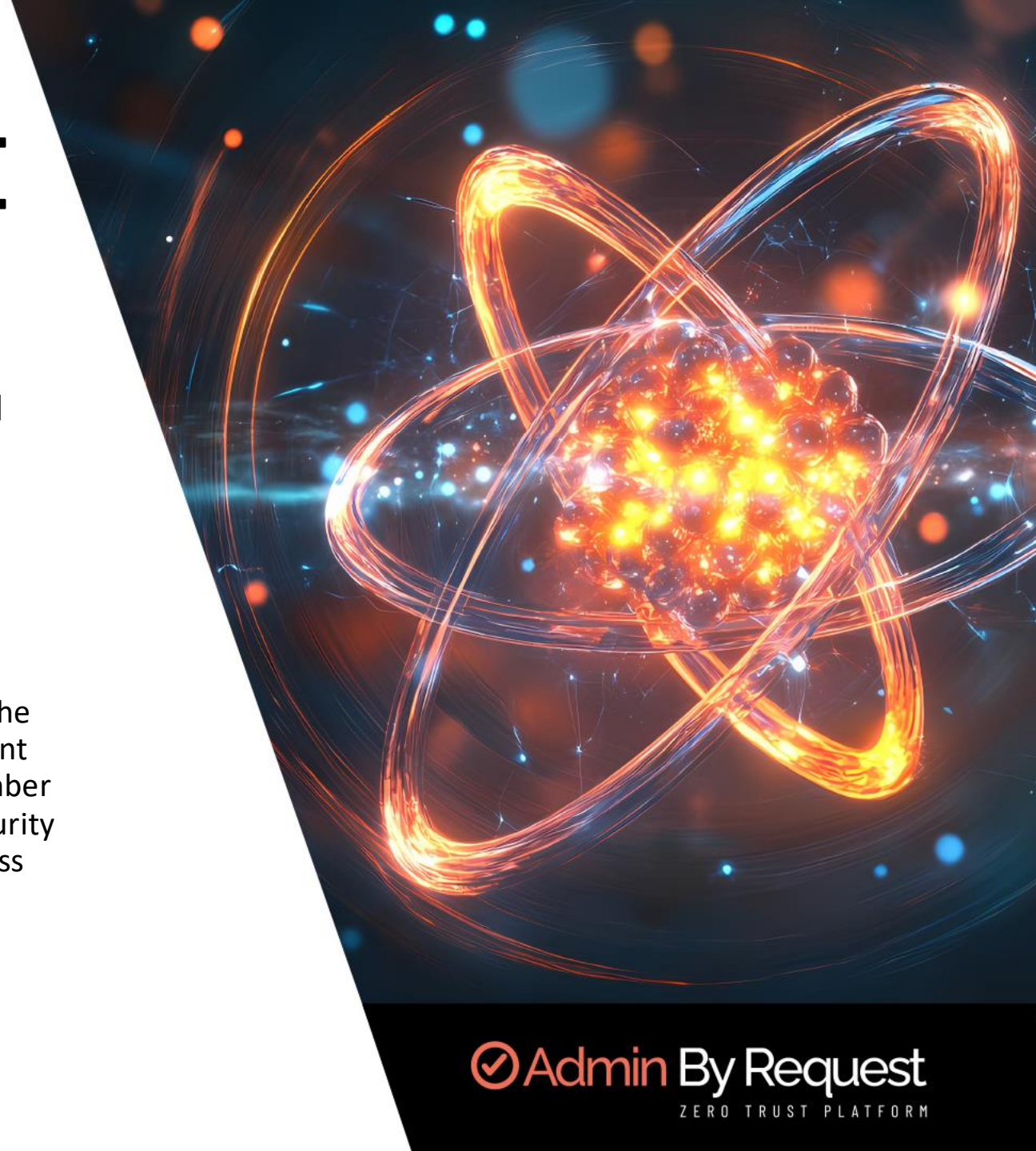
AGENT INSTALLER SIZE < 3MB

AGENT INSTALLER SIZE < 3MB

Admin By Requests OFFLINE installers do not exceed 3MB in size.

FURTHER DETAILS:

In today's world of bloated, oversized software installers, the tiny size of Admin By Request makes automated deployment rapid, even on the slowest networks. Due to the small number of files that make up the solution, there is a significant security advantage in that the attack surface of the product is far less than any competitive solutions.



UNMATCHED SECURITY RECORD

UNMATCHED SECURITY RECORD

Admin By Request has had ZERO CVEs (Common Vulnerabilities and Exposures) reports in the last five years.

FURTHER DETAILS:

No CVEs have been lodged against Admin By Request in the last five years despite having millions of installed endpoints globally. In the history of the product to date, only two CVEs have been lodged against Admin By Request (January 2020). Both issues were addressed in under 24 hours of being reported to us.

Evidence of this can be found in the CVE database found here:
https://notcve.org/search.php?query=product%3A%22Admin+By+Request%22

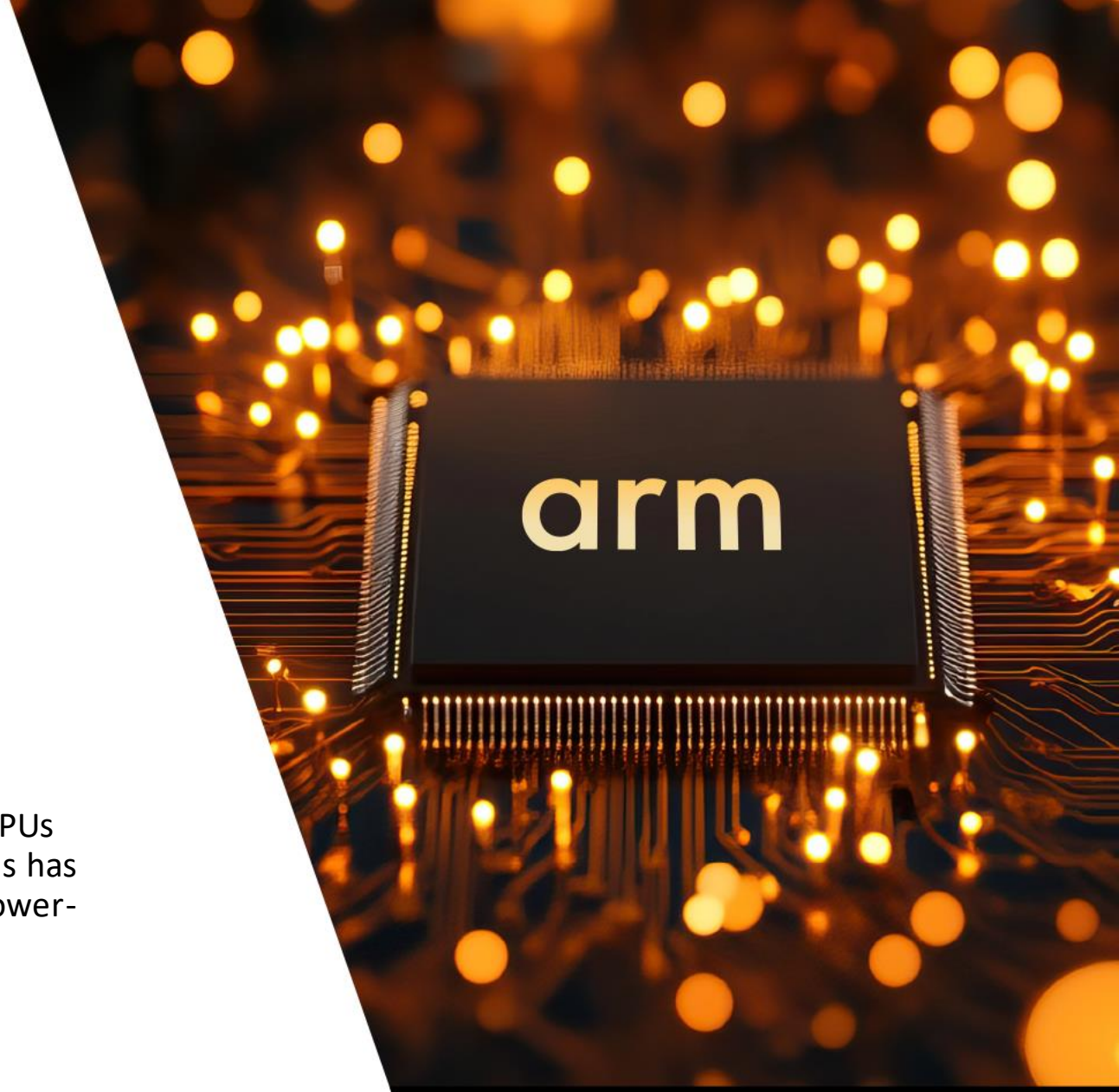
CROSS-PLATFORM ARM CPU SUPPORT

CROSS-PLATFORM ARM CPU SUPPORT

Admin By Request EPM Workstation supports ARM CPUs on both Windows and Mac based systems.

FURTHER DETAILS:

Admin By Request EPM for Windows has supported ARM CPUs since version 8.5, Demand for Windows-based ARM systems has been steadily growing as customers look for smaller, less power-hungry devices with both performance and endurance.



Admin By Request
ZERO TRUST PLATFORM

BUILT IN MULTI ENGINE REPUTATION SOLUTION (OPSWAT META DEFENDER)

BUILT IN MULTI ENGINE REPUTATION SOLUTION (OPSWAT META DEFENDER)

Admin By Request includes (at no extra cost) a real-time multi-AV engine file reputation checker in OPSWAT Metadefender.

FURTHER DETAILS:

Admin By Request EPM ships with OPSWAT Metadefender integration built-in at no extra cost. This solution does not conflict with any installed A/V or EDR solution; instead, it references an aggregate repository of file reputation populated by up to 35 anti-virus vendors. The lookup is performed in real time as part of the file elevation process and consumes virtually no system resources.

Admin By Request
ZERO TRUST PLATFORM

< 1% ENDPOINT CPU UTILISATION

< 1% ENDPOINT CPU UTILISATION

Admin By Request uses negligible amounts of CPU on the endpoint for average daily use. No more than 1% endpoint CPU is typically consumed.

FURTHER DETAILS:

Our testing shows sub 1% CPU utilisation for typical average use. This is in stark contrast to most competing solutions, which are extremely resource-intensive and dramatically impact the user experience. This is one of the major reasons why developers favour Admin By Request.

‘ALL YOU CAN EAT’ FEATURES

‘ALL YOU CAN EAT’ FEATURES

Admin By Request EPM Workstation has only one SKU, which includes all existing and all future features of the solution. There are no paid add-ons, modules, extensions, or features.

FURTHER DETAILS:

Admin By Request is just as easy to buy as it is to use. There is no confusing list of options or annoying tiers which require you to upgrade to use specific features. For a price, you only need to know how many endpoints you need to license and the duration of the term. All features and support are included. It's as simple as that.

JUST IN TIME = REAL TIME

JUST IN TIME = REAL TIME

Approve / Deny notifications appear on the end user's desktop in real time (<1 second) from approval.

FURTHER DETAIL:

Admin By Request uses advanced IoT technology to send immediate approval response notifications to end users in real time (sub 1 second). The same technology is also used in our Break Glass solution, enabling Break Glass accounts to be delivered to endpoints instantly.

Admin By Request
ZERO TRUST PLATFORM

IN PROFILE CONTEXT SWITCHABLE POLICIES

IN PROFILE CONTEXT SWITCHABLE POLICIES

Helpdesk staff can perform instant ‘context switching’ of Privilege Management policies from within the end users' OS profile to necessitate a ‘Zero Trust’ approach to IT support that requires all support-invoked privilege elevations to be fully audited by the EPM.

There is no need for IT support to disable/bypass the EPM to perform their duties.

FURTHER DETAILS:

This capability is possible using Admin By Requests ‘Support Assist’ feature and can be found on both Windows and Mac agents.

NETWORK LOCATION WHITE LISTING

NETWORK LOCATION WHITELISTING

IT / Security teams can create read-only network shares of safe applications and installers and be able to present these drives / shares to users as ‘safe repositories’ where nonprivileged users can ONLY run those applications with the required admin privileges.

FURTHER DETAILS:

This capability was available in the very first version of Admin By Request. The specific feature is “Run As Admin location pre-approval (all files in folder tree)”

Admin By Request
ZERO TRUST PLATFORM

TIME LIMITED PRIVILEGE GRANT

TIME LIMITED PRIVILEGE GRANT

Users can be granted a predetermined amount of time, either through approval or via a PIN code, to perform allowed privileged elevation actions.

The time-limited session can be granted to both online and offline users and respects reboots (continuing after a reboot).

Blocking policies are also adhered to while the session is active.

FURTHER DETAILS:

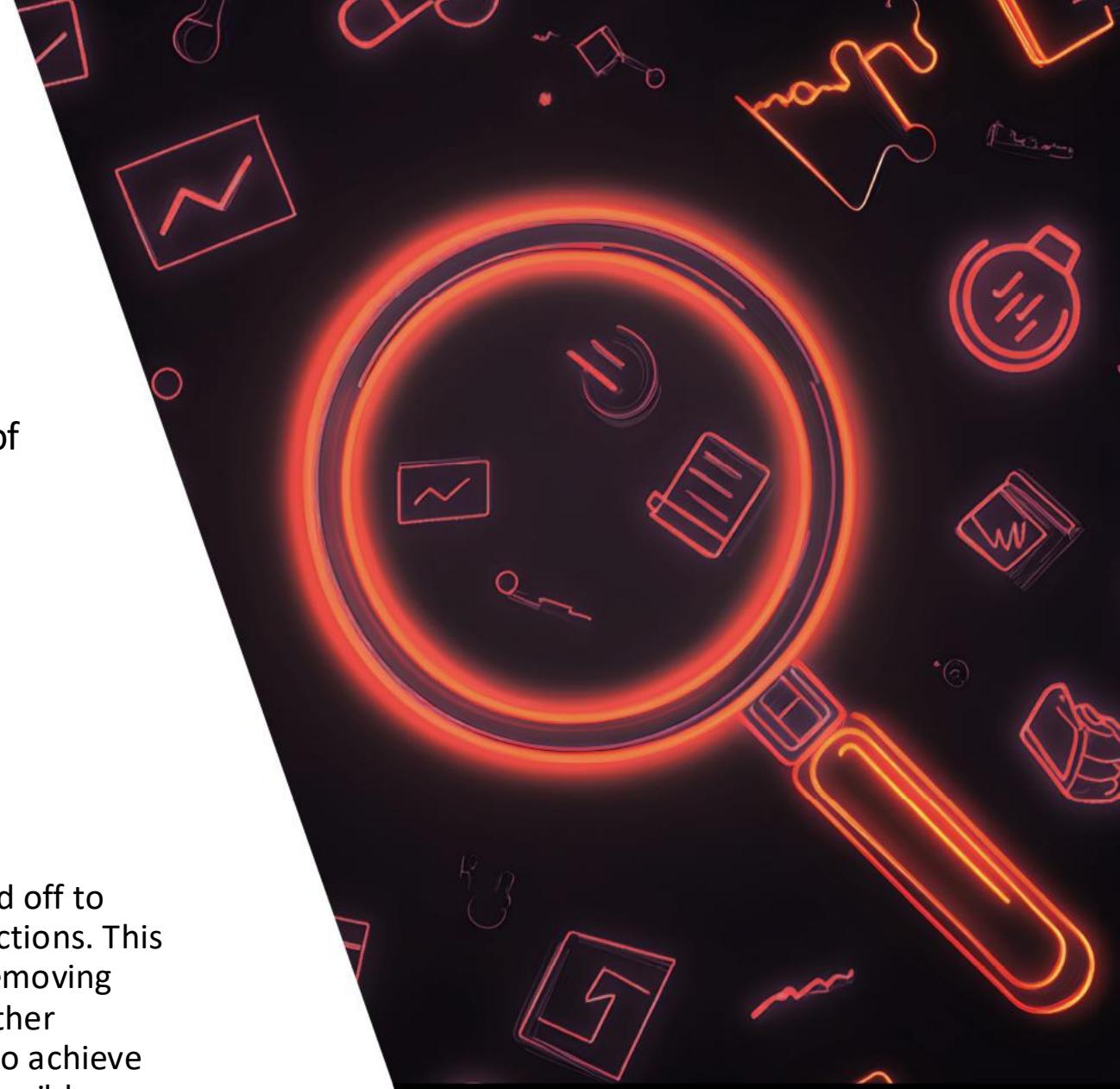
This capability was available in the very first version of Admin By Request. The specific feature is “Admin Session”. Configured blocking rules are still respected when an Admin Session is being used, as is the OPSWAT Metadefender protection. The use of Admin Sessions is, therefore, still highly controlled and safe.

PRE-POLICY RECONNAISSANCE

PRE-POLICY RECONNAISSANCE

Admin By Request records privileged elevation use of users with permanent admin rights to perform detailed auditing of admin rights use before admin rights are removed.

During reconnaissance mode, the user ‘full admin’ experience is not altered in any way.



FURTHER DETAILS:

Deploying Admin By Request with the revoke feature turned off to users with existing Local Admin Rights audits all elevation actions. This is useful to understand Admin Rights usage better before removing them and applying policies. Doing this results in a far smoother transition from full admin to granular admin, enabling you to achieve full user acceptance. Pre-Policy Admin Reconnaissance is possible on both Windows and Mac agents.

Admin By Request
ZERO TRUST PLATFORM

NON-PRIVILEGED ACCOUNT SEPARATION

NON-PRIVILEGED ACCOUNT SEPARATION

Admin By Request is configurable in such a way that users can be forced to use a separate non-privileged account for EPM use, other than the account they logged in with.

FURTHER DETAILS:

The ‘Account Separation’ feature was introduced in Admin By Request version 8.5 and can be a requirement in some implementation scenarios/compliance standards such as UK Cyber Essentials Plus.

USER > HARDWARE FUSING

USER > HARDWARE FUSING

Admin By Request contains functionality that ‘fuses’ a user to a specific hardware asset so that only that designated user can perform EPM functions on that fused computer device.

There is a simple, one-button action for designated portal administrators where they can perform immediate pairing/unpairing of the user to/from the hardware.

FURTHER DETAILS:

With the Admin By Requests’ Device Owner feature, non-privileged users are automatically ‘fused’ to their hardware when Admin By Request is deployed. When ‘Owner Blocking’ is enabled in the portal, users who are not the owners of their hardware are blocked from using Admin By Request and instead presented with a PIN code.

INTUNE COMPLIANCE INTEGRATION

INTUNE COMPLIANCE INTEGRATION

Admin By Request contains functionality that blocks use of the EPM if the hardware they are using fails Intune compliance tests and becomes non-compliant.

FURTHER DETAILS:

The feature is called ‘Intune Compliance Locking’ and can be configured for specific groups of users or computers. When enabled, computers that become non-compliant are not permitted to use Admin By Request EPM, instead presenting the user with a PIN code option.

AI BASED APPROVAL

AI BASED APPROVAL

Admin By Request can intelligently automate approvals for specific groups of users based on global vendor/application privileged elevation use. The Admin By Request databases, which are used for AI training, exceed 10M successful unique application elevations and are among the largest application intelligence databases of their kind.

FURTHER DETAILS:

Admin By Request AI approval automatically scores vendors and applications from a database of over 14 million applications. The AI Approval system can be configured (per policy) with a ‘score threshold, ’ the value the vendor or application must meet or be exceeded to bypass the approval workflow system.

UAC MODE SELECTION

UAC MODE SELECTION

Admin By Request EPM has three different UAC handling modes for standard EPM process elevation:

- A driverless ‘native’ mode using standard Windows UAC / Mac authentication prompts
- A user consent mode which requires the user to perform a simple interactive ’yes/no’ input
- A SAML 2 compliant MFA mode that requires the user to authenticate with MFA in order to perform EPM elevation functions.

FURTHER DETAILS:

Admin By Request can be configured (per user/computer group) for any of these three types of EPM elevation modes.

Admin By Request
ZERO TRUST PLATFORM

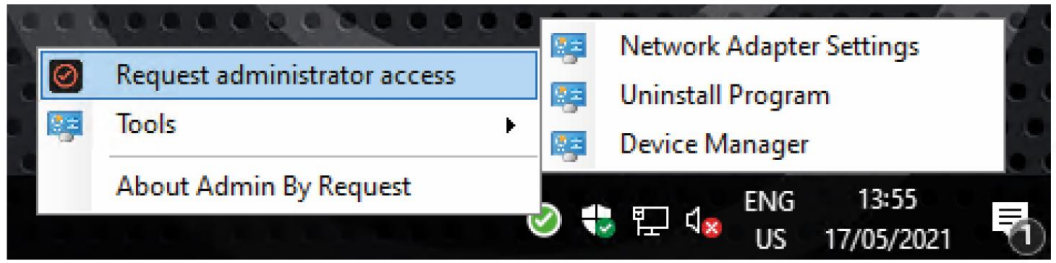
POLICY BASED SHORTCUT TOOLING

POLICY BASED SHORTCUT TOOLING

You can configure commonly used applications and URLs to be launched elevated / non-elevated from the Admin By Request ‘Tray Icon’ on the user's toolbar.

Different sets of tools should be configurable/presented to different groups of users.

Tools also dynamically change based on the Support Assist feature.



FURTHER DETAILS:

Admin By Requests ‘Tray Tools’ feature does just this. Tray Tools allow users to launch applications, elevated or non-elevated, or URLs from a menu in the Tray Icon.

INNOVATIVE, UNLIMITED POLICY LAYERING

INNOVATIVE, UNLIMITED POLICY LAYERING

The Admin By Request policy configuration methodology, ‘Sub Settings,’ enables portal admins to create more nuanced/layered configurations rather than simply assigning a single policy to a single group of users or computers.

Sub Settings can be used like ACLs or firewall rules, where an unlimited number of rules can be applied to multiple layers of groups of users or computers. Those rules can then be ’matched’ hierarchically on a ‘first setting, first match’ basis.

Settings are configurable in policies, which are selectable and overwritable from the configured global defaults.

There is a change log for all settings changes in the solution, showing who changed a setting, when, and what the setting was before and after the change.

FURTHER DETAILS:

Admin By Request’s Innovative Sub-Setting methodology is key to the solution's intuitiveness and long-term manageability. While other systems quickly become overly complicated as multiple rule sets accumulate, Admin By Request remains a pleasure to use, with configuration changes consistently yielding completely predictable outcomes.