

# Krontech

## Single Connect™

Protect What You Connect™

### Privileged Access Management

---



# Company Overview

## Protect What You Connect™

Krontech is a software company established in 2007, and produces and integrates advanced technology software in the fields of Access Control Systems, Network Packet Brokerage, Streaming Analytics, Fast Data & Real Time Data Processing, and Next-generation Security and Audit. With cost-efficient, flexible, and tailored solutions, Krontech is a respected and proven partner, supporting many Tier-1 telecom service providers and large global enterprises.

Krontech's core offering is **Single Connect™**, a Privileged Access Management (PAM) solution granting privileged access to enterprise resources, used as an information security and governance tool to prevent internal data breaches and internal attacks through the use of privileged accounts.

**Single Connect™** enables IT managers and network admins to efficiently secure the access, control configurations and indisputably record all activities in the data center or network infrastructure, in which any breach in privileged accounts access might have material impact on business continuity.

Krontech is headquartered in New Jersey with research and development facilities in Istanbul, and regional sales and support offices in Europe, Middle East and Africa, and Asia Pacific.



# Privileged Accounts – Keys to the Kingdom

- Privileged accounts provide IT professionals with administrative or specialized levels of access based on higher levels of permissions to manage applications, software, databases, and server hardware
- In 2017, 81% of hacking related data breaches were due to either stolen and/or weak passwords. Almost half (43%) of the successful breaches were linked to internal actors, half intentional and half accidental\*
- In many recent breaches, end-user passwords are initially hacked through various social engineering techniques, then permissions are escalated to gain access to privileged accounts. This unauthorized access can easily go undetected for weeks or months
- Privileged accounts are all too often managed by using common passwords across multiple systems, unauthorized sharing of credentials, and default passwords that are never changed

# Data Breach Statistics

RECORDS BREACHED IN FIRST HALF OF 2017

1,901,866,611

NUMBER OF BREACH INCIDENTS

918

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

59.3%

PERCENTAGE OF DATA BREACHES WHERE ENCRYPTION WAS USED

4.6%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

EVERY DAY  
10,507,550

EVERY HOUR  
437,815

EVERY MINUTE  
7,297

EVERY SECOND  
122

\*Due to legal requirements, not all breaches are reported or publicly disclosed. Regional differences of data may not accurately reflect total data breaches that occur.

Statistics presented are based on the Breach Level Index [breachlevelindex.com]

**gemalto**  
security to be free



**IHG**  
InterContinental  
Hotels Group

**EQUIFAX**

dun & bradstreet

**Deloitte.**

**YAHOO!**

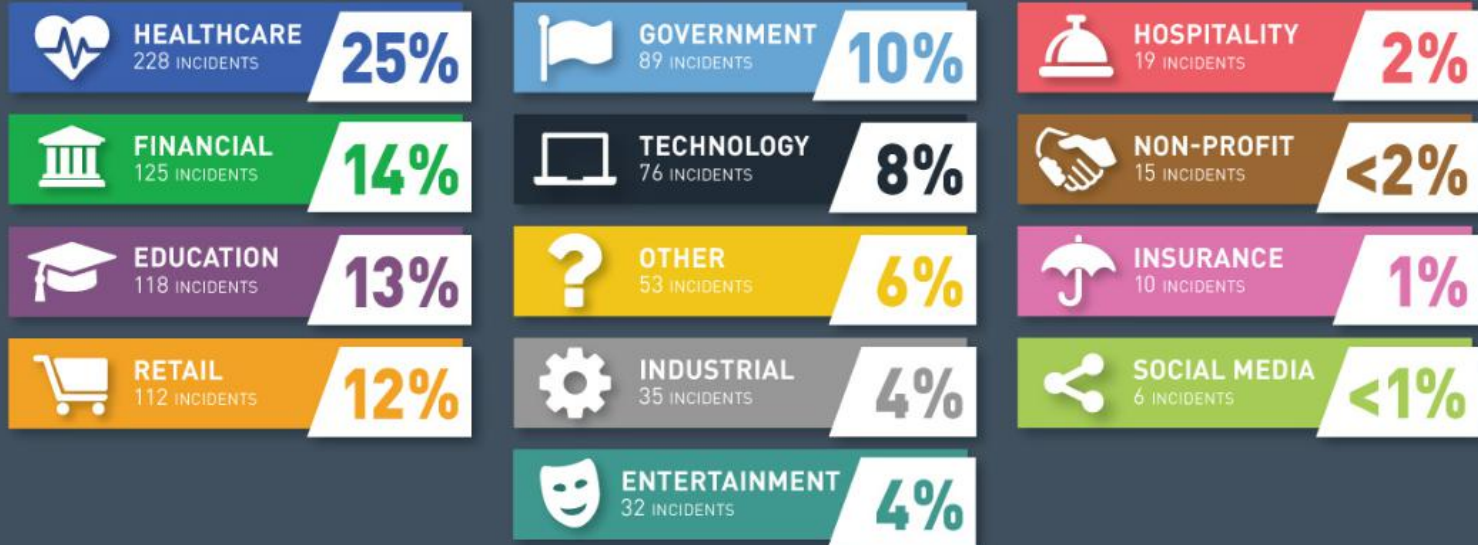
**ESEA**  
ESPORTS ENTERTAINMENT



**UBER**

# Data Breach Statistics – Incidents by Industry Jan-Jul 2017

## Number of Breaches Incidents by Industry



\*Due to legal requirements, not all breaches are reported or publicly disclosed.  
Regional differences of data may not accurately reflect total data breaches that occur.


Statistics presented are based on the Breach Level Index [breachlevelindex.com]


**gemalto**  
security to be free


# Data Breach Investigations Report



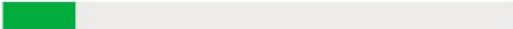
## What tactics do they use?

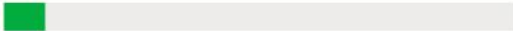
**62%**   
of breaches featured hacking.

**51%**   
over half of breaches included malware.

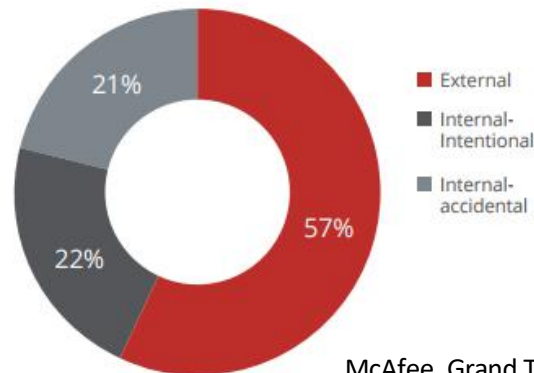
**81%**   
of hacking-related breaches leveraged either stolen and/or weak passwords.

**43%**   
were social attacks.

**14%**   
Errors were causal events in 14% of breaches.  
The same proportion involved privilege misuse.

**8%**   
Physical actions were present in 8% of breaches.

Verizon 2017 Data Breach Investigations Report



McAfee, Grand Theft Data

# Privileged Accounts

- Local Administrative Accounts
- Privileged User Accounts
- Domain Administrative Accounts
- Emergency Accounts
- Service Accounts
- Application Accounts



# Privileged Users and Best Practices

	Time	Privileges	Systems
<b>System, DB and Application Admins</b>	Continuous	Broad	Broad
<b>Operators, Help Desk</b>	Continuous	Medium	Broad
<b>Developers</b>	Continuous	Restricted	Restricted
<b>Project Staff</b>	Occasional	Limited	Narrow
<b>Third Parties (Contractors, Vendors)</b>	One-Off	Depends	Narrow

- Implement strict password and account management policies
- Enforce separation of duties and least privilege
- Log and record all actions of administrators and 3rd party users
- Use layered defense against remote attacks
- Deactivate access following termination
- Collect and save data for use in investigations





# Single Connect

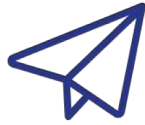
- Krontech's core offering is **Single Connect™**, a Privileged Access Management (PAM) solution granting privileged access to enterprise resources, used as an information security and governance tool to prevent internal data breaches and internal attacks using privileged accounts
- Single Connect enables IT managers and network admins to efficiently secure the access, control configurations and indisputably record all activities in the data center or network infrastructure
- Single Connect provides critical tools, monitoring and reporting to help provide and audit GDPR compliance

# Single Connect Addresses Key Enterprise Challenges



## Mitigate Risks of Privileged Accounts

A large enterprise has thousands of users and tens of thousands of devices creating more than a billion possible toxic access combinations.



## Manage Outsource Access

Outsourcing inherently creates security risks. Remote access security controls can only be done with proper privileged access management control systems to secure third-party access to privileged accounts.



## Mitigate Risks of Insider Threats

More than 43% of the security incidents reported are originating from insiders with access. Privileged Access Management controls who has access and monitors activity.



## Inappropriate Use of Admin Access

Detects potentially inappropriate use of administrative access by alerts, recordings and user behavior analytics.



## Malware specifically targets privileged accounts

The most terminal methods of malware are to use uncontrolled privileged access.



## Control Access of Drones, Robots & IoT

Ensures proper operation of scripts and automated tools with privileged access. Detects any behavioral anomalies in these accounts and will take automated actions.



## Geo-Fencing & Time Restrictions

Uses geo-location based access policies and time based access policies to minimize exposure regarding the external use of privileged accounts.



## Integrity of User Database by Aggregation

Single access to privilege tables stored in TACACS+ , RADIUS, LDAP, or database tables of software systems and appliances.



## Segregation of Duties

With integrated role management, pre-defined command sets, double-confirmation features and “detect/respond” functionality when users execute dangerous commands; privileged users can now operate safely in their day-to-day roles, maintaining systems, performing upgrades and troubleshooting issues.



## Network Automation for Security

Network automation enforces consistent processes for any type of privileged user by providing pre-defined and validated secure workflows. Integration of PAM with Network Automation increases security while maintaining organizational agility.



## Regulatory Compliance

PCI/DSS, SOX, BASEL III, FISMA, GDPR and many other mandates require organizations to comply with the growing list of regulations.



## Prepare for Audits Efficiently

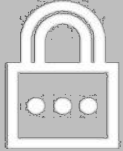
Easily collect data from Single Connect, and prepare professional reports in minutes, not days or weeks.



# Single Connect Modules

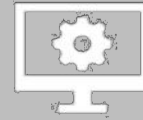
Can be bundled or used separately

# Single Connect Modules



## Dynamic Password Controller

Takes control of device and database passwords, providing security while sustaining efficiency.



## Session Manager

Logging and recording of all sessions, including command and context-aware filtering.



## 2FA Manager

Additional layers of authentication integrating mobile device, geo-location, and time.



## Access Directory Manager

Protocol-based security software unifies AAA, Active Directory, LDAP, & TACACS+.



## Data Access Manager

Securing Data Access with logging, policy enforcement, and real time data masking.



## Cloud PAM

PAM services from the cloud; secures 3<sup>rd</sup> party remote access from the cloud.



# Dynamic Password Controller

**Takes control of device and database passwords, providing security while sustaining efficiency.**

# Dynamic Password Controller

## Problems and Challenges

Easy to remember passwords

Using same password for many systems

Not changing passwords at regular intervals

No or minimal accountability

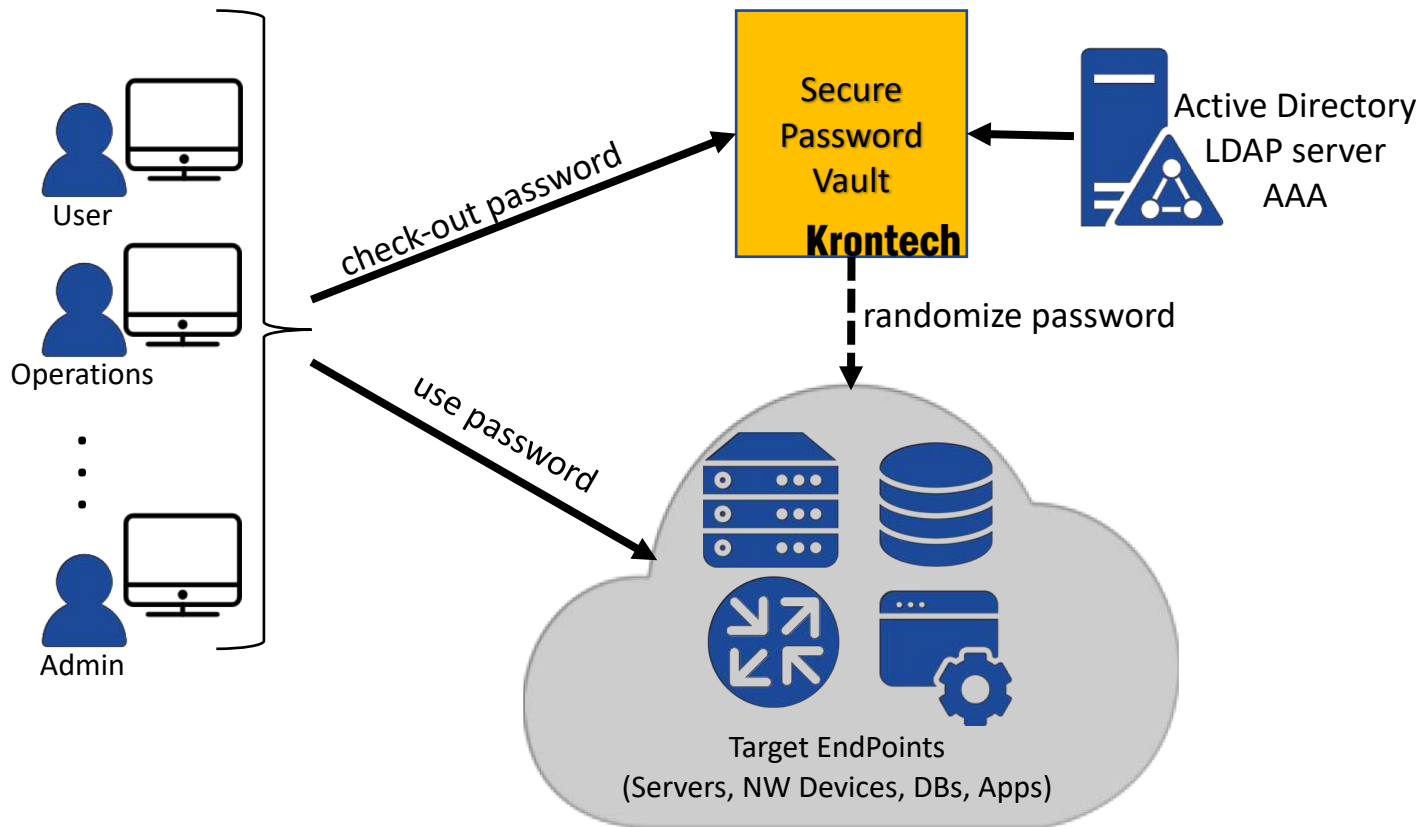
64% of end users report that they have written down their password at least once.

52% of the employees see no security risk to share their passwords with their colleagues.

Applications store credentials in configuration files, DB or source code



# Overview



# Dynamic Password Controller - Benefits

- Eliminate embedded passwords that are stored in unencrypted text files, DB or in source code.
- Passwords generated by Single Connect ensure maximum strength.
- Eliminate usage of non-expire passwords. Single Connect changes the password after every usage, one-time-password.
- Password is not shared among employees, because nobody knows/sees the password.
- Password is stored securely, in a vault.
- Platform supports password management of user accounts on NMS/EMS.
- Auto lock user account when an employee terminates employment (integration with enterprise Active Directory or LDAP is required).

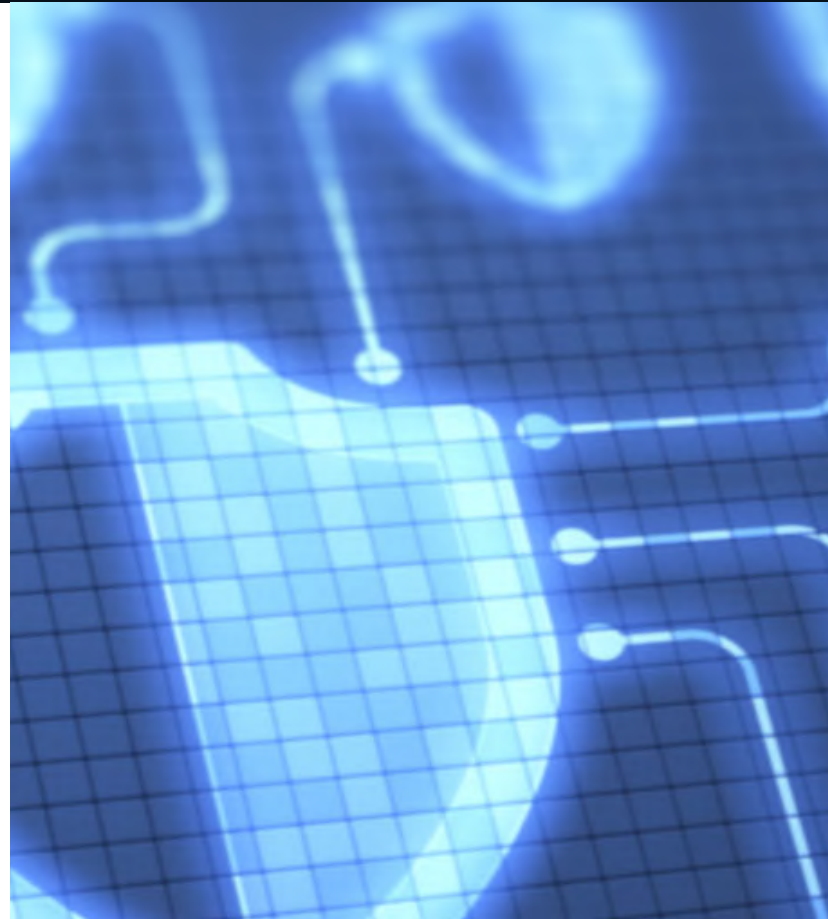




# Dynamic Password Controller

## Supports Local Users Accounts on:

- **Operating Systems:** Windows/Linux/Unix
- **Databases:** Oracle, MySQL, PostgreSQL, MsSQL, etc.
- **Devices and Appliances** with CLI interface
- **Applications** with password change API



# Dynamic Password Controller - Benefits

- Password is randomized by Single Connect at regular intervals to ensure maximum strength
- Password is stored securely, in a vault.
- Eliminate usage of non-expire passwords. Single Connect changes the password after every usage, one-time-password.
- Password is not shared among employees, because nobody knows/sees the password.
- Single-Sign-On and 2FA to check-out password
- Accountability when using shared password
- Auto lock user account when an employee terminates employment (integration with enterprise Active Directory or LDAP is required).
- Eliminate embedded passwords that are stored in unencrypted text files, DB or in source code.
- Agent-less. No software/app on user computers or servers to be installed
- Unified Visibility and Control of passwords





# Session Manager

Logging and recording of all sessions, including command and context-aware filtering.

# Session Manager

## Problems and Challenges

Complexity: Hundreds of privileged users connecting to thousands of servers every day

Visibility of all sessions

Excess of Privileges

No or minimal accountability

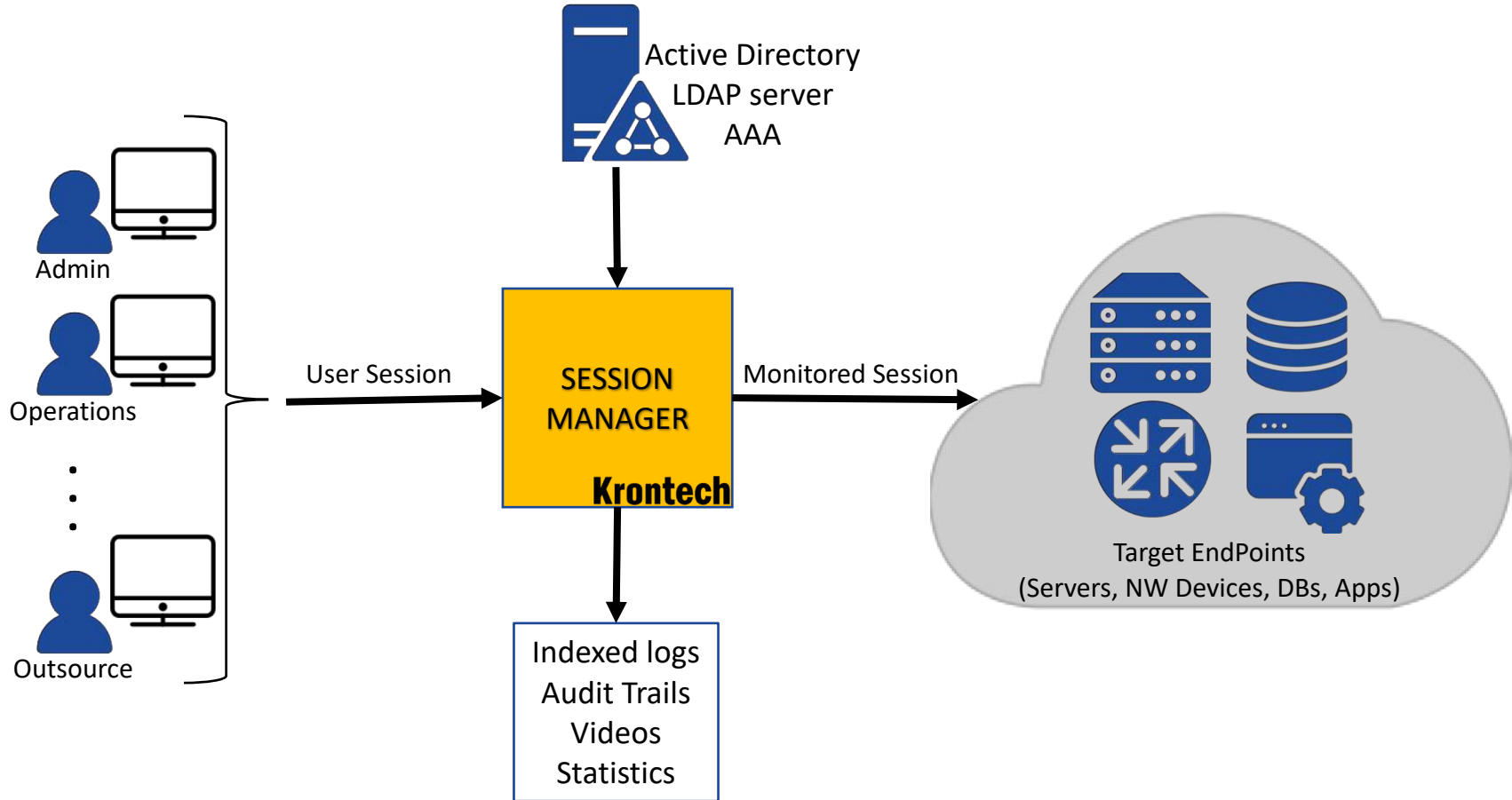
Layered defense

Data for use in investigations

Unsecure 3<sup>rd</sup> part remote access



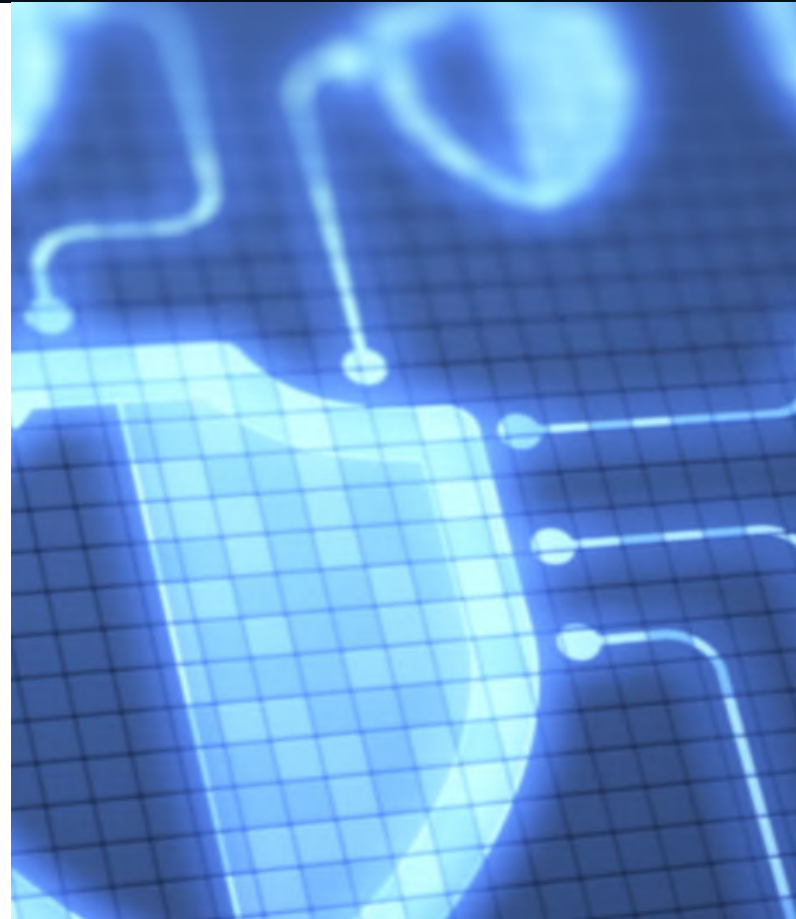
# Session Manager Overview



# Session Manager

**Supports Virtually all types of sessions :**

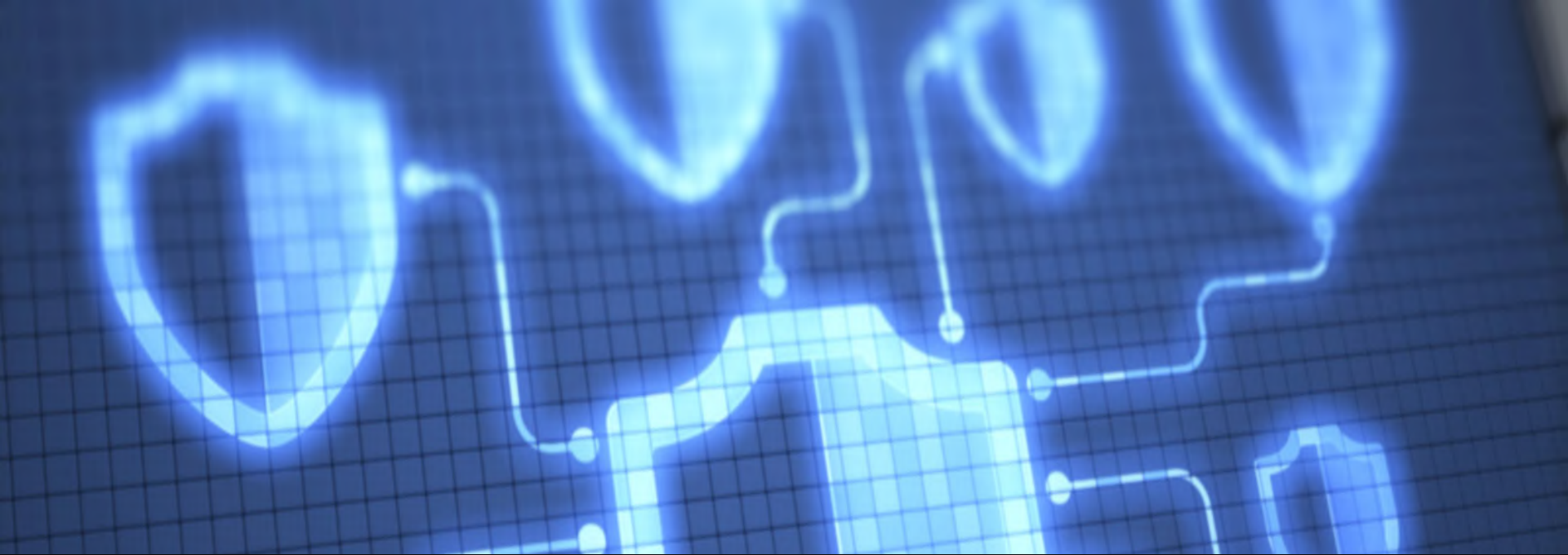
- **Console Sessions:** SSH, TELNET
- **Remote Desktop Sessions:** RDP, VNC
- **Database Sessions:** Oracle, MS-SQL, MySQL, Cassandra, etc.
- **Web Sessions:** HTTP/S
- **File Transfer:** SFTP



# Session Manager - Benefits

- Agent-less, man-in-the middle solution
- Indexed Logging, Session Recording and Session Replay
- Unified Visibility and Management of all privileged sessions
- Granular and Advanced Privileges Management (blacklist/whitelist, double confirmation, OTP, geo-fence, managerial approval, context-aware, score based privilege, time&date based access)
- Agent-less. No software/app on user computers or servers to be installed
- Enforces Security Policies Transparently
- User sessions are seamless, continue to use their own native client apps
- Termination of all active connections automatically for maintenance mode
- Enable Accountability and Records for use in investigations
- Database session support (including DB firewall and real time data masking)
- Carrier Grade and Scalable (active-active redundancy, lightweight native protocol support instead of workaround RDP jump server, storing raw data instead of full video record)





# 2FA Manager

**Additional layers of authentication integrating mobile device, geo-location, and time.**



# 2FA Manager

Additional layer of security to verify user identity.

You are secure even if username/password of your internal privileged account is hacked.



User enters credentials to log into system.



User is asked for token



User logged into system.

**Online Token  
(SMS, eMail, Mobile App  
Notification)**

**Offline Token  
(Mobile App)**

**Geo-Fencing and Time  
Restrictions**

# 2FA Manager - Benefits

- Even if an employee account is stolen, it is still not possible to access the enterprise's critical assets/resources unless employee's account and mobile phone are stolen, simultaneously.

---

- 2FA introduces another level to security defense. Even if the password is weak or non-expired, it is exponentially more secure with 2FA token verification.

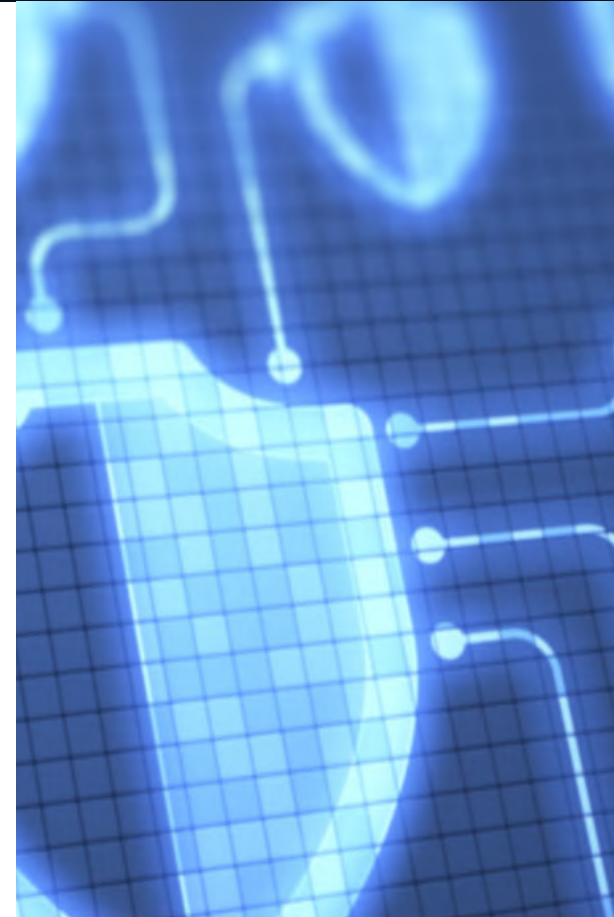
---

- Eliminates password sharing. Even if a password is shared with a colleague, it is useless.

---

- Auto-lock user accounts when an employee is terminated.

---



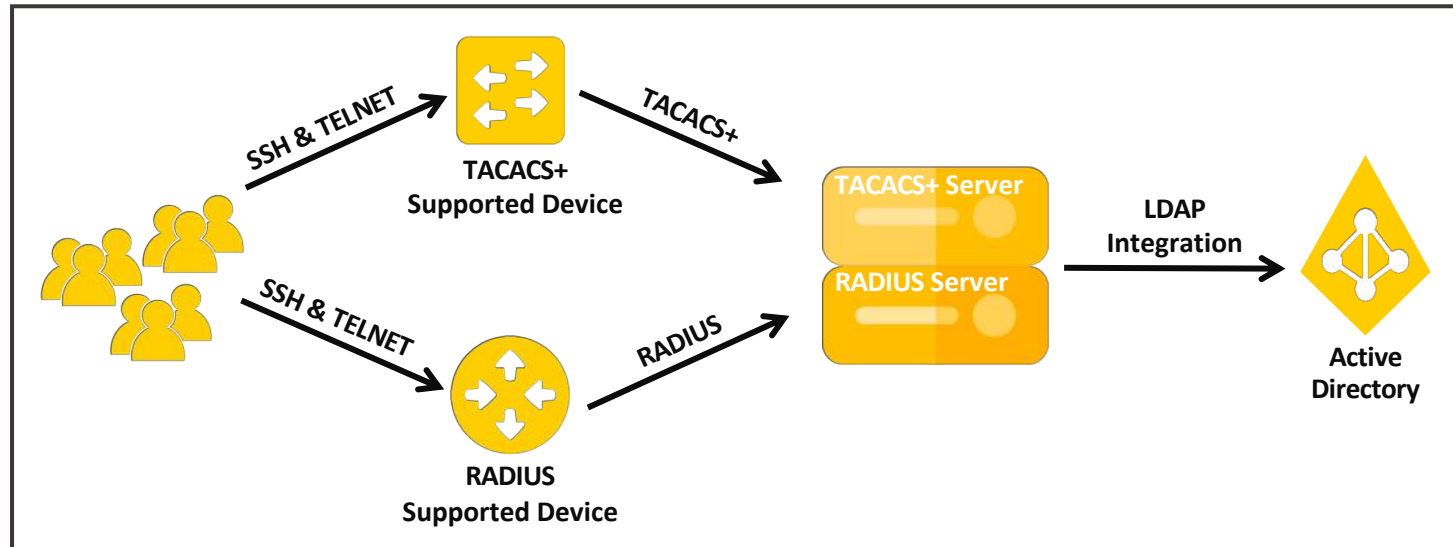
# **Access Directory Manager**

**Protocol-based security software unifies AAA, Active Directory, LDAP, & TACACS+.**

# Access Directory Manager

TACACS+ (Terminal Access Controller Access-Control System) and RADIUS (Remote Access Dial-In User Service) are used to control access to network devices via SSH/TELNET sessions.

Single Connect has a built-in support for internal and/or external TACACS+ and Radius servers to provide AAA (Authentication, Authorization and Accounting) services.



# Access Directory Manager - Benefits

- Built-in TACACS and Radius natively, no need for a 2<sup>nd</sup> platform to replace aging Cisco ACS servers.

---

- Standalone AAA solution and support RADIUS and TACACS+ protocols.

---

- Platform supports configuration of custom AVP (Attribute Value Pair).

---

- Supports up to 250,000 devices.

---

- TACACS includes per-command authorization and logging.

---

- TACACS enables you to set access policies by user, device, location or time of day.

---

- TACACS protocol is supported by most enterprise and carrier-grade devices.

---

- Central management for authorization of configuration.





# Data Access Manager

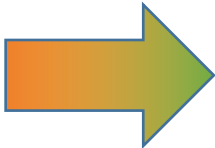
Securing Data Access with logging, policy enforcement, and real time data masking.

# Data Access Manager

Data masking is a technology aimed at preventing the abuse of sensitive/confidential data by giving users fictitious (yet realistic) data instead of real sensitive data

It aims to deter the misuse of data at rest, typically in nonproduction databases (static data masking), and data in transit, typically in production databases (dynamic data masking)

Dynamic Data Masking is necessary especially for application testing use cases that require representative and coherent data.

ORIGINAL DATA				MASKED DATA		
Name	Phone	Birth Date		Name	Phone	Birth Date
John Doe	511-336-44-55	11.4.1986	John Doe	511-111-11-11	1.2.1987	
Adam Smith	511-472-13-14	2.2.1967	Adam Smith	511-123-45-67	10.11.1966	

# Data Access Manager - Benefits



- All queries are logged indisputably. Users authenticate with their own credentials even if there is no such DB user. So real user who is running a query is known and logged.

---

- Sensitive data is manipulated and delivered to applications or users which is not sensitive anymore but still coherent and usable.

---

- Policies (DB masking rules) can be assigned to users' and applications' accounts easily and instantly.

---

- Eliminates weak and non-expiry passwords. Disables inactive accounts.

---

- Accounts can be limited time-wise (hours of day, day of week, etc.).

---

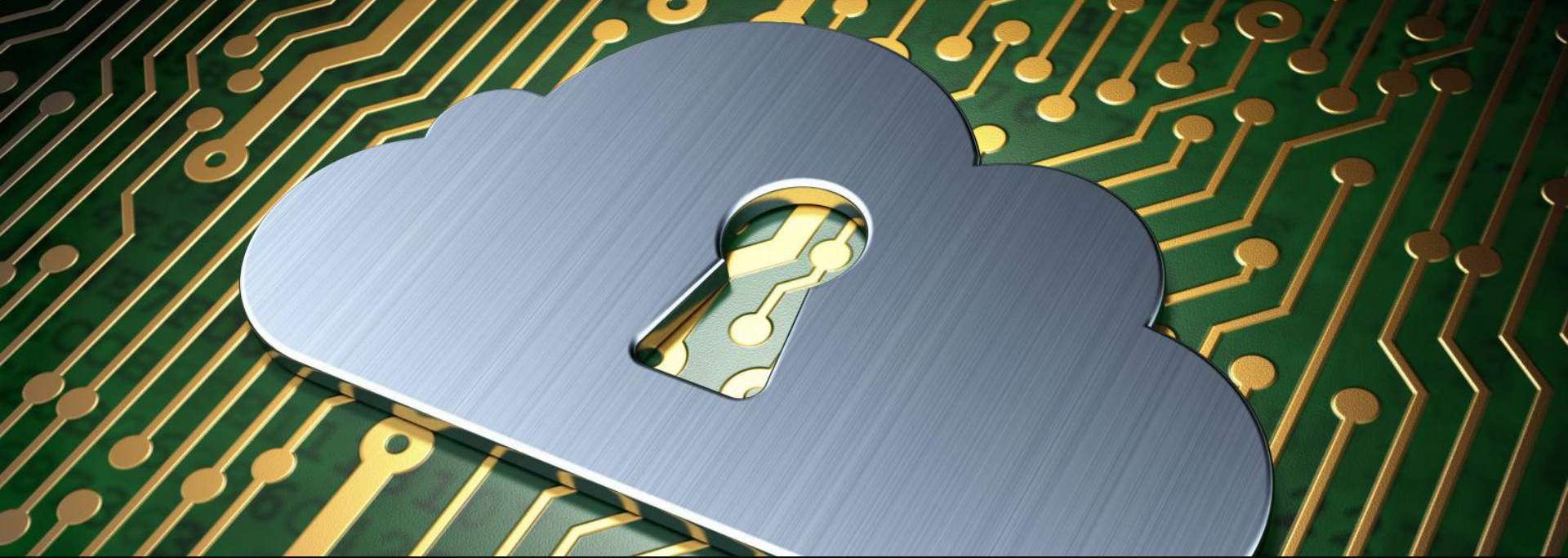
- Has almost no performance degradation impact on target Databases.

---

- Users continue to use their favorite clients, such as toad.

---

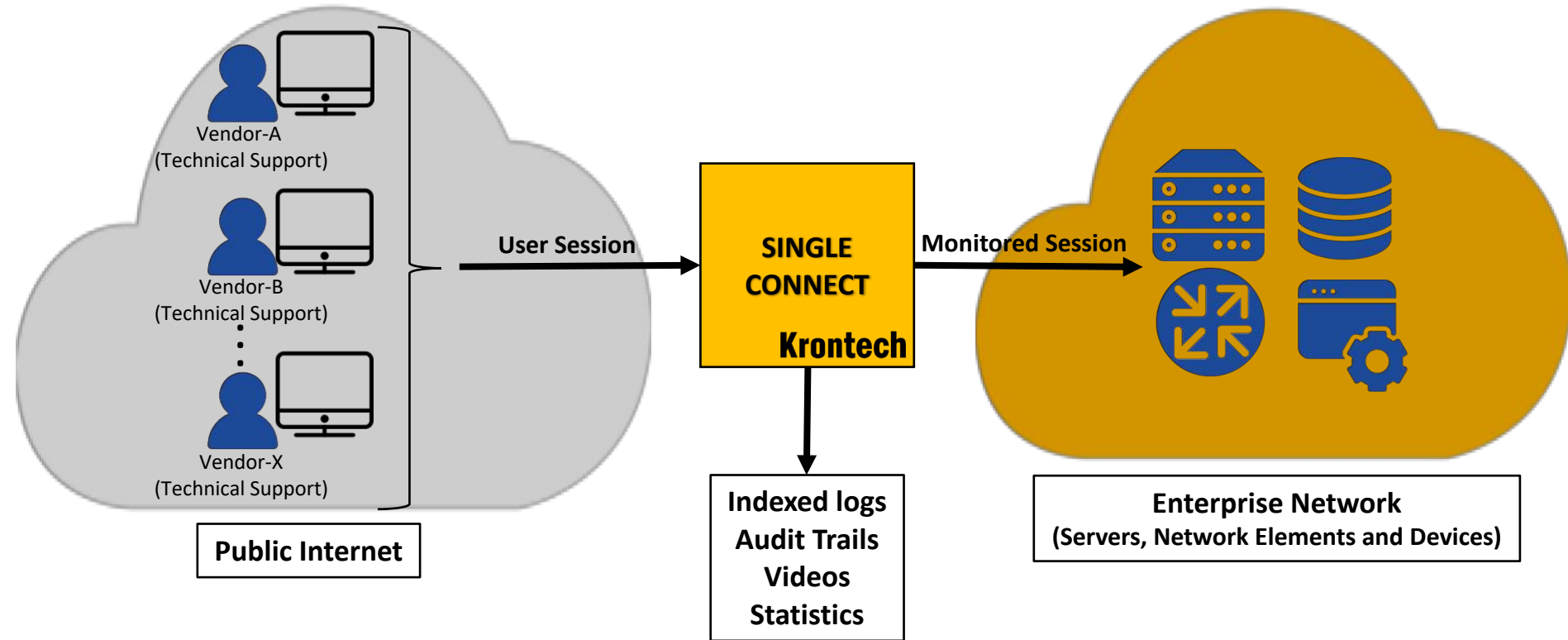




# Cloud PAM

**PAM services from the cloud; secures 3<sup>rd</sup> party remote access from the cloud.**

# Cloud PAM



# Cloud PAM - Benefits

- All 3<sup>rd</sup> party CLI and RDP access is secured and managed centrally by isolating the enterprise network from 3<sup>rd</sup> parties. No direct connection from 3<sup>rd</sup> party PCs to the enterprise network anymore.
- Single Sign on. Eliminate disclosure/sharing of privileged account passwords on enterprise servers and network elements.
- Indexed and searchable logging of all sessions, including video recording and re-play.
- Least privilege support. Policy enforcement based on target endpoint list, date & time of access, command filtering (blacklist/whitelist).
- Dual Control. Real-time, “over-the-shoulder” viewing of sessions with session control take-over and release capabilities.
- Additional Layer of Security. One-Time-Password (2FA) to connect to a server or network element.
- Easy to use. Access directly from browser, 0-install and VPN-less.



# PAM Features

	Krontech	CyberArk	BeyondTrust	Thycotic
Account Discovery	●	◐	◐	◐
Account Vaulting	●	●	●	●
App-to-App Credential Management	●	●	○	○
Secret Vault	●	●	●	◐
Logging	●	●	●	●
Notification and Approval	●	●	●	●
Built-in Two-Factor-Authentication	●	◐	◐	◐
Multi-Tenancy	●	○	○	○
Session Monitoring & Recording	●	●	●	◐
Jump Server	●	●	●	●
Least Privilege	●	◐	◐	◐
Network Elements Support	●	◐	◐	◐
Built-in AAA and TACACS Server	●	○	○	○
Operating System Desktop Support	●	◐	◐	◐
Database Server Support	●	◐	◐	○
File Transfer Server Support	●	◐	○	○
Web Application Support	●	○	○	○
Privileged Task Automation	●	○	○	○
High Availability	●	●	●	●
Disaster Recovery	●	●	●	●
Ease of Implementation	●	◐	◐	◐
Time to Value	●	◐	◐	◐
Security & Operational Efficiency	●	◐	◐	◐
Versatile Pricing	●	○	○	○
Total Cost of Ownership	●	◐	◐	◐



**| Krontech**

---

Protect What You Connect™