On the Radar: NextLabs offers protection across enterprises' applications and data

Protection for data "anywhere," regardless of application, location, transition state, or device

Publication Date: 24 Mar 2017 | Product code: IT0018-001527

Alan Rodger

Summary

Catalyst

Data protection is a key organizational capability, and the right level of protection must be applied to different data types in all places and situations to meet business needs. Implementing strong protection without a smart approach can result in high overhead costs, and can also limit flexibility to accommodate the change that is necessary as roles, business needs, and data evolve. Integrating the protection applied to data access rights across business applications, persistent protection of files shared over communication channels such as email and in the cloud, as well as protection against unauthorized access via other means (e.g. using direct access to a database, or intercepting data in transit) can increase efficiency and reduce risk on an ongoing basis.

Key messages

- NextLabs' solutions can protect data from unauthorized access via and across applications, impose persistent data protection onto files/documents shared and on the move, as well as provide other data protection methods.
- Data access rights can be controlled by leveraging various existing attributes, taking into account user information (e.g. identity, function, and organization structure), the attributes of the resource (e.g. nature of the data being accessed, and its classification and metadata), environment attributes, and the action requested, all in real time.
- Using access management controls, rights management technology, and digital rights protection with strong encryption, data can be protected while it is on any device, stored in any application, in transit via networks, or at rest on a file repository.
- Protection (which can encompass mobile and cloud environments) is integrated out-of-the-box for common enterprise applications, and can be added to any custom application through standards-based software development kits (SDKs) and APIs.

Ovum view

While increasing cyber-attack and data-focused compliance needs arising from privacy-related legislation such as the EU General Data Protection Regulation (GDPR) are driving organizations to implement stronger data protection controls, they also require a policy-driven, integrated approach to the overall problem. This not only is better from a compliance assurance perspective but also reduces the scale of overhead costs associated with implementing an advanced capability. NextLabs' data-centric security protection integrates Entitlement Management and Enterprise Digital Rights Management capabilities on a centralized policy management platform, enabling central enforcement of policies based on a wide range of attributes. Protection is dynamically applied via a real-time assessment of user and data attributes, across all systems and applications to protect data wherever it resides or moves. Ovum believes that NextLabs is well positioned as an expert in this area and could prosper well as a result, particularly given the deep, out-of-the-box integration that it provides with solutions from SAP, Microsoft, and Siemens (via joint solution and go-to-market partnerships). This enables advanced protection facilities to be more easily implemented.

Recommendations for enterprises

Why put NextLabs on your radar?

Organizations of all kinds are pressured to consider automating and strengthening protection of their data, to enable strategic goals such as reduce information-sharing risk across organizational borders, and to avoid compliance problems arising from the growing data privacy regulatory burden. NextLabs' solutions are worthy of serious consideration by large organizations looking to address these issues, and seeking to gain both flexibility and strong control that will support future business change while reducing risk, cutting overheads, and improving agility.

Highlights

Background

NextLabs was founded in 2004 by Keng Lim, a veteran of numerous advanced technology companies including Netscape and Sygate Technologies. Its leadership team has broad experience from many technology companies, with a particular emphasis on advanced security solutions. NextLabs is privately owned, with funding from a small number of Silicon Valley investors. It holds more than 50 patents relating to specialist technology capabilities that are deployed within its solutions, and states that it has applied for 30 additional patents.

The company has in the past focused on vertical industries in which there are key, specific data protection challenges. As such, its customers include numerous international defense and intelligence agencies, as well as well-known companies including BAE Systems, AXA, Pratt & Whitney, Saab Group, Qualcomm, Boeing, Lockheed Martin, and Morgan Stanley. Today, its technology evolution equips NextLabs with data protection capabilities that a much greater variety of organizations will need to consider because of the problems they face from compliance with privacy regulations.

Current position

The key to the power and flexibility provided by NextLabs is that security is centered on the organization's data, and on knowledge of what protection is appropriate to each data element. The solution combines this knowledge with the native application integration by leveraging the metadata and classification of the data object (e.g. customer, supplier, sales order, or product) from the application, using it to automatically classify legacy data, new data, and data transiting out of application into storage outside the application. NextLabs also offers capabilities to enable user-driven classification and rule-based bulk classification of data. Ongoing policy control over data access identifies attributes and applies protection appropriate to the user that is requesting access, on any device, via any application, or when data is in transit, on the move, or at rest. Centrally managed authorization policies are dynamically evaluated and enforced based on user attributes (e.g. citizenship, security clearance, department, or roles), resource attributes (e.g. data classifications, content, and transaction details), and environment attributes (e.g. time of day, location, authentication scheme, and device type). User attributes used to determine access rights can be resident in any data source including internal or cloud-based applications, and external identity definitions (e.g. federated from a business partner).

NextLabs solutions use its standard-based Dynamic Authorization technology, based on eXtensible Access Control Markup Language (XACML), to implement the attribute-based access control (ABAC) capability. This allows attributes of a user identity to be assessed via policy against the protection that has been specified for data. The solutions have native, out-of-the-box application-level integrations with solutions from SAP (ERP, S/4HANA, CRM, BW, PLM, and more), Siemens (PLM and MES), and Microsoft (SharePoint, Windows, Exchange, Dynamics365, Office 365, Skype for Business, and more), and they enable authoring, management, and deployment of policies for other application types using an XACML-based, 4GL policy language. The solutions also measure the effectiveness of information compliance and protection controls with continuous analysis and reporting. The fine-grained protection applied at attribute level permission can enable applications to redact parts of a dataset, enabling users to gain a view that is appropriate to their authorization credentials. Data leaving the application environment (e.g. via email) is detected and automatically protected with persistent digital rights, using strong encryption. Subsequently, files protected in this manner can only be opened by an authorized user, regardless of location or environment context, and of the document type of the file. Documents are automatically protected based on policy and requirements at the time of upload or download.

Data sheet

Key facts

Table 1: Data sheet: NextLabs

Product name	Entitlement Management, Enterprise Digital Rights Management, Control Center	**Product classification**	Data security, entitlement management, digital rights management, dynamic authorization management
Version number		**Release date**	2016
Industries covered	Aerospace/defense, financial services, high tech, manufacturing, life sciences and pharmaceuticals, chemicals, automotive, government, energy	**Geographies covered**	North America, EMEA, Asia-Pacific
Relevant company sizes	Large	**Licensing options**	Term license, and subscription per CPU core or user
URL	www.nextlabs.com	**Routes to market**	Direct sales; indirect sales via system integrators and consulting firms; partner channel – SAP, Siemens, Microsoft (SAP resells EDRM and EM globally)
Company headquarters	San Mateo, California, US	**Number of employees**	About 200

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

Data Privacy Legislation Impact on Enterprises, IT0018-001493 (April 2016)

"Identity is the missing link between privacy and security," IT0014-003238 (February 2017)

Author

Alan Rodger, Senior Analyst, Infrastructure Solutions

alan.rodger@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

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

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