sectona

Datasheet

Sectona Security Platform

A light, integrated approach to privileged management

Sectona Security Platform helps enterprises mitigate targeted attacks' risk to privileged accounts spread across data centers and the cloud. Sectona delivers integrated privilege management components for solving access challenges of modern dynamic workforce & machine to machine communication for modern IT infrastructure & endpoints spread across on-premises, virtual environments, or the cloud.

Sectona, with its light, integrated approach, provides a single console for securing passwords and secrets in an embedded vault, secure access with cross-platform access technology, and manage privileges over endpoints.

Manage privileges everywhere

Secure Passwords and Secrets with an integrated platform across endpoints, applications & workloads.

Scalable Session Management

Leverage cross-platform session management technology to manage sessions on endpoints, browser, or terminal server.

Build for Scale & Security

Deploy & manage the platform with embedded high availability options, modular components and, distributed architecture support.

Use Cases

Secure Remote Privileged Access

Isolate Privileged Sessions, Manage Complex access policies with Dynamic Grouping, Support users accessing from an unknown network

Remove Administrator rights

Lockdown Privileges on Endpoints, On-Demand Privilege Elevation, Stop unknown application execution

Secure Cloud Environments

Manage Identities & Authentication, Expedite On-boarding, Enable VPN-less Remote Access

Automate Entitlement Reviews

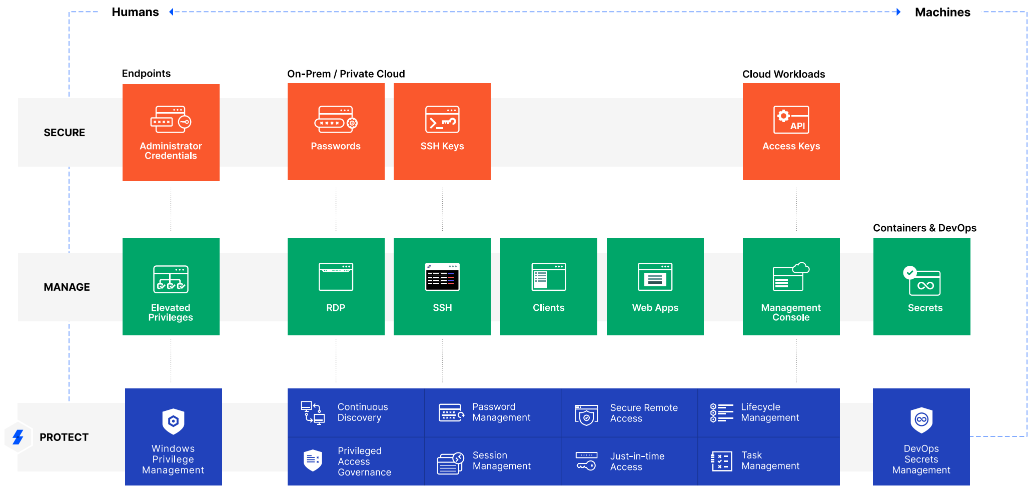
Centralized Monitoring of Allocation and Use of Privileged Access, Set Ownership of Critical Accounts

Simplify Privileged Access

Automated Provisioning of Privileged Accounts, Flexible Account Management Operations

Platform Overview

The Sectona Security Platform brings together elements to secure privileges on growing attack surfaces for organizations. Tight integration across the platform for IT operations, security, and governance teams deliver consistent security privilege management across cloud, virtual, and endpoints. The Complete platform developed from the ground up, integrated by default for incredible ease of use, simpler administration & operations.



Platform Capabilities

Address dynamic needs & challenges with simplicity & scale with an integrated platform & capabilities. The Sectona Security Platform consists of Core Capabilities to address Password Management, Session Management for IT Operations & Security teams. Advanced capabilities targeted for Governance, endpoint privilege management, and DevOps scale easily extend privilege management to governance teams and extended attack surfaces.

Core

Continuous Discovery

Secure and Control newly added assets and hidden privileged accounts.

Password Management

Robust Password Vaulting to secure privileged Identities and SSH Keys.

Secure Remote Access

Enable VPN-less Remote Access for Modern Workforce.

Session Recording & Threat Analytics

Advanced session monitoring for all privileged activities with risk-profiling & behavior-based analytics.

Multi-Factor Authentication

Neutralize the risks associated with compromised credentials using a broad set of mechanisms.

Just-In-Time Access

Remove standing privileges and leverage a combination of approaches to implement JIT policies.

Privileged Task Management

Automation of privilege assignment and usage.

Account Lifecycle Management

Streamlines lifecycle management of privileged accounts and groups across heterogeneous infrastructure.

Advanced

Privileged Access Governance

Govern privileged entitlements and access to privileged access platform, Account Inventory to Secure and Comply.

Window Privilege Management

Control & Secure Administrator Account usage on Organization Windows system, Control Elevated Permissions for Windows Desktop users.

DevOps Secrets Management

Secure Secrets of Teams employing DevOps practices to access applications and services, eliminate embedded/ hardcoded credentials and log all the privileged sessions.

Platform Features

- Integrate more than RDP & SSH, integrate specialized clients & utilities with DIY Plugin Development Kit.
- Leverage cross-platform session management technology to secure every session by isolating endpoints for privileged sessions.
- Integrated Privileged Access Governance.
- Secure passwords, ssh keys, and secrets in a purpose-built vault supporting authorized only access via PAM, APIs.
- Commercial grade embedded high availability & module-level scalability options can help you design the best fit environment to respond to spikes in demand.
- Sectona MFA provides stronger security for your PAM setup by requiring a second verified step generated over Sectona App or SMS.
- Easily deploy PAM across regions or sites, be it cloud or on-premises, with flexible and decoupled components build for cloud environments.
- Secure passwords & secrets in passive & encrypted, authenticated application for break-glass scenarios.

sectona

Sectona with its light, integrated approach provides a single console for securing passwords & secrets in embedded vault, secure access with cross-platform access technology & manage privileges over endpoints.

For more information, visit www.sectona.com and follow @sectona1 on Twitter or @Sectona on linkedin