Privileged Access Management (PAM) is the mixture of technology and tools utilized to secure, monitor, and control access to an enterprise’s vital resources and information. PAM subcategories include application access management, vendor privileged access management, privileged session management, and shared access password management.

PAM software functions by collecting the credentials of privileged accounts, also called administrator accounts, into a secure database to log their activity and isolate their use. This isolation helps to reduce the risk of admin credentials being misused or stolen. Advanced PAM systems do not permit privileged users to select their own passwords. Rather, the platform’s password manager will give administrators the password for a particular day or provide one-time passwords every time an administrator logs in.
The FeaturedCustomers Customer Success ranking is based on data from our customer reference platform, market presence, web presence, & social presence as well as additional data aggregated from online sources and media properties. Our ranking engine applies an algorithm to all data collected to calculate the final Customer Success Report rankings. The overall Customer Success ranking is a weighted average based on 3 parts:

**Content Score** is affected by:
1. Total # of vendor generated customer references (case studies, success stories, testimonials, and customer videos)
2. Customer reference rating score
3. Year-over-year change in amount of customer references on FeaturedCustomers platform
4. Total # of profile views on FeaturedCustomers platform
5. Total # of customer reference views on FeaturedCustomers platform

**Market Presence Score** is affected by:
1. Social media followers including LinkedIn, Twitter, & Facebook
2. Vendor momentum based on web traffic and search trends
3. Organic SEO key term rankings
4. Company presence including # of press mentions

**Company Score** is affected by:
1. Total # of employees (based on social media and public resources)
2. Year-over-year change in # of employees over past 12 months
3. Glassdoor ranking
4. Venture capital raised

---

### Customer Success Report Award Levels

**Market Leader**
Vendor on FeaturedCustomers.com with substantial customer base & market share. Leaders have the highest ratio of customer success content, content quality score, and social media presence relative to company size.

**Top Performer**
Vendor on FeaturedCustomers.com with significant market presence and resources and enough customer reference content to validate their vision. Top Performer's products are highly rated by its customers but have not achieved the customer base and scale of a Market Leader.

**Rising Star**
Vendor on FeaturedCustomers.com that does not have the market presence of Market Leaders or Top Performers, but understands where the market is going and has disruptive technology. Rising Stars have been around long enough to establish momentum and a minimum amount of customer reference content along with a growing social presence.
2020 Customer Success Awards
Check out this list of the highest rated Privileged Access Management software based on the FeaturedCustomers Customer Success Report.
ABOUT CYBERARK
CyberArk is the only security company laser-focused on striking down targeted cyber threats, those that make their way inside to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk is trusted by the world’s leading companies -- including 30 of the Fortune 100 -- to protect their highest-value information assets, infrastructure and applications.

74
Customer references from happy CyberArk users

"CyberArk PAM-as-a-service provides an enterprise-grade, centralized approach that works well for us. And as a small team, having a 100% cloud-based based solution makes it easy."
Bassam Alqassar
Vice President, Information Systems and Technology, Princess House

"Selecting CyberArk was definitely the right decision. By introducing the CyberArk Privileged Account Security Solution, we were able to significantly improve process quality and meet statutory requirements more efficiently."
Stephan Zimmermann
Fiducia IT AG

"From a security perspective, using CyberArk is the best approach because there is now only one source/point of connection. We no longer have to manage multiple points of access. With CyberArk in place, we’ve simplified the process of managing security."
Marcos Henrique Igutti
Information Security Manager, FS

"CyberArk Privileged Account Security really is a great, all-round solution – not only does it manage, secure and monitor our privileged accounts, it also allows us to maintain compliance with a number of regulations, such as Sarbanes Oxley, which is hugely beneficial to us."
Karon Davies
Global Security Privileged Access Manager, BT
2020 MARKET LEADERS

BeyoNdTruSt

CenTrify

thycotic
ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing data breaches related to stolen credentials, misused privileges, and compromised remote access. Their extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. BeyondTrust unifies the industry's broadest set of privileged access capabilities with centralized management, reporting, and analytics, enabling leaders to take decisive and informed actions to defeat attackers. Their holistic platform stands out for its flexible design that simplifies integrations, enhances user productivity, and maximizes IT and security investments. BeyondTrust gives organizations the visibility and control they need to reduce risk, achieve compliance objectives, and boost operational performance. They are trusted by 20,000 customers, including half of the Fortune 100, and a global partner network.

“Previously, the only way we could let vendors remote in was to set up a VPN. With Bomgar, we can give them limited access to our environment and record their session so I have an audit log of exactly what has been done. That makes our environment much more secure.”
Brian Bard
Business and Technology Analyst, UNC Charlotte

“I am very impressed with both the PowerBroker functionality and with the BeyondTrust services team. PowerBroker has deep auditing capabilities, which is helping us to quickly get to the information we need. The logging, auditing, and role-based access capabilities are all excellent and allow us to very effectively manage privileges and audit AD changes...”
Mastan Vail Shaik
IT Architect, Tata Consultancy Services

“It was essential for us to deploy a remote support solution that ensured secure access and could record data and create an audit trail of actions taken during support sessions. Only Bomgar, with its single-tenant appliance architecture, encrypted session traffic, advanced authentication and access controls, and session recording features, met every...”
Jorge Wilson da Silva Mendes
IT Manager, Anatel

“Our customers are pleased to see we now have a single solution for accessing all of our customer using Bomgar Privileged Access, and they are happy to see that we enable our customers to on-board their vendors so they have access logging and video recordings for their vendors.”
Rick Kramer
Sr. System Engineer, Pink Elephant
ABOUT CENTRIFY

Centrify Zero Trust Security provides Zero Trust Security through the power of Next-Gen Access to secure access to applications, endpoints and infrastructure while significantly reducing the possibility of access by bad actors. More than 5,000 customers have deployed Centrify across millions of servers, workstations, and applications. With Centrify, organizations are reducing their costs associated with identity lifecycle management and compliance by over 50%. NEVER TRUST, ALWAYS VERIFY. Centrify Zero Trust Security Defined. VERIFY THE USER - Confirm Jane’s identity by asking her to provide something she has, something she knows or something she is. Also leverage user behavior unique to Jane and context such as location, day and time of login as additional factors to ensure authenticity. VALIDATE THE DEVICE - Make sure Jane is using a trusted endpoint before granting access to resources. If Jane logs into a resource from an untrusted endpoint, challenge Jane with MFA or block her access if the resource should only be accessible from a secure trusted endpoint. LIMIT ACCESS & PRIVILEGE - Once Jane has confirmed her identity and is using a trusted endpoint at a verified location, Jane is then granted just enough access she needs to perform her job at any given time. LEARN & ADAPT - Continuously leverage data about Jane, her device(s) and her behavior to allow access, block access or enforce additional authentication. With machine learning, policies can be adjusted automatically and in real-time.

“Upon implementation, Centrify immediately began to solve a number of compliance issues by providing us with three key ingredients: Centralized privileged identity management, granular access controls, and privileged activity auditing.”

Brad Settles
Technical Services Administrative Manager, State of Michigan DTMB

“VPNs typically provide full network access, creating security risks. With Centrify’s App Gateway, only specific apps are made available. Access for each endpoint is limited, and IT maintains strict control over who can access what. This helps to reduce our overall attack surface.”

David Howell
IT Associate Director, Chugai

“With Centrify, we have a 100% cloud-based identity solution that provides authentication, provisioning and de-provisioning, SSO, MDM, Mac management, and the ability to track which users are logging into which apps and services.”

Steve Winter
IT Director, Apttus

“We were looking for a solution that met three main criteria: Password management that would enable user single sign-on, easy installation and management, and the ability to ‘lock up’ our passwords. Centrify met all three.”

Wayne Dale
Application Security Engineer, FastMed Urgent Care
ABOUT THYCOtic

Thycotic is the leading provider of cloud-ready privilege management solutions. Thycotic’s security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility and control. Headquartered in Washington, DC, Thycotic operates worldwide with offices in the UK and Australia.

"Thycotic allows us to control and protect sensitive accounts, manage privileged user access, and secure client data at the source, keeping our client data safe. We evaluated several competitors in this space and Thycotic came out on top.”

Huw Evans
Principal Security Consultant, IT Weapons

“One of the key advantages with Secret Server is the ability to hand out credentials to team members without revealing the password. Secret Server gives us an approval workflow process that lets us respond to requests for access, but also control the elevation of credentials and track access as well.”

CJ Wiemer
Information System Security Engineer, kCura

“Secret Server saves us a huge amount of man hours every month, while increasing the predictibility of password changes, and helping meet our policy compliance obligations.”

Peter Yu
Corporate IT Operation Manager, Trend Micro

“Having privileged account management with Secret Server is very important to us because our clients trust us with their information. Having Secret Server assign secrets to technicians and the ability to check sensitive passwords in and out is very important to our clients.”

Johanny Torrico
Vice President of Operations at Community IT Innovators, Community IT Innovators
TOP PERFORMERS
2020 TOP PERFORMERS

Hitachi ID Systems, Inc.
Omada
ONE IDENTITY
SecureLink
Wallix

Cybersecurity Simplified
ABOUT HITACHI ID SYSTEMS

Hitachi ID Systems delivers access governance and identity administration solutions to organizations globally, including Fortune 500 companies to secure access to systems in both the enterprise and in the cloud.

17
Customer references from happy Hitachi ID Systems users

VIEW ALL REFERENCES

“Hitachi ID Password Manager met all our objectives and has ensured significant ROI.”
Samuel Tran
American Museum of Natural History

“The capabilities of Hitachi ID’s application, the ease of implementation and cost were the biggest factors influencing our decision to choose Hitachi ID Systems.”
J.R. Zimmer
IT Senior Manager, NCR Corporation

“Transparent password synchronization was the feature that really helped our user adoption process.”
Terri Root
Project Leader, Cessna

“Hitachi ID Password Manager addresses the problem of offering a self-service password reset and synchronization capability without having to deploy a third-party GINA DLL at each desktop. This is an effective way to reduce the cost of deployment and on-going management of this type of solution.”
Jackson Shaw
Program Manager, MetaDirectory, Microsoft Corporation
Omada is a market-leading provider of IT security solutions and services for identity management and access governance enabling organizations to achieve compliance, reduce risk exposure, and maximize efficiency. Omada’s solution empowers enterprises to manage identities across heterogeneous IT-systems and is acclaimed for its business-centric approach and high adaptability.

“IT provides added benefits, such as efficient license control handling. I can see precisely how many people use the various licenses, providing a potential cost saving.”
Kaj Mortensen Stoltenberg
Team leader, Digitalization and IT, Varde Municipality

“The solution has brought about immense savings for the Ministry when it comes to controlling our identity management processes. The Omada Identity Manager solution has reduced the complexity and workload involved in order to coordinate tasks and progress.”
Martin Niels Pedersen
IT Manager, Ministry of Economic and Business Affairs

“For various reasons Omada has been chosen as the solution to address our identity and access management needs. The main reasons for choosing OIS include its intuitive user interface, direct connectivity to Active Directory as well as automation of lifecycle processes such as employees and contractors joining the company, leaving, or changing…”
Lothar Klose
Head of Department, IT User Service, Barmenia Versicherungen

“Omada gives us the opportunity to automate our user and authorization management in the long run and to realize efficient, transparent processes for our employee administration. All our staff will benefit from the implementation of standard processes and an increased IT security.”
Ulrike Schlutt
Project Manager, Customer Service Construction Machinery, Liebherr
ABOUT ONE IDENTITY

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Their solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

"Safeguard for Privileged Sessions is a reliable and straightforward solution, which integrated seamlessly into our existing identity management system and is able to support our needs for both Linux and Windows server access. Implementation went very smoothly as it did not require any changes to our network or servers. We are happy with the...

Matt Magleby
Sr. Computer Scientist, Adobe

"We finally chose Safeguard for Privileged Sessions because this solution offered full transparency on the network and the capability of searching in the audit trail content. Safeguard for Privileged Sessions has been a quite secure product, as bypassing the audit system is almost impossible."

Bogdan Mistrapau
Middleware Infrastructure Administrator, Orange Romania

"One Identity Safeguard for Privileged Sessions enables me to sleep easy with its fine-grained access control, supervision, and audit of shell access to our critical systems."

Georg Petzl
Chief Security Officer, T-Mobile

"One Identity’s Safeguard for Privileged Sessions is a reliable and feature-rich product that helps the security department enforce internal policies and minimize the risk of fraud."

Charalambos Charalambous
Security Engineer, CYTA
ABOUT SECURELINK

SecureLink is the leader in managing secure vendor privileged access and remote support for both highly regulated enterprise organizations and technology vendors. More than 30,000 organizations across multiple industries including healthcare, financial services, legal, gaming, and retail rely on SecureLink’s secure, purpose-built platform. The company was founded in 2003 and is based in Austin, Texas with a second office in Costa Rica.

“"The ability to give access to our production floor managers so that they can approve vendor access is great; it’s one less thing that our IT team has to do and manage. Plus the fact that SecureLink will help train our vendors is an added bonus.”
Ashley Torvinin
Network Administrator, Whelen Engineering

“"All of the application analysts love the fact that they can get notifications on their vendor activity and that they can be the ones to authorize access at the vendor rep level. Another benefit is also not having to sit on a WebEx as they did previously with their vendors who needed to connect at 2 in the morning.”
David Nedd
Information Security Analyst, Aspirus

“"By converting our customers to SecureLink’s remote support network, we were able to save our customers money on their connectivity costs, enhance the reliability of the connection, improve our response and resolution times, all while increasing the security and auditing capability of the customer’s systems. Not bad for 15 minutes work.”
Robert Bell
VP of Product Support Services, Allscripts

“"Any remote access for any type of vendor is required to go through SecureLink. We’ve standardized our policies and our remote access management. It’s simplified things.”
Hilary Farley
Director of IT, Prairie Flower Casino
ABOUT WALLIX GROUP

WALLIX Group is a cybersecurity vendor dedicated to defending and facilitating organizations' success against cyber threats. For over a decade, WALLIX has striven to protect companies' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management. The Bastion PAM solution was also the first government-certified solution on the market. As a leader in PAM, major players trust WALLIX to secure access to their data, resources, and endpoints.

“"We were looking for a solution which could simplify and secure access to our infrastructure for our users and third-party suppliers. We chose the WALLIX Bastion as it was easy to use and manage, as well as meeting all our security requirements.”

Michael Massingham
IT Manager, Systech International

“WALLIX provides real-time resource management, reporting and monitoring capabilities for IT administrators, improving the overall efficiency of Gulf Air's IT function. Also, Privileged Access Management is instrumental for Gulf Air in complying with the required international and industry standards. We're currently certified against the ISO 27001...”

Jassim Haji
IT Director, Gulf Air

“Thanks to the WALLIX Bastion's all-in-one architecture, the product has shown that it is perfectly adapted to our perimeter both in terms of scale and simplicity. To summarise, WALLIX offers the best value for our requirements.”

Thomas Lefaure
ISS Architect, Michelin Group

“The Bastion provides a truly safe zone for remote connections on industrial systems, that is fully transparent for the user and whose performance remains unaffected.”

Jean Christophe MATHIEU
Product and Solution Security Officer, Siemens
Ekran System was established in 2013 by a group of experienced digital security specialists. In late 2013 the first official market version of Ekran Systems® was released. The company, backed by Commonwealth of Virginia (CIT funding via MACH37 accelerator) and private investors, focuses on the development of insider security solutions and delivering them to customers worldwide via its global partner network.

“Ekran System product completely meets our requirements. Its maintenance is intuitive, and configuration is easy and painless.”
Maciej Galiński
Senior Application Specialist - IT Department, Dendro Poland

“In order to comply with regulations and corporate policy rules, we wanted to ensure uninterruptible privileged user audit, as well as provide local and remote employee activity monitoring. That’s why we have chosen Ekran System, easy-to-use and affordable solution, which met our expectations in full measure.”
Kelvin Goh
Managing Partner, Global B2B Consultancy

“Ekran System is a reliable product that meets its functions. We use it to monitor privileged activity on corporate servers because of maximal simplicity of the interface and the most integrated and easy to analyze format.”
Adrian Pupek
Team Manager of Network and Security, PKO Polish Bank

“Ekran System has become a great choice to record and audit user actions in our infrastructure. It delivers a powerful and flexible toolset; moreover, the Ekran team was ready to customize the platform for our needs adding several new features.”
Necati Mancar
IT Infrastructure Manager, MSC Turkey Agency
ABOUT OSIRIUM

Osirium prevents attacks on Privileged Accounts by separating people from passwords. Those privileged passwords never enter any workstation, they undergo Enterprise Class Password Life Cycle Management. They can build a least privileged model by removing the need for direct system access using Privileged Task Automation. Add Session Recording to allow you to see who did what, where and when.

"Osirium’s PxM Platform was set up and installed in two days, compared to the two weeks our previous solution had taken.”

John Slator
Head of IT and Informatics, Mental Health Concern

"Osirium’s PxM Platform has met our objectives - it gives us the accountability and auditability of our privileged user activities which was our primary goal. We can also enforce a least privileged model and control legacy accounts through one central environment.”

Sompo Canopius

"We chose Osirium’s PxM Express solution to remove the risk of our privileged accounts being compromised both internally and by potential external threats.”

Kevin Holland
IT Manager, Targetfollow Estates Limited

"Out of the box, the Osirium platform lived up to our expectation. The user interface makes it obvious who can access what, where and when. The interface itself is easy to learn and it also has great depth. We love the look of the management pages, and in day to day use they have proven really useful - they definitely show us when and how work..."

Karim Kronfli
IT and Data Security Manager, M-Netics
SSH.COM is the market leader in developing advanced security solutions that enable, monitor and manage encrypted networks. They have developed leading edge security solutions that enable organizations to protect against a rapidly growing threat landscape that includes both internal and external actors. Their platform based approach to Secure Shell deployment and management provides the only solution on the market that addresses the need for security, compliance and operational efficiency in today’s complex enterprise environments.

“Universal SSH Key Manager brings the business IT into compliance with SOX regulations and saves on costs.”
Multinational Energy Company

“The National Cyber Security Authority at the Finnish Transport and Communications Agency (Traficom) has certified the SSH NQX firewall and virtual private network (VPN) appliance as a cryptographic product for protecting classified information according to Finnish national (FI) ST III (Confidential) security requirements.”
Finnish Communications Regulatory Authority

"The PAM market is becoming more competitive and size alone will no longer keep vendors at the top. This is especially true in a period when vendors like SSH.COM can go from Challenger to Leader in one year due to a strong focus on technology and innovation."
Paul Fisher
KuppingerCole
senhasegura is a company that integrates the MT4 group, they develop and provide a password vault solution for Privileged Access Management (PAM). The vault aims to assure sovereignty of actions and critical information of companies. Moreover, they act on data theft and they provide tracking of all actions taken by administrators in networks, servers and data bases to attend all regulatory requirements for PCI, SOX and ISO 27001. Furthermore, they are also GDPR ready by offering an end-to-end protection of privileged accounts that have access to systems and applications that contain personal data.

“Today, senhasegura is more than an indispensable tool to our company, in which we are able to safely audit our servers and store passwords. The Support team replies promptly, whenever we need them.”

Thais Figueiredo
Construtora Tenda

“Senhasegura Support has the technical knowledge and service synergy that it feels more like a department in the company than an external service provider.”

Information Security Specialist
Important Financial Company

“With senhasegura Support we have guaranteed excellent service solution for every doubt or problem that we may face each day. People with vast technical knowledge and agility on problem solution.”

IT Manager
Large Brazilian Construction Company

“Senhasegura Support is without a doubt the best we ever had in the technology business.”

Julian Hoche
Catho