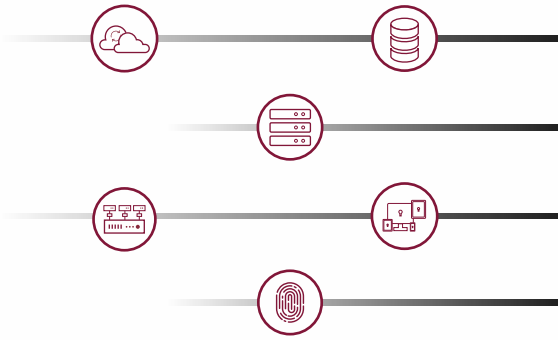
Datasheet

Sectona



Managing Economies of Privileged User Security

Rise in breaches because of privilege abuse is apparent in today's environment. Organizations are investigating why password management tools and techniques are poorly adopted by administrators and support teams. Often, it's difficult for businesses today to categorize users under conventional definitions of internal and external users. With the changing landscape of users, servers & applications, there has been a shift in infrastructure with more dependence on virtualization and cloud platforms. Remote users are constantly growing, so are the complexities of managing user requirements and pace of technology adoption thereby posing a challenge for security teams to build adaptive protection strategies.

Spectra PAM provides agility to organizations of any size with its productivity based SSO for access management, password automation for eliminating credential sharing, privileged task management for reducing excessive privilege delegation and granular access control with server privilege management capabilities for controlling access privileges. The solution is bundled with deep integrations with MFA tools, Virtualization & Cloud platforms, Ticketing solutions and SIEM systems.

Spectra Privileged Access Management

Balance Security & Productivity of Remote(Privileged) Users

Empower administrators to access any device on any network with Spectra's simple and secure single sign-on capability. The solution's purpose built utilities help govern administrator needs across multiple devices using client-based tabbed browsing or browser-based access for users on the go. Balance the access needs of internal and external users using Spectra's multiple secure access mechanisms and privileged account categories along with prepackaged connectors and rulesets. Manage access rules and policies within seconds by leveraging the 'Discovery to Access' capability across VMWare, ESX, ESXi, Active Directory and Cloud Resources.

Automate Password and Task Management

Administrators, vendors and remote support teams often require access to privileged or unmanaged accounts, services and applications. Spectra Password Vault is tailor-made for managing and auditing access to interactive accounts as well as application and non-human accounts. The solution's Automated Password Management helps reduce attack surface of privilege accounts by securely integrating access channels within your infrastructure. Spectra's Task Management automates routine tasks and eases administrators from the constraints of following a workflow process for accessing an asset every time. Human error is minimized by delegating tasks.

Realise more impact on your investment

Scale flexibly without compromising on security with our integrated privileged access management modules designed with all-inclusive pricing options. Leverage 100+ prepackaged connectors and utilize SDKs to develop any new connectors to help save on additional services or future shocks. Save time and costs by utilizing Spectra's integrated High Availability and Disaster Recovery capabilities. The solution is designed for easy deployment and provides simple licensing options.

Competitive Advantage

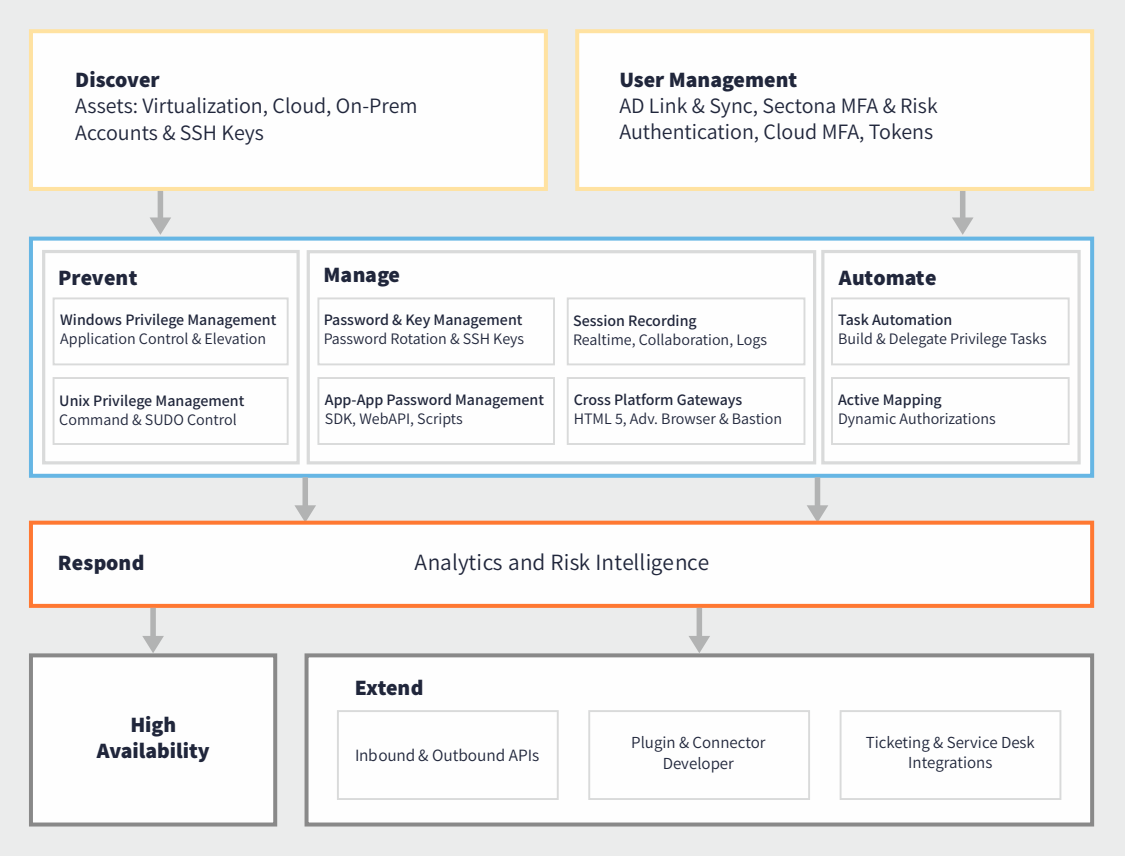
CROSS PLATFORM ACCESS
Access using any browser, any device, native clients, advanced access utilities or landing server.

INTELLIGENT RISK SCORING
Automatic scoring for every session activity categorized by security risk indicators.

ENHANCED SECURITY
Encryption Algorithms AES-256, RSA-1024 with FIPS 140-2 Support and Salting of Encrypted Passwords. Auto Hardening Capabilities of Host Layer

APP-APP PASSWORD MANAGEMENT
Web Servers (Apache, IIS), SDKs (Java. NET), WebAPI Support, Application Configuration Files

Spectra PAM Functional Architecture Stack



Integration

Password Management
Operating System
Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, MACOS, Windows Vista, Windows 8, Windows 10, Solaris, AIX, Ubuntu, RHEL, HP-UX, Debian, MacOS

Databases
MSQL 2000, MSSQL 2012, MSSQL 2014, MSQL 2016, DB2, MySQL, MS Azure SQL, MariaDB, Oracle 11g, Oracle 9i, Oracle 10g, PostgreSQL, Sybase

Network Devices
Checkpoint, Cisco IOS, Fortigate, F5, Juniper, HP ProCurve, Palo Alto, Riverbed

Virtualization
VMWare ESX, VMWare ESXi,Microsoft Hyper-V

Directory Services
Active Directory, Open LDAP, IBM Tivoli Directory, Oracle Internet Directory, Azure AD

Mainframes
AS/400, OS/390, z/OS

Others
Windows Service Accounts, Dependent Services, Config Files, Application Configuration Files, Dell DRAC, HP iLO

SSO & Access Interfaces
Generic Interfaces: RDP, SSH, SFTP, FTP, Telnet, HTTP/HTTPs
Database: SQL Server Management Studio, MySQL Workbench, Toad, SQL Developer, PL-SQL Developers, SQLPlus, MySQL Administrator, Oracle Enterprise Manager, IBM Data Studio
Virtualization: vSphere Client, VMWare Remote Control, Hyper-V Manager
Cloud: AWS Console, Azure Portal
Network Device: Checkpoint Console, FortiWeb, Cisco ASDM, Juniper Network Manager,
Remote Tools: Dameware, X11, VNC
CLI Interfance: SecureCRT, TeraTerm, SmartTerm

Authentication & MFA
Authentication: Active Directory, Sectona Local Authentication, Open LDAP, IBM Tivoli Directory, Oracle Internet Directory, Azure AD , Radius, Oauth
MFA: Sectona Authentication, RSA SecureID, Vasco, Okta, Onelogin, Duo, EZMCom, Safenet, Radius

Discovery
Network Based, Active Directory Computer, Azure Resources, AWS Resource, VMWare Guest OS, Local Accounts (Windows, Unix, Linux, Oracle, MSSQL, MySQL, Sybase, Db2)

SIEM & Log Forwarding

Ticketing Systems