FUDO PAM vs. competition

	FUDO	OneIdentity	(Veracode) PAM	Centrify	BeyondTrust	CyberArk	Thycotic	Wallix	Arcon	Osirium	Hitachi ID Systems	ManageEngine
			Acquired by Thoma Bravo									
"All-in-one" system: no additional licenses required	✅	✅	✅	❌[1]	✅	❌[1]	❌[1]	✅	❌[1]	✅	❌[1]	❌[1]
Solution capabilities	PAM, PSM	PAM, PSM, PEDM	PAM, PSM, PEDM	PAM, PSM, PEDM	PAM, PSM, PEDM	PAM, PSM, PEDM, PIM	PAM, PSM, PEDM	PAM, PSM	PAM, PIM, PSM, PEDM	PAM, PASM	PAM, PSM, PEDM	PAM, PSM, PEDM
Hardware appliance / Virtual appliance	✅/✅	✅/✅	✅/✅	Microsoft Server and SQL Server required	✅/✅	Two Microsoft Servers instances are required	Microsoft Server and SQL Server required	✅/✅	Microsoft Server and SQL Server required	❌/✅	Microsoft Server and SQL Server required	Microsoft Server and SQL Server required
Operating modes:	Bastion, Proxy, Gateway, Transparent (Bridge), and mixed modes	Bastion, Router, Proxy	Behind firewall, behind/paralel to VPN	?	?	Bastion	Proxy	Bastion, proxy, transparent, jump server mode	?	Proxy	Proxy	Proxy
Supported communication protocols:	SSH, RDP, Citrix ICA, HTTP(s), Modbus SCADA/ICS, MS SQL, MySQL, Telnet, TN3270/2550, VNC, X11	SSH, RDP, HTTP(s), Citrix ICA, Telnet, TN3270/TN5250, VNC, X11, VMware View	SSH, RDP, Citrix ICA, HTTP, MS SQL, MySQL, Telnet, TN3270/2550, VNC, X11	Agents for macOS, Unix, Linux, Windows	SSH, RDP, VNC	SSH, RDP, Citrix ICA, HTTP, MS SQL, MySQL, Oracle, Telnet, TN3270/2550, VNC, X11, VMWare	Agents for macOS, Unix, Linux, Windows	HTTP/HTTPS, RDP/TSE, rlogin, SSH, VNC, Telnet, SFTP	SSH, RDP SQL - custom clients required	HTTPS, RDP, SSH TDS MS SQL, Telnet and vSphere	HTTPS, SSH, RDP	SSH, RDP SQL - custom clients required
Session recordig capabilities	full network protocol data recording with OCR	Limited, no recording of direct or local network login, OCR	?	basic: Gateway Session Monitoring, separate product	BeyondTrust is agentless; Bomgar agent records and performs PAM features - bad efficiency	jump host is required for recording, adaptive framerate	RDP does not provide keystroke data or names of executed applications w/o agent	capable PSM, RDP extensions, SSH filtering, agent-based application fingerprinting	secure gateway required	poor and inefficient, one screenshot per second	poor, local session recording, capture data streamed to a log server	Limited web-based access interface, slow
Agentless operation (nothing installed on targed machines, no special access tools)	✅	✅	❌	❌	❌	✅	❌	✅	❌	❌	❌	❌
Live session collaboration via browser	✅	❌	❌	❌	❌	✅	❌	✅	❌	❌	❌	❌
Distinctive actions recording for collaborative sessions	✅	❌	❌	❌	❌	❌	❌	❌	❌	❌	❌	❌
4-eyes authorization for critical systems access	✅	✅	✅	❌	❌	✅	✅	✅	?	?	✅	❌
Certified source for timestamping of session recordings	✅	✅	❌	❌	❌	✅	❌	❌	?	?	❌	❌
Session efficiency analysis for efficiency and productivity	✅	❌	❌	❌	❌	❌	❌	❌	❌	❌	❌	❌
Prevention: ability to stop forbidden user actions	✅ static rules	✅	❌	❌	❌	✅	✅	❌	?	?	?	❌

1. Microsoft Sever and SQL licenses are required, along with apriopriate security tools

PAM: Privileged Access Management and Privileged Account Management, also known as Privileged Account and Session Management (**PASM**). It is the process of using software to control who gets they keys to what doors.

PSM: Privileged Session Management. It means managing what someone is allowed to do after they've logged in with a privileged account.

PEDM: Privilege Elevation and Delegation Management. It allows certain standard users to request an elevated privileges to superuser status for a specific task, and when they've completed their task they revert to being a standard user.

PIM: Privilege Identity Managemet, also known as Identity Access Management (**IAM**) is a security and business discipline, that enables the right individuals to access the right resources at the right times and for the right reasons

User and Entity Behavior Analytics is the use of sophisticated machine learning algorithms to create a baseline for the activity of entities such as users, devices, servers, etc. Once baseline behavior is established an organization can calculate its risk based on deviations from the baselines in order to identifv securitv anomalies.

Transparent mode: user is accessing target system directly connecting through Fudo in invisible way

Proxy mode: user is connecting to Fudo and specified port points to target system

Gateway mode: user is connecting to target system directly, but network routing is forcing traffic through Fudo

Bastion mode: user is connecting to Fudo address by specifying target system name along with login information, not knowing target system access credentials, most secure mode