On the Radar: Prevoty provides a runtime application security platform for the enterprise

Protection for large-scale runtime environments

Publication Date: 29 Dec 2015 | Product code: IT0021-000138

Richard Absalom

Summary

Catalyst

There are multiple approaches for monitoring and protecting enterprise applications and data in real time. However, a rule-based approach that relies upon securing the perimeter defenses of an enterprise from attack can become increasingly complex and difficult to maintain over time. Once such defenses are breached, the consequences and effort of remediation can be massive. Prevoty's approach relies upon securing any form of app from the inside, without introducing processing overheads or network latency. It is targeting large enterprises that depend on applications for their daily business.

Key messages

- Prevoty uses a self-contained in-app contextual processing and analysis engine to automatically secure content, queries, and users in real time.
- It offers extensive support, including protection against the 10 most critical web application security risks identified by the Open Web Application Security Project (OWASP).
- It supports an extensive range of databases and programming languages.

Ovum view

Security is an increasingly important strategic issue for the enterprise. Protection from a large, diverse, and rapidly changing set of vulnerabilities requires a highly dynamic approach that can detect abnormal behavior and respond appropriately in real time. Doing this for modern apps is one thing, but providing the same level of support for legacy applications is even more challenging. Prevoty offers an elegant solution that supports all kinds of apps, including those that are cloud-based, in a consistent fashion without adding performance overheads.

Recommendations for enterprises

Why put Prevoty on your radar?

Prevoty will be a welcome addition to the armory of online businesses, particularly those with a wide variety of constantly changing applications that require protection. Prevoty offers runtime protection against the most threatening vulnerabilities, as well as those that are as yet unknown. The ease with which it is deployed and the broad range of databases and languages supported make it suitable for large-scale enterprises with a wide variety of business-critical applications to protect.

Highlights

Background

Prevoty was founded in March 2013 and is headquartered in Menlo Park, Los Angeles. Co-founder and CTO Kunal Anand was previously head of technology at BBC Worldwide, responsible for all engineering, operations, results, and security. He was acutely aware of how vulnerable applications were if the focus on security was to put technologies in front of the applications to protect them.

Together with Julien Bellanger, Prevoty's co-founder and CEO, Anand approached a strong set of initial angel investors that included Eric Hahn, the chairman of Proofpoint and CTO of Netscape. They went on to secure seed funding with further investors that included Shinya Akamine, the co-founder and CEO of Postini before it was acquired by Google. A further Series A funding round that included USVP brought the company's total funding to more than $11.5m. The company has achieved growth of more than 100% year on year.

Main features of Prevoty release 3+

Prevoty provides application security monitoring and protection from inside each application at runtime. The new release increases performance over previous releases by a factor of ten due to the placement of processing and analysis within each app.

- There are no changes required to the applications.
- Applications call a security engine deployed in the cloud, as a virtual appliance or a self-contained plug-in in the application.
- There is no network I/O call, very low usage of CPU, and very low usage of memory inside an application.

Monitoring and application security intelligence:

- Prevoty provides insights into what attacks are currently targeting production applications.
- Prevoty identifies who, what, where, and when an attack is being made and makes this visible.

Runtime application self-protection (RASP):

- Prevoty supports automatic vulnerability mitigation.
- Prevoty protects content against cross-site scripting (XSS), and protects databases against SQL injection, tokens, cross-site request forgery (CSRF), and many other vulnerabilities.
- It provides the holding time needed for the development teams to remediate critical vulnerabilities.

How it works

- Prevoty has SDK support and plug-ins that use deep instrumentation to inspect application activity at runtime and call the security engine for payload analysis.
- Prevoty uses language-based security (LangSec) for this analysis rather than a pattern- or signature-based approach that might require matching against thousands of signatures and hence introduce latency issues. LangSec provides a virtual vision of how the payload will run to identify potentially malicious behavior in advance of execution.
- If the payload is malicious, an alert is issued to log files and any configured security information and event management system (SIEM), and is exposed via a Sentinel console. The intelligence can also be passed on to logging tools such as Splunk, IBM QRadar, and HP ArcSight, and to network appliances such as web application firewalls (WAF), next-generation firewalls (NGFW), and intrusion prevention systems (IPS).

- If protection mode is enabled, the payload is neutralized and secured payloads are instantly sent back to the application.

Current position

Prevoty is a young company that is growing fast, with excellent backing. Since the company entered the market in 2014 it has gained strong traction, mainly with large Fortune 500 enterprises in regulated industries such as financial services that have significant in-house application development efforts. However, other industries that either rely on content to drive their businesses or face recurrent public breaches, such as retail and healthcare, also present good opportunities. Prevoty has approximately 20 customers, which include several of the top financial and retail customers, including a major global payments technology company and a major online retailer. It is also represented in other verticals, for example by Oscar Healthcare, Bleacher Report, MINDBODY, Michigan State University, and Hulu. Partners include Amazon Web Services, WhiteHat Security, and Splunk.

Prevoty does not release detailed financial figures. Annual corporate revenue for 2014 was less than $100m, and Prevoty currently has fewer than 50 employees.

Software licenses are charged on an annual basis. Products are sold by or delivered through solution providers, system integrators, VARs, or other channel partners. The service is offered via a capacity-based model: enterprises only pay for the level of capacity they require. Similarly to the way that enterprises buy load balancers, Prevoty's service capacity depends on the number of requests per second that the security engine needs to process (regardless of how many applications are taking advantage of the service). Prevoty's engine was designed to scale horizontally, automatically, and transparently, adding capacity as needs grow. Thus, scalability is not an issue. It currently supports individual customers processing up to 50,000 requests per second at peak times. Enterprises can start small and then add capacity on demand.

Data sheet

Key facts

Table 1: Data sheet: Prevoty

Product name	Prevoty	**Product classification**	Runtime application security platform
Version number	R3	**Release date**	November 2015
Industries covered	Banking, insurance, financial services, media, retail, healthcare, education, e-commerce	**Geographies covered**	North America
Relevant company sizes	Enterprise	**Licensing options**	Subscription-based
URL	www.prevoty.com	**Routes to market**	Direct and indirect
Company headquarters	Menlo Park, Los Angeles	**Number of employees**	Fewer than 50

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further Reading

2016 Trends to Watch: Security, IT0022-000522 (October 2015)

On The Radar: Bluebox Security, IT0021-000050 (January 2015)

Authors

Martin Gandar, Associate Senior Analyst

martin.gandar@ovum.com

Richard Absalom, Principal Analyst, Enterprise Mobility

richard.absalom@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum’s consulting team may be able to help you. For more information about Ovum’s consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo