WINNA PAM

Privileged Access Management

One of the most critical company's threats is facing up to a sophisticated external attacker or malicious insider – is already within its perimeter. Malicious insiders comprise company's primary security tools, because they are allocated for protecting against external threats, not against trusted employees, therefore, controlling and monitoring privileged access is extremely critical to alleviating the risks incurred by insider threats, preventing data violation as well as fulfilling compliance requirements. But security and IT leaders have to draw a fine border between protecting the organization's critical data aimed at providing business continuity to enable users and administrators to be efficient.

Privileged users perform sensitive activities that involve access to strategic corporate assets. In most corporates, privileged accounts are not well-defined and are often shared with multiple users concurrently. Privileged accounts are crystal clear across a multitude of critical Information Technology (IT) resources such as operating systems, network devices, hypervisors and enterprise applications.

Spotting unsuitable access to these accounts and specifying how many staffs have taken part in unauthorized activities is extremely challenging, because privileged accounts are not connected to individual end users. The number of privileged accounts rises including various number of servers, devices, and applications. In most large corporates, there are numerous privileged accounts for multiple individuals aimed at knowing the credentials without tracking who actually logged into an account at specific time.

Winna enables your corporate to have a full control over who is allowed to access what resources and when. Winna aids corporates to bridge the gap between IT security requirements and user enablement. This process mitigates IT security risks, simplifies compliance as well as providing user's productivity.

Main features of Winna PAM are as follows:

- Providing remote access using RDP, VNC, SSH, Telnet
- Automatic node discovery
- Online user activity monitoring
- Offline forensic investigation using command history and session videos
- Fine-grained access management
- Detailed audit logs and reports
- Auditing keyboard and clipboard streams
- OTP-based user authentication
- Active/Passive high availability architecture

There is no need to install any agents for Winna PAM to work with desired protocols. Any standard operating system is suitably enough. It is just required to simply add the node, specify connection parameters and provide suitable accesses to the users to enable them to make connections and send files on specified times.

	FEATURE	DESCRIPTION
OVERVIEW	LDAP Integration	Open LDAP/Active Directory Integration
	Discovery	Node discovery using SNMP
	Data Protection	Various capabilities for protecting sensitive data such as nodes information, audit logs, copy of transferred files
	Encryption	Disk encryption
	Monitoring	Monitoring dashboards for Winna services
	Management	Everything is done through Winna's web interface and a limited shell
USER MANAGEMENT	Local LDAP server	Winna is installed with a local LDAP server in case no external server exist in the organization
	Multi-LDAP support	No limits for the number of LDAP/AD servers
	Time-based access control	Users' access can be defined based on date, work hours in each day of week or even for a couple of hours
	Client IP filter	IP patterns can be used to restrict client workstations
	File transfer permissions	The ability to upload to or download from nodes can be enabled separately
	One Time Password	User authentication using OTP
AUDITING AND REPORTING	User audits	From login every actions users takes is audited.
	Node and connection audits	Everything that is done on nodes and connections such as creation, deletion, remote access, file transfer is audited.
	Key-log audits	Everything that user types is logged and searchable
	Online activity monitoring	Everything that the user is doing while connected to the remote node can be monitored by super user.
	File transfer reports	A detailed report with file content (if enabled by admin) is shown to make forensic investigation easier.
	Remote connection reports	A detailed report with a video of user activity during connection is provided.
	Command history reports	Everything that is typed in the textual sessions is available for search.
	OCR	OCR can be enabled for graphical sessions to make it possible to search for opened programs.
	SIEM sender	Audit logs can be sent to SIEM applications via syslog