اسپارا
SPARA

SATRAP

Privileged Access Management (Satrap)

About Spara

Established in 2018, Spara is a prominent cybersecurity company that originated with a team of four individuals. Our primary product is Privileged Access Management (Satrap), which helps protect businesses and organizations from advanced cyber threats. Through a strategic partnership formed in 2021, we have expanded our capabilities and experienced accelerated growth. Today, boasting a team of over 100 cybersecurity experts, we offer a comprehensive range of products and services including Satrap, EDR (Endpoint Detection and Response), EMS (Execution Management System), Red Team, SOC (Security Operation Center), Pentest (Penetration Test), and more. Our mission is to enhance cybersecurity measures within organizations and elevate their defense strategies.

Global statistics

86%

Data breaches involve the use of stolen credentials (Verizon)

71%

Year-over-year increase in cyberattacks that used stolen or compromised credentials (IBM)

$4.45 million

The global average cost of a data breach in 2023 (IBM)

$26.9 billion

Is the expected PAM market value by 2030 (KBV research)

Privileged Access Management – (Satrap) –

Privileged user accounts are accounts whose users have privileged access. These accesses can lead to macro-level changes to programs and systems and dealing with confidential company information. That's why these accounts and their users are the main targets for cybercriminals. Hackers try to gain these privileged accesses by targeting users and stealing their credentials.

Based on different research, more than 80% of data breaches are caused by stolen or compromised credentials[1] and the average global cost of this incident is $4.45 million[2]. As a result, one of the main concerns in organizations is managing privileged access.

Spara **"Satrap"** is a software product designed for privileged access management. It allows organizations to monitor, control, and secure privileged users' access to critical systems.

1- https://www.crowdstrike.com/cybersecurity-101/what-is-privileged-access-management/

2- https://www.ibm.com/reports/data-breach

Satrap specifications

Main Features

_Management, control, and audit of multiple remote user sessions

_Support is provided for SSH, RDP, VNC, Oracle database, and MS SQL server protocols

_System management through the web console

_No requirement to install a software agent on both the client and server

_The capability to access servers via the web console, Transparent, and Bastion modes

_Compatibility with PCI-DSS and FIPS 140-2 standards

_RemoteApp: providing application software in an isolated and monitored environment (browser, desktop, IDE, etc.)

_The possibility of implementing HA (high availability) in different types of Satrap deployment models

_Providing all applications utilized by the organization with multi-factor authentication

Other Features

Auditing sessions

_Enabling online monitoring of user activities during the session and allowing the user to terminate it at their discretion (4-Eye Authentication)

_Check out user activities in sessions as videos

_Check out all keyboard and clipboard activities in RDP, SSH, and VNC sessions

_Check out the name, volume, and checksum of the files being transferred during RDP sessions

_Full-text search on sessions and play videos instantly from the time the searched term appears on the page, based on OCR

_Full-text search on the content of all sessions

_Storing session data (videos and logs) in a compact and low-volume format (on average 30 MB/hour for each meeting)

_There is no software restriction on the number of sessions that can be saved and played in the system

_Filter sessions based on source, destination, session time, etc

Access control

_Four different authentication methods (Ask, Save Credential, PAM Credential, Ask Password)

_User authentication with centralized user management systems such as LDAP and Active Directory

_Authentication of users using public key in SSH sessions

_Automatic mapping of passwords of destination systems using Password Vault and keeping them hidden from users

_Providing the list of servers and credentials of destination servers that the user can access after authentication

_Restricting user access to specific periods, including daily limits.

_Automatic removal of access rules that have expired

_Restricting user access based on source IP address, destination, and user groups

_Centralized control of SSH and RDP servers' public keys to prevent Man-in-the-middle attacks

_Defining fixed values for IP address groups, time ranges, data patterns and referencing them in access rules

_Restricting and preventing users from running executable programs and accessing network connections during RDP sessions

_Implementing a multi-level approval workflow system for managing user access to operating systems, with up to 10 levels of authorization

Controlling the content of sessions

_Limitation of authorized and unauthorized commands entered by the user in Regular Expression format (according to the used protocol)

_Limiting the type of channels allowed in SSH sessions (Port Forward, Exec, SFTP, etc)

_Limiting the type of channels allowed in RDP sessions (Clipboard, File System, etc)

_Limiting the allowed commands and tables in Oracle sessions (Select, Update, etc)

Monitoring

_Comprehensive system status monitoring dashboard

_Automatic monitoring of system components and services in the form of health indicators

_Monitoring system resources (processor, memory, disk, etc.)

_Creating an event in case of a change in the system's health indicators

_Integration with monitoring tools

_No change of the source and destination IP ddresses in transparent deployment mode

_Automatic archiving of sessions in network storage

_Automatic deletion of old session videos

User management

_Creating multiple directories for users

_Defining users locally on Satrap

_Grouping users based on groups defined in Satrap

_Generating temporary one-time passwords (OTP) for users for temporary access

_Restricting the IP addresses permitted for each user to log in to the web console

_unlimited assignment of different roles to each user

_Limiting auditable sessions based on session tag per user

_Restricting the type of events visible to each user

_Applying password complexity rule for local Satrap users

_Creating a Lockout Policy for each user

_Creating and applying Check-In/Out policies on user IDs

Password management

_ Ensuring secure storage of passwords in the Password Vault system

_Password encryption with AES-256 algorithm

_It is impossible to access system administrator passwords stored in the Password Vault

Reporting

_Generating reports of the number and duration of sessions by protocol, origin, destination, etc

_Generating reports of channels established in RDP and SSH sessions

_Generating reports on the commands entered and database tables accessed during Oracle sessions

_Dynamic reporting based on source and destination server

Recording events

_Centralized search and recording of all system events

_Transmitting system events in Syslog format for SIEM systems

_Unlimited storage and archive of events

Integration

_Integrating users and enabling LDAP authentication

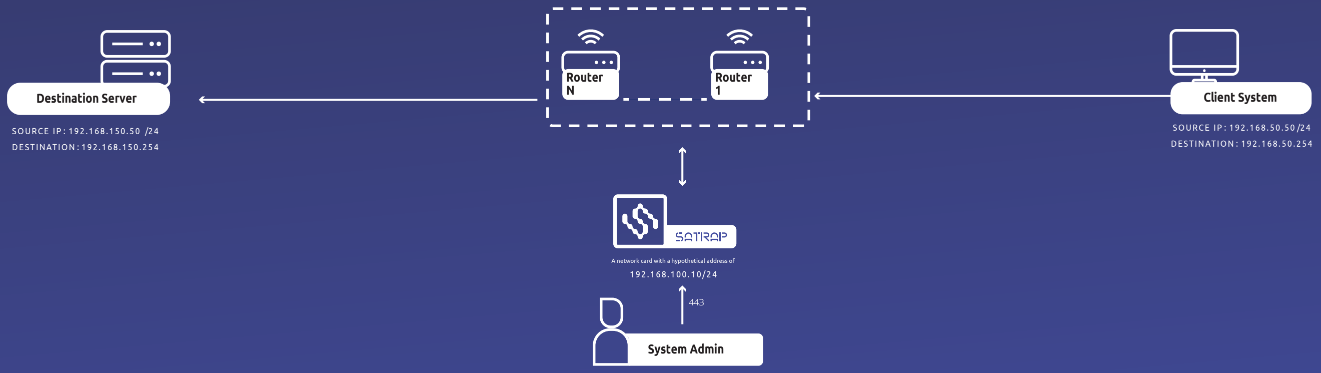
_Creating various changes in the system using API

Deployment

The Spara privileged access management system (Satrap) offers the flexibility to be deployed in transparent or non-transparent modes, based on the employer's preference.

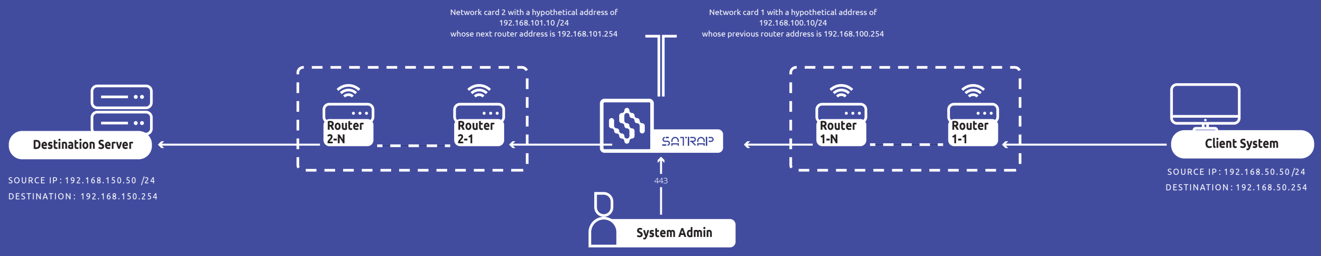
Non-transparent

To establish a connection with the destination server, the user must first connect to the Satrap server address and then input the destination server address into the console provided by Satrap.


Destination Server
SOURCE IP: 192.168.150.50 /24
DESTINATION: 192.168.150.254
Router N
Router 1
Client System
SOURCE IP: 192.168.50.50 /24
DESTINATION: 192.168.50.254
SATRAP
A network card with a hypothetical address of
192.168.100.10/24
443
System Admin

Transparent

Privileged access traffic can be efficiently directed through the Satrap server, allowing users to input the destination server address during connection. Furthermore, integration of the system as an ARP Proxy is also a viable option


Network card 2 with a hypothetical address of
192.168.101.10 /24
whose next router address is 192.168.101.254
Network card 1 with a hypothetical address of
192.168.100.10/24
whose previous router address is 192.168.100.254
Destination Server
SOURCE IP: 192.168.150.50 /24
DESTINATION: 192.168.150.254
Router 2-N
Router 2-1
SATRAP
Router 1-N
Router 1-1
Client System
SOURCE IP: 192.168.50.50 /24
DESTINATION: 192.168.50.254
443
System Admin

Competitive advantages

24hour support

A simpler interface and better user experience

Authorized by AFTA*

Customization based on organization needs

Support for Oracle and SQL server protocols

Affordable Cost

*AFTA is the strategic document for the security of the country's production space and information exchange in Iran

Satrap customers

بانک پاسارگاد

MIDHCO

pod
پایگاه اطلاع رسانی پشتیبانی پاد

سنباد

ریاست جمهوری
معاونت علمی و فناوری

داتین

(021) 222 75 003 ☎
info@spara.ir ✉
www.spara.ir www

اسپارا
SPARA