FORRESTER®

For: Security & Risk Professionals

The Forrester Wave™: Privileged Identity Management, Q1 2014

by Andras Cser, February 3, 2014

KEY TAKEAWAYS

Vendors Enhance Threat Mitigation And Cloud Capabilities

Today's economic environment is forcing S&R professionals to consider alternatives to on-premises solutions and use cloud services. Leaders in the PIM space now offer cloud support, threat mitigation to prevent data breaches, and privileged identity intelligence.

The PIM Market Is Growing As Security Pros Look For Comprehensive Controls

The PIM market is growing because more S&R professionals see PIM as a relatively simple but effective way to address their top security, compliance, and efficiency challenges. Also, S&R pros increasingly trust PIM providers to act as strategic partners, advising them on top password safe decisions and offering layered controls.

Cloud, Hypervisor, And Behavioral Analytics Are Key Differentiators In The PIM Market

As pure password safe technology becomes more mature, improved cloud platform support, availability as a cloud offering, support for cloud environments, better hypervisor support, and ability to detect behavioral anomalies dictate which providers will lead the pack.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 | Fax: +1 617.613.5000 | www.forrester.com

The Forrester Wave™: Privileged Identity Management, Q1 2014

The Nine Providers That Matter Most And How They Stack Up

by Andras Cser
with Stephanie Balaouras, Eve Maler, and Kelley Mak

WHY READ THIS REPORT

The privileged identity management (PIM) market has matured significantly during the past three years, and it continues to play a significant role in protecting an organization's data and in business continuity. In Forrester's 18-criteria evaluation of privileged identity management vendors, we identified the nine most significant solution providers — BalaBit, BeyondTrust, CA Technologies, Centrify, CyberArk, Dell, Hitachi ID, Lieberman Software, and Thycotic — in the category and researched, analyzed, and scored them. This report details our findings about how well each vendor fulfills our criteria and where they stand in relation to each other, to help security and risk (S&R) professionals select the right partner for their privileged identity management.

Table Of Contents

Notes & Resources

Forrester conducted product evaluations in Q3 2013 and interviewed nine vendor companies: BalaBit, BeyondTrust, CA Technologies, Centrify, CyberArk, Dell, Hitachi ID, Lieberman Software, and Thycotic.

Related Research Documents

An S&R Pro's Guide To Security To, In, And From The Cloud
December 31, 2013

The Forrester Cloud Security Compliance Checklist
November 8, 2013

Market Overview: Privileged Identity Management
December 8, 2010

PIM IS A BUILDING BLOCK AND ENABLER OF ON-PREMISES AND CLOUD SECURITY

Privileged identity management (PIM) (sometimes referred to as privileged access management, privileged user and password management, etc.) is about understanding who and what has access to system administrator and high-risk business, such as shared accounts. Privileged identity management is important because it:

- **Ensures that only authorized administrators and programs can access high-risk environments.** Disgruntled systems administrators or employees (e.g., employees who were recently laid off) have repeatedly caused catastrophic damage at firms and government agencies: Think of the 2011 McDonalds breach, the most recent NSA leak, or Target breach. Since systems administrators can bypass all application and database security controls, they have unfettered access to the most-sensitive data. Controlling, monitoring, and auditing their privileged access is extremely important to managing insider threats and preventing data breaches. This is even truer when your system administration is outsourced to an offshore third party, like Deloitte, IBM, or Wipro, and you can't control turnover of personnel.

- **Creates irrefutable and tamper-proof evidence for sensitive system access.** There are numerous compliance mandates that dictate access to sensitive systems: Almost every major regulation (e.g., HIPAA, FERC/NERC, SSAE 16 SOC 2, GLBA, PCI-DSS) has sections that pertain to adequate controls of environments. PIM solutions allow S&R pros to automatically track who checked out which password, for which system, at what time, and what they did with that password.

- **Secures "non-carbon-based" application-to-application high-risk access.** Almost every inquiry Forrester takes on PIM concerns high-risk access by nonhumans: For example, when a script or program needs root or database administration privileges to run properly, it needs the privileged level credentials, typically user name and password, to the system it calls programmatically. In many cases, IT pros have hard-coded these user names and passwords in clear text into configuration files, which may be viewed by unauthorized eyes and hard to maintain when target system privileged-user passwords change. Protecting API-level privileged calls is also a priority for many Forrester clients.

- **Enables cloud providers to protect their clients' workloads much better.** Most cloud providers (infrastructure-, platform-, but also software-as-a-service) hardly understand who accesses hypervisors and guest operating systems in a systems administrator capacity; it may be an employee of the cloud provider company or of the client. Controlling use of sensitive passwords and privileges on a large number of virtual environments is extremely complex, costly, and difficult without a PIM solution.

PIM Layers Password Safe, Session Recording, And Privilege Delegation

Forrester's customers want the smallest number of vendor relationships to manage as possible — this is why we evaluated PIM stacks or vendors that partner with one another to provide a complete PIM solution (see Figure 1). Here's how a modern PIM solution's components provide layered protection:

- **The password safe validates and checks privileged passwords in and out.** The password safe or vault is a component of the PIM solution that consists of a (web and/or Win32) user interface, a background program, and highly secured, encrypted password database. It periodically checks the validity of the stored passwords on the managed sensitive systems (endpoints) and alerts if it can no longer access an endpoint. System administrators or applications can log in to the user interface and check out passwords for a certain time period, such as 1 to 2 hours. Once the checkout time expires or the systems administrator or application checks the password back into the safe, the system can automatically change the privileged password on the endpoint. This effectively ensures that no system administrator or application has continuous access to all endpoints and the checkout of passwords is tracked.

- **Session recording ties password checkouts to actions.** Once a systems administrator checks out the password, the system can optionally spawn a session (e.g., SSH, RDP, VNC,) which is recorded, monitored, and controlled. This allows for a deep understanding of what a system administrator did on the endpoint after he checked out the password. Most solutions evaluated in this Forrester Wave can also search for strings in sessions (both on Windows and Unix) when you're looking for a command or configuration step that may have caused instability in the production environment.

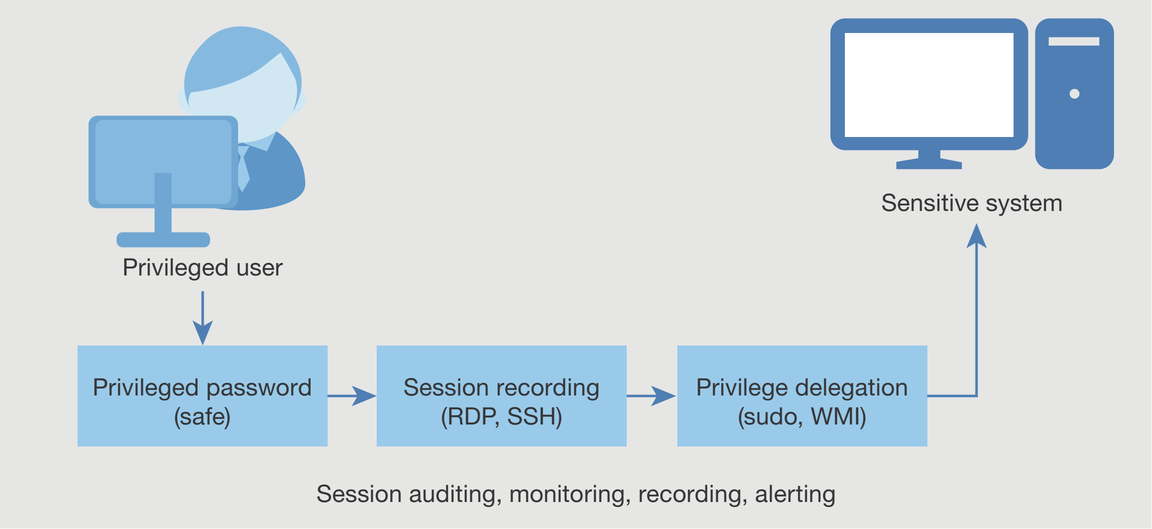
- **Privilege escalation and delegation on endpoints allows for least privileges.** For systems with a user access rights framework (e.g., Windows, Linux, Mainframe) it's a good idea to either create functional or service accounts that can only perform certain actions and control passwords to that functional account using the password safe. An even better solution is to use privilege escalation (or host access control) solutions on endpoints that allow a normal user to run certain commands but not others with system administrator rights. Many of the evaluated vendors' privilege escalation solutions build on the open source Unix "sudo" command.[1]

- **An Active Directory (AD) bridge allows sensitive access policy centralization on AD.** Many SMBs use AD as their authoritative user store and have built group policies to control user access on Windows endpoints. AD bridge solutions allow firms to extend this framework to non-Windows endpoints, such as Unix machines, and thus centralize privileged and nonprivileged access using a single solution. Many companies also use AD bridging technology to centrally provision and deprovision high privileges to users.

- **Offers access governance, SIM, and help desk integration, threat management, and reporting.** PIM access governance (a periodic review as to which system administrator has access to which machines) has gained importance in preventing data breaches: If a systems administrator has already moved to a different organization or left the company, he or she should not have access to the PIM solution and endpoints. Security information management (SIM) systems consume and provide information from and to PIM solutions; they ingest sensitive access information to alert on a threat. SIM solutions also provide information to a PIM system to block risky systems administrator access based on the administrator's activity recorded in the SIM system. Good PIM systems should allow for easy-to-define, ad hoc reports and visual, clickable dashboards to make the "watching the guards" process more streamlined.

Figure 1 Layers Of A PIM Solution Provide Sound Security For Administrative Users

Anatomy of privileged identity management


Sensitive system
Privileged user
Privileged password (safe)
Session recording (RDP, SSH)
Privilege delegation (sudo, WMI)
Session auditing, monitoring, recording, alerting

109901 Source: Forrester Research, Inc.

Hypervisor Support And Identity Intelligence Differentiate Vendors

To evaluate the vendors in the PIM market, we concentrated on several differentiating criteria but also on criteria that, while difficult to truly differentiate on, are nevertheless important:

- **Hypervisor support and headless operations are essential for cloud security and providers.** Infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) providers increasingly use PIM solutions to control who has access to which sensitive resource in a workload. Understanding and controlling what a system administrator can and can't do in a hypervisor (what guest images they can start, stop, migrate, and remove, when, from where, etc.) at scale (for thousands of hypervisors and guest images) is highly desirable if a cloud provider wants to even maintain its security certification status, such as SSAE 16 SOC 1 and 2.[2] PIM solutions that can operate in a completely API-centric mode without web-based access or policy management and which support high levels of multitenancy (policy and workload separation) are essential for cloud providers to build a solid PIM infrastructure for themselves and for their clients.

- **Identity intelligence eases the burden of policy creation and maintenance.** You can only protect and code policies against threats you have identified and understand; as a result, any new or emerging threat (e.g., APT, data breaches, excessive or anomalous system privilege use) is a nightmare: You can't effectively code PIM policies against it. Enter identity intelligence: building normal behavioral models for system administrators' actions when they check out passwords or type administrative commands on command line or graphical sessions. Solutions increasingly focus on identifying and alerting on any behavior that is different from the user's past or the user's peers' behavior and allow for a better scrutiny as to why a system administrator suddenly dumped the entire CRM database at 5:50 p.m. this Friday but never before.

- **Security and breadth of endpoint support is constantly growing but is nondifferentiating.** All solutions evaluated in this Forrester Wave provide: 1) extensive support for many different types of endpoints: Windows flavors, many different vendors' Unix environments, and more exotic systems (e.g., mainframe, network equipment); 2) at least 1,024 bit encryption of the privileged passwords stored; 3) some sort of a role-based access control that allows groups of systems administrators to access groups of machines; and 4) regular updates to their user interface to provide a good user experience.

PRIVILEGED IDENTITY MANAGEMENT EVALUATION OVERVIEW

To assess the state of the market for PIM solutions and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top PIM vendors.

Evaluation Criteria

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 18 criteria, which we grouped into three high-level buckets:

- **Current offering.** We looked at how: 1) the password safe supports endpoints, application-to-application management, database pools and discovery of endpoints, agent-based and agentless deployment, hypervisors, and spawning administrative sessions; 2) the privileged session management supports SSH and RDP session recording, behavioral modeling, and searching of recorded sessions, dual control, API calls; 3) the privilege escalation component supports Unix, hypervisors, Windows endpoints, and proxy-based operations; and 4) the AD bridge supports endpoints, and mobile devices. Finally, we looked at the solution's overall support for cloud applications, SIM, and help desk integration, as well as attestation of privileged users and high availability and scalability.

- **Strategy.** We looked at vendor staffing (how many people are developing and selling the solution), the vendor's overall, mobile, cloud, virtualization, and identity intelligence strategy, as well as customer satisfaction, partner ecosystem, solution pricing models, and vendor's PIM revenue. We also provided nonscored information on what the vendor believes the top differentiating features of its PIM solution are.

- **Market presence.** We looked at the number of organizations and their growth that use the vendor's PIM solution in production as well as geographical split and balance of the vendor's PIM revenues.

Inclusion Criteria

Forrester included nine vendors in the assessment: BalaBit, BeyondTrust, CA Technologies, Centrify, CyberArk, Dell, Hitachi ID, Lieberman Software, and Thycotic. Each of these vendors has (see Figure 2):

- **PIM covering password safe, session recording, privilege escalation, and AD bridge.** Forrester invited vendors that provide at least two of the above functionality with internally developed components, and the rest using OEM relationships or partnerships.

- **At least $3 million in PIM revenues and 200 paying, production customers.** In order to look at companies with potential to execute against strategy, we included only vendors who have a significant paying, production customer base and vendors that make at least $3 million in PIM annual revenues (including perpetual product license and subscription fees).

- **Ability to provide unfettered access to an online demonstration environment.** Forrester not only conducted interactive demonstrations with vendors but also requested that vendors provide unrestricted access to a demonstration environment where Forrester could independently verify and repeat demo and criteria scenarios.

- **Significant mindshare with Forrester's customers.** In this Forrester Wave evaluation, we included vendors for whom we regularly receive questions from our customer base. Based on client conversations and inquiries we included PIM vendors which represent thought leadership in PIM.

Forrester also invited IBM, Fisher International, ManageEngine, NetIQ, Oracle, and Xceedium, but these vendors declined to participate.

Figure 2 Evaluated Vendors: Product Information And Selection Criteria

Vendor	Product evaluated	Product version evaluated	Product release date
BalaBit IT Security	Shell Control Box	3F4	February 2013
BeyondTrust	PowerBroker Identity Services PowerBroker for Unix and Linux PowerBroker Password Safe Retina CS Threat Management Console PowerBroker for Windows	7.5.0 7.5.0 SP4 CR12 4.5.1 6.0.1	June 2013 June 2013 June 2013 June 2013 June 2013
CA Technologies	CA ControlMinder CA ControlMinder for Virtual Environments CA GovernanceMinder CA Session Recording	12.7 2 12.6.01 5.6.4	April 2013 October 2011 June 2013 February 2013
Centrify	Centrify Server Suite	2013.1	January 2013
CyberArk	CyberArk Privileged Account Security Solution	7.2	June 2013
Dell	Privileged Access Suite for Unix Privileged Password Manager Privileged Session Manager	2.5 2.5	April 2013 December 2012
Hitachi ID	Hitachi ID Privileged Access Manager	8.2	May 2013
Lieberman Software	Enterprise Random Password Manager (ERPM)	4.83.6	May 2013
Thycotic	Secret Server	8.2.00000	July 2013

Vendor selection criteria

A PIM offering covering password safe, session recording, privilege escalation, and AD bridge. Forrester invited vendors that provide at least two of the above functionalities with internally developed components, and the rest using OEM relationships or partnerships.

At least $3 million in PIM revenues and 200 paying, production customers. In order to look at companies with potential to execute against strategy, we included only vendors who have a significant paying, production customer base and vendors that make at least $3 million in PIM annual revenues (including perpetual product license and subscription fees).

Vendors who could provide unfettered access to an online demonstration environment. Forrester not only conducted interactive demonstrations with vendors but also requested that vendors provide unrestricted access to a demonstration environment where Forrester could independently verify and repeat demo and criteria scenarios.

Significant mindshare with Forrester's customers. In this Forrester Wave evaluation, we included vendors about whom we regularly receive questions from our customer base. Based on client conversations and inquiries, we included PIM vendors that represent thought leadership in PIM.

Source: Forrester Research, Inc.

EVALUATION ANALYSIS: CA TECHNOLOGIES LEADS A MATURE MARKET

The evaluation uncovered a mature market in which many vendors provide viable alternatives for PIM (see Figure 3):

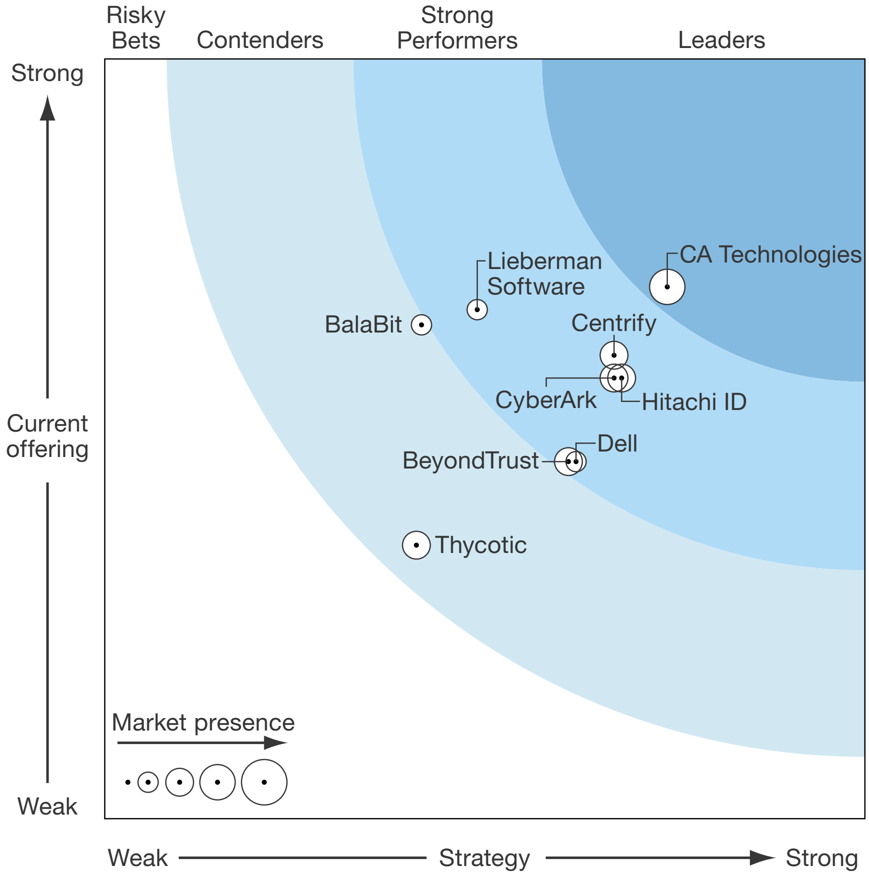
- **CA Technologies leads the pack.** CA Technologies has only recently built its privileged password safe but has long been a leading player in privilege escalation (CA Access Control, recently renamed to CA ControlMinder). CA OEMs ObserveIT's leading session management and recording solution and provides best-in-class identity and access governance around privileged users. CA Technologies' vision for PIM is the broadest of all evaluated vendors, integrating PIM into its cloud-based PIM solution, CA CloudMinder.

- **There is a crowded field of Strong Performers.** BeyondTrust, Centrify, CyberArk, Dell, Hitachi ID, and Lieberman Software all offer competitive options. Although BalaBit and Lieberman Software offer a combination of surprisingly strong features in the current offering, they lack the reach that larger vendors have. BeyondTrust, Centrify, CyberArk, Dell, and Hitachi ID offer mature and competitive offerings, but they lack functionality, strategy elements of a Leader.

- **BalaBit And Thycotic lack important functionality.** While Thycotic provides robust password safe and session recording functionality (as well as web-based AD group management services, which was not evaluated in this Forrester Wave), it provides no privilege escalation or AD bridging capabilities and is fairly small in terms of employees and revenues, raising questions of long-term stability. BalaBit provides strong session management and privilege escalation capabilities but provides no own password safe services.

This evaluation of the PIM market is intended to be a starting point only. We encourage clients to download and view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

Figure 3 Forrester Wave™: Privileged Identity Management, Q1 '14



Source: Forrester Research, Inc.

Figure 3 Forrester Wave™: Privileged Identity Management, Q1 '14 (Cont.)

	Forrester's Weighting	BalaBit	BeyondTrust	CA Technologies	Centrify	CyberArk	Dell	Hitachi ID	Lieberman Software	Thycotic
CURRENT OFFERING	50%	3.25	2.35	3.50	3.05	2.90	2.35	2.90	3.35	1.80
Privileged password safe	15%	5.00	3.00	4.00	2.00	4.00	2.00	4.00	5.00	3.00
Privileged session spawning	15%	3.00	0.00	4.00	4.00	3.00	3.00	4.00	3.00	3.00
Privileged session recording	15%	4.00	3.00	4.00	4.00	2.00	3.00	4.00	4.00	1.00
Privileged session management	15%	4.00	0.00	2.00	0.00	2.00	1.00	1.00	4.00	0.00
Privilege escalation	15%	2.00	3.00	4.00	4.00	4.00	2.00	0.00	2.00	0.00
Active Directory bridge	5%	0.00	4.00	2.00	5.00	1.00	4.00	0.00	0.00	0.00
Cloud and SIEM support	5%	2.00	4.00	5.00	4.00	4.00	2.00	4.00	4.00	4.00
Reporting and integration	10%	3.00	5.00	3.00	4.00	3.00	3.00	5.00	3.00	4.00
Attestation and performance	5%	3.00	2.00	3.00	2.00	2.00	2.00	5.00	3.00	3.00
STRATEGY	50%	2.10	3.05	3.70	3.35	3.35	3.10	3.40	2.45	2.05
Vendor staffing	15%	3.00	4.00	5.00	4.00	4.00	5.00	5.00	2.00	0.00
Future plans	25%	3.00	2.00	4.00	2.00	2.00	1.00	4.00	2.00	1.00
Customer satisfaction	15%	2.00	4.00	2.00	5.00	3.00	5.00	2.00	4.00	5.00
Partners	15%	0.00	4.00	4.00	3.00	5.00	3.00	1.00	1.00	1.00
Solution pricing	15%	3.00	3.00	4.00	4.00	3.00	3.00	5.00	2.00	4.00
Revenue	15%	1.00	2.00	3.00	3.00	4.00	3.00	3.00	4.00	2.00
Differentiating and unique strategy for features of the solution	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
MARKET PRESENCE	0%	1.50	2.50	3.50	3.00	2.50	2.00	2.50	1.50	3.00
Installed base	50%	1.00	3.00	2.00	4.00	2.00	3.00	2.00	1.00	4.00
Verticals and geographies	50%	2.00	2.00	5.00	2.00	3.00	1.00	3.00	2.00	2.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

VENDOR PROFILES

Leaders

- **CA Technologies assembles session recording, virtualization support, and privilege escalation.** CA Technologies is long past the acquisition fever: This vendor has gone back to the drawing board to understand how to integrate a comprehensive and robust PIM portfolio consisting of organically developed (password vault, privilege escalation, attestation, SIM, help desk) PIM capabilities with OEMs and partnerships (ObserveIT OEM for session recording and HyTrust for comprehensive virtualization support). CA Technologies also uses its broad partner ecosystem and partner base globally to sell and integrate its PIM solution. The password safe lacks ability to discover endpoints through IP addresses or IP address ranges, and the session recording solution today lacks ability to use multiple keys for session recording to avoid disclosing passwords. The privilege escalation solution is kernel agent-based that provides outstanding protection but can limit its deployment due to customer-dictated constraints.

Strong Performers

- **Centrify extends its AD bridging capabilities to PIM.** Centrify has been extending its AD bridge capabilities to password safe and session management and privilege escalation capabilities. The solution extensively supports cloud applications, multitenancy for centralized policy management across its components, and agent-based and agentless deployment for session recording. Centrify has the largest number of paying, production customer organizations. However, it does not support dual control of monitored sessions, hypervisor API call management, and attestation of privileged users.

- **Hitachi ID builds its PIM solution on its identity management platform.** Hitachi ID's solution is highly fault tolerant (the vendor even built its own multimaster but optional database replication for PIM) and comes with built-in attestation and separation of duties capabilities. The solution offers broad endpoint support, wide endpoint discovery capabilities, and agent-based or agentless deployment options. However, the solution provides no dual control for session management and lacks WMI support for Windows endpoints. There is no privilege escalation or AD bridging capabilities.

- **CyberArk branches out from password safe to APT threat mitigation and social media.** CyberArk has been one of the pioneers of PIM; its password vault solution has been one of the first in the market. The vendor provides hypervisor support, outstanding application-to-application, and database connection pool password management. CyberArk also uses its SIM integration for privileged threat detection and mitigation. The solution today lacks an AD bridge, does not offer searchable Windows session logs (this is planned), and provides no separation of duties enforcement or PIM attestation capabilities.

- **Lieberman Software password safe shows signs of aging, focuses on headless MSP operations.** Of the solutions evaluated, Lieberman Software has one of the most robust policy management, application-to-application password management and endpoint discovery capabilities for the password safe. The solution's password safe consists of the legacy ERPM (AKA Roulette) administrative user interface for policy management as well as the more modern web-based user interface for everyday use of the product. The password safe provides direct support for hypervisors. For session recording and privilege escalation, Lieberman Software partners with BalaBit plus ObserveIT and ViewFinity, respectively. The company is well under way to build a fully headless PIM platform for use by managed security services providers.

- **Dell provides agent and agentless deployment and hypervisor support for the password safe.** Dell (based on the eDMZ EPAR solution that Quest acquired) offers an industrial strength password safe that supports agent-based and agentless deployment and hypervisors. The solution also supports spawning and extensive searching of sessions. However, the vendor lacks a cloud-based PIM strategy, offers no native mobile application for the password safe, and lacks privilege escalation on Windows endpoints.

- **BeyondTrust's single platform offers a great AD bridge and shared policy management.** BeyondTrust provides excellent privilege escalation for Unix (legacy Symark) and Windows endpoints and agent-based application control on Windows endpoints. All of the solution's components are in-house-developed now (after the Likewise acquisition for AD bridging and the BeyondTrust acquisition for Windows privilege escalation), which puts the company into a uniquely strong position for future development. Today, the password safe solution provides no capabilities for session spawning (this is planned), no virtualization or SAML support. The session recording solution does not support agentless deployment, only agent-based.

Contenders

- **BalaBit offers industrial strength session monitoring and recording.** BalaBit's appliance-based solution can be deployed in a variety of ways (router, bastion, etc.) in line between the system administrator and the managed endpoint. The solution provides extensive and extensible support for network protocols beyond SSH and RDP: VNC, X11, Citrix ICA, HTTP, and other session protocols are supported out of the box and the administrator can define new connections easily. BalaBit's solution can selectively permit or deny access to certain protocol-specific channels. The session recording solution offers optical character recognition (OCR) on Windows, which allows for alerting and policy management of non-command-line administrative actions. The solution provides a very effective, interactive, and timeline-based session recording search. However, the solution today lacks agent-based recording and offers neither hypervisor support nor an AD bridge.

- **Thycotic offers robust application-to-application password management and multitenancy.** Thycotic offers a robust password safe with outstanding application-to-application management capabilities, which offers both agent-based and agentless deployment options. Thycotic also provides rich, native mobile applications for its password safe to be used in disconnected, offline environments. The vendor lacks Windows endpoint session recordings, privilege escalation, and AD bridging capabilities. Compared with other vendors, it has a much smaller number of employees and a smaller partner base, which raises concerns with Forrester's customers.

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 3 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

Forrester used a combination of the following data sources to assess the strengths and weaknesses of each solution:

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.

- **Product demos and unsupervised usage.** We asked vendors to conduct demonstrations of their product's functionality. We used findings from these product demos to validate details of each vendor's product capabilities. We also gained unsupervised access to environments in which we could test the products' features.

- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with two of each vendor's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and we encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. For more information on the methodology that every Forrester Wave follows, go to http://www.forrester.com/marketing/policies/forrester-wave-methodology.html.

Integrity Policy

All of Forrester's research, including Forrester Waves, is conducted according to our Integrity Policy. For more information, go to http://www.forrester.com/marketing/policies/integrity-policy.html.

ENDNOTES

[1] "Sudo" is a command that allows nonprivileged, regular users to run commands as root, the highest privilege user on a Linux system. Source: Sudo Main Page (http://www.sudo.ws/).

[2] For more information on these audit standards and their effectiveness, see the October 31, 2011, "SAS 70 Out, New Service Organization Control Reports In" report.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals

Forrester Research (Nasdaq: FORR) is a global research and advisory firm serving professionals in 13 key roles across three distinct client segments. Our clients face progressively complex business and technology decisions every day. To help them understand, strategize, and act upon opportunities brought by change, Forrester provides proprietary research, consumer and business data, custom consulting, events and online communities, and peer-to-peer executive programs. We guide leaders in business technology, marketing and strategy, and the technology industry through independent fact-based insight, ensuring their business success today and tomorrow. 109901