sectona

DATASHEET

Endpoint Privilege Management

Revoke local admin rights, enforce the Principle of Least Privilege and deploy essential Endpoint Privilege Management measures across on-premises, hybrid & cloud environments.

Modern workforce challenges

Organizations face significant challenges when balancing user productivity and security, particularly in managing local admin rights. Granting users elevated privileges can lead to compromised security, while restrictive policies may hinder their ability to perform essential tasks. This creates a reliance on help desks for permission restoration, resulting in high support tickets that overwhelm IT teams. Additionally, the phenomenon of privilege creep emerges when users claim admin rights for urgent needs but fail to relinquish them afterward, increasing the risk of security breaches.

Privilege creep leads to the attack spreading out to other machines in the network, disrupting user productivity, and compromising IT Infrastructure assets. Furthermore, malware can exploit vulnerabilities without robust application control measures, leading to successful attacks that compromise sensitive data. Thus, organizations must find a balance between enabling user efficiency and maintaining stringent security protocols to mitigate these risks effectively.

Regulatory compliances mandate that passwords be managed across IT equipment, including endpoints, to ensure adherence to cybersecurity standards. EPM enhances this compliance requirement by reinforcing key security principles such as the following:

Zero Trust

Least Privilege

Limited Access

Assume Breach

How does Sectona EPM help address challenges faced by organizations?

Sectona's Endpoint Privilege Management (EPM) solution focuses on protecting endpoints and users from cyber threats, minimizing the risk of compromising an organization's IT infrastructure and reputation. By controlling and monitoring user and application privileges, enforcing the least privilege model, preventing unauthorized privilege escalation, and enabling early detection of suspicious activities, EPM effectively prevents and contains attacks at the endpoint level.

This proactive approach significantly reduces the risk of data breaches and ransomware incidents, allowing IT teams to focus on strategic initiatives rather than support tickets. With compatibility across Windows and macOS, EPM empowers organizations to maintain strong security measures without compromising user productivity. By automating privilege management and ensuring that only trusted applications are permitted to run, EPM effectively minimizes the attack surface and fortifies overall cybersecurity defences.

Critical Capabilities

Device Support

- macOS 13, macOS 14, Windows 10 ×64 bit, Windows 11

Application Control

- Effectively control and manage application access with static policies or adaptive learning mode.
- Continuously profile applications installed on endpoints.
- Streamline approval workflows and elevate applications based on user requirements.

Password Management & Device Security

- Effectively manage and control the usage of local admin rights.
- Securely store, rotate and manage local account passwords.

Discovery

- Thoroughly discover Windows domain, non-domain and Mac accounts.
- Continuously discover endpoints from AD hosted on-prem or cloud.

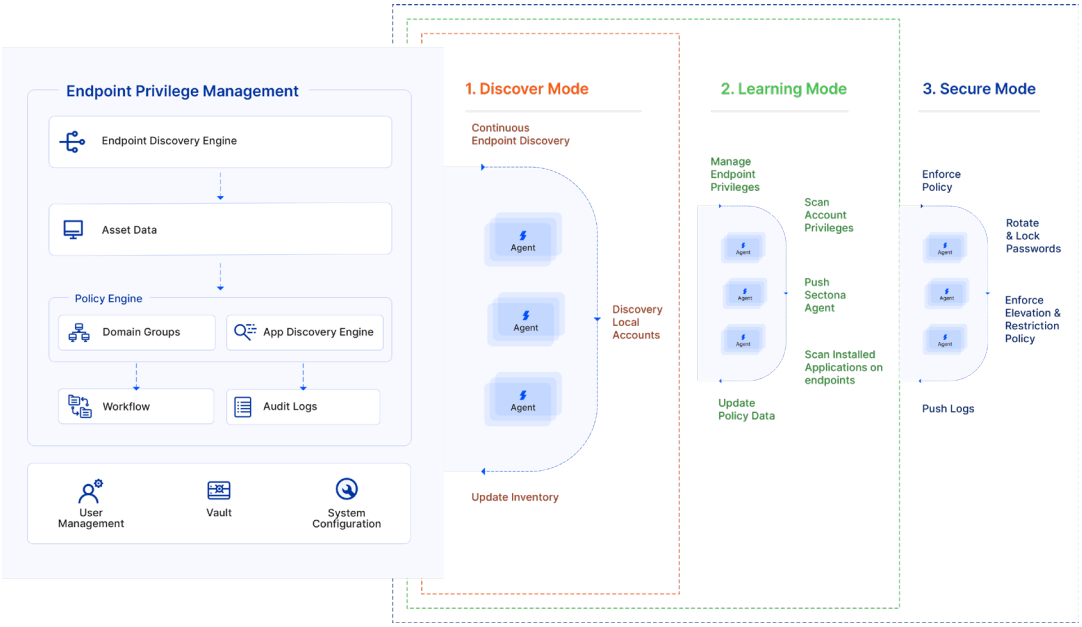
Integrations and Enterprise Grade Features

- Utilise robust and accessible public APIs.
- Ensure uptime with high availability and load balancing
- Integrate with active directory, service desk tools, SIEM, and syslog.

Auditing and Analytics

- Get detailed, auditable logs of activities performed by users for privilege elevation, applications accessed and rights used.
- Utilize customizable dashboards for insight-based analysis.
- Comprehensively audit user and group activity.
- Customize and automate activity report scheduling.

Sectona Endpoint Privilege Management works in parallel with the overall integrated Privilege Management approach built on a set of modular components. Endpoint Privilege Management is an integral part of the core Sectona Security platform.



Use Cases

Allow Users to Elevate Privileges On Demand

Security teams require a mechanism to remove standing privileges and allow users to elevate applications at runtime or during installation. With Sectona EPM, organizations can define trust-based policies to allow users elevated privileges on demand for accessing applications needing administrator rights.

Empower Users with Controlled and Need Based Administrator Access

Technical users like developers may require admin rights for installing specific applications for which they can request for administrator rights in Sectona EPM and request access for a defined time to perform administrative activities.

Continuously Monitor and Remove Administrator Rights

Sectona EPM helps users stay in control of administrator rights granted over a period and keep track of usage of local administrator privileges with special reports. Backdoor admins or admins created for temporary purposes can be removed through EPM services. Admins that are not part of the EPM local admin membership are removed routinely.

Empower Administrators with User Application Control

Admins can have full control over the applications users are elevating or requesting. Unknown applications simply cannot be elevated, and this enforces the least privilege in the true sense. With Sectona EPM, enable users to access trusted applications only and facilitate request-based access otherwise. Block unknown and risky applications on endpoints

Authorize Remote Workforce Access

As most of modern workforce is working remotely, remote access outside the LAN network or unstable internet connection is a common scenario. When a user wants to elevate privileges in such a scenario, they can contact the IT administrator and get a system generated offline code to gain the required privileges and perform the delegated task ensuring business continuity.

Sectona EPM Key benefits

Zero Trust Security

Manage or remove local and domain administrative rights and allow controlled application management across endpoints.

Centralized Policy Management

Control and manage policies from a centralized console to allow specific users access to applications on specific endpoints.

Prevent Malware and Ransomware

Reduce your attack surface and prevent lateral & vertical movement of threat actors by removing local administrator rights on desktops and endpoints.

Boost productivity

Dealing with vast volumes of devices and policies attributed to accounts and application access, EPM can help reduce help desk tickets by speeding up ticket resolution and empowering employees with necessary permissions on demand.

sectona

Sectona is a Privileged Access Management company that helps enterprises mitigate the risk of targeted attacks on privileged accounts spread across data centres and the cloud. Sectona helps secure dynamic remote workforce access across on-premise or cloud workloads, endpoints and machine-to-machine communication.

For more information, visit www.sectona.com and follow @SectonaTech on X (Twitter) or @Sectona on LinkedIn