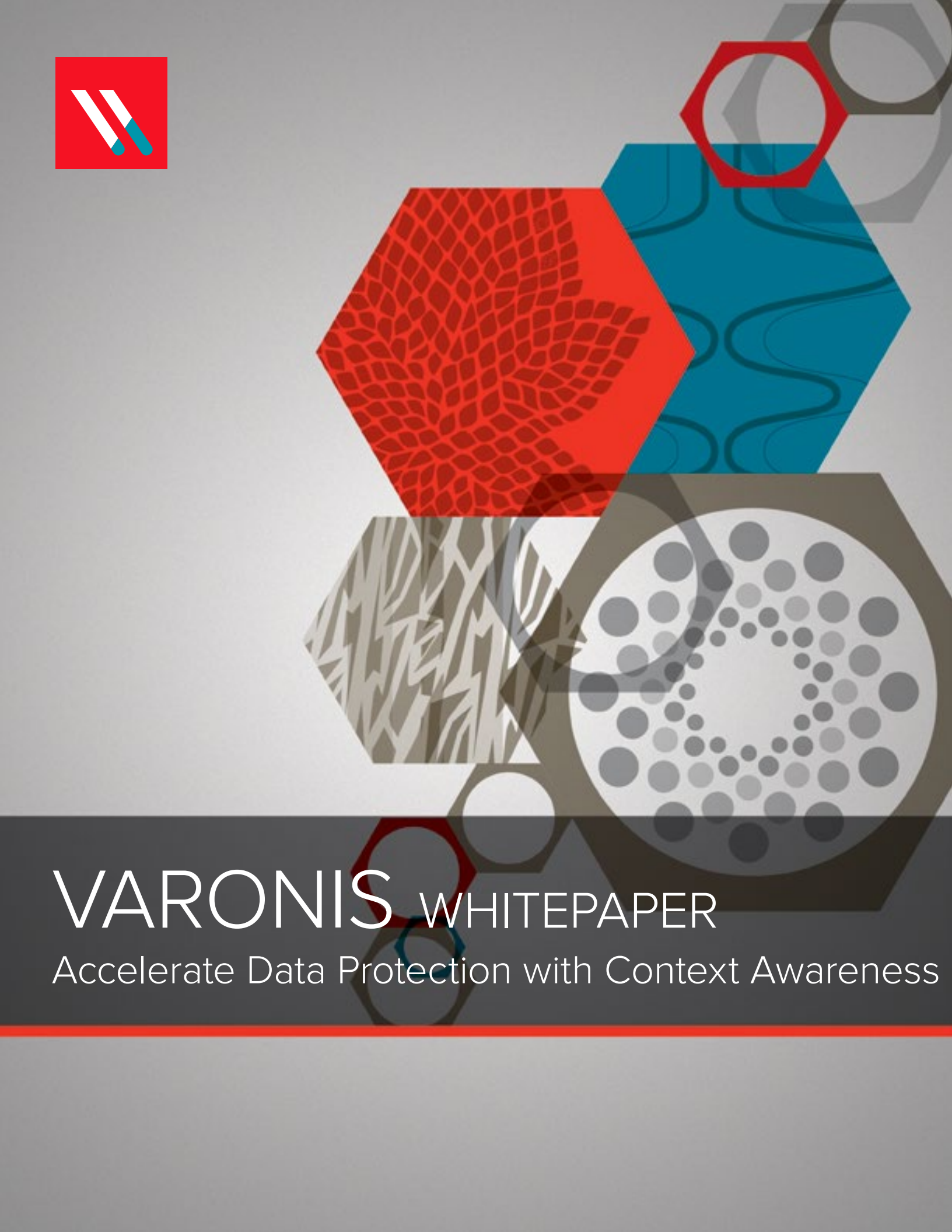

VARONIS WHITEPAPER

Accelerate Data Protection with Context Awareness

CONTENTS

ACCELERATE DATA PROTECTION WITH CONTEXT AWARENESS

The Inevitable Breach

Odds are fairly high that there is sensitive data on your corporate network that is overexposed and itching to escape. But will it? Forrester thinks so – in a recent survey, 22% of security decision-makers reported a data breach in the past twelve months[1], and at an average cost of $7.2 million per breach[2], it's no shock that organizations are constantly working to strengthen their defenses.

IT and security professionals are in a perpetual arms race with attackers. Packet sniffers, firewalls, virus scanners, and spam filters are doing a good job securing the borders, but what about insider threats? According to Forrester, "trusted" insiders and business partners, malicious or not, are responsible for 43% of security breaches[3].

The prospect of legitimate, authorized users unwittingly (or wittingly) leaking critical data just by showing up to work and accessing data that is available to them is enough to make your skin crawl. Analyst firms estimate that in 5 years, unstructured data will grow by 650%. The risk of data loss is increasing above and beyond this explosive rate, as more dynamic, cross-functional teams collaborate and data is shuffled between network shares, email accounts, SharePoint sites, mobile devices, and countless other platforms. As a result, security professionals are turning to data loss prevention (DLP) solutions for help.

DLP IS NOT A PANACEA

DLP solutions typically take a three-pronged technology approach to protecting data:

ENDPOINT PROTECTIONS

1. encrypt data on hard drives and disable external storage to stop data from escaping via employee laptops and workstations.

NETWORK PROTECTIONS

2. scan and filter sensitive data to prevent it from leaving the organization via email, HTTP, FTP and other protocols.

SERVER PROTECTIONS

3. focus on content classification and identifying sensitive files that need to be protected before they have a chance to escape.

Early solutions that focused primarily on endpoint and network protections were quickly overwhelmed by the massive amounts of data traversing countless networks and devices. “For DLP technology to be successful, you must inventory and classify all of your sensitive data and understand your information flows” advises Forrester. “This is hard to do if you have hundreds, possibly thousands, of terabytes of unstructured data.”[4]

Unfortunately, DLP’s file-based approach to content classification is cumbersome at best. Upon implementing DLP it is not uncommon to have tens of thousands of “alerts” about sensitive files. Where do you begin? How do you prioritize? Which incident in the colossal stack represents a $7.2 million risk that warrants your immediate, undivided attention?

The challenge doesn’t stop here. Pick an incident/alert at random – the sensitive files involved may have been autoencrypted and auto-quarantined, but what comes next? Who has the knowledge and authority to decide the appropriate access controls? Who are we now preventing from doing their jobs? How and why were the files placed here in the first place?

You can see a pattern forming here – with traditional DLP solutions we end up with excellent questions, but we urgently need answers that a DLP solution alone cannot provide.

DLP solutions provide very little context about data usage, permissions, and ownership, making it difficult for IT to proceed with sustainable remediation. IT is not qualified to make decisions about accessibility and acceptable use on its own; even if it were, it is not realistic to make these kinds of decisions for each and every file.

All preventive controls (e.g., quarantining and encryption) must be implemented and maintained correctly. Without proper ongoing maintenance, these controls are either too permissive, and therefore ineffective, or too restrictive, leading to a deleterious effect on collaboration and business activity.

The reality is that sensitive files are being used to achieve important business objectives. We can't deny the benefits of digital collaboration. Instead, we must achieve secure collaboration. In order to do this, sensitive data must be stored somewhere that allows people to collaborate with it while at the same time ensuring that only the right people have access and that their use of sensitive data is monitored.

Network and Endpoint DLP solutions are like security guards that detain every single patron as they try to leave the bank with cash in hand, without any clues to help sort out the criminals from the customers. Server DLP is a bean counter that dutifully points out that there is a lot of money in the bank, stored in a lot of places. What's needed is intelligence and automation for the tellers, empowering them to correctly and efficiently govern the dissemination of cash, leaving only the fringe cases to the guard.

CONTEXT IS KING

When an incident occurs or an access control issue is detected, we shouldn't turn our business into a giant panic room. Rather, our software solutions should enable the businesspeople with the most knowledge about the data to take the appropriate action to remediate risks quickly, in the right order. We can't do this, however, without enterprise context awareness – i.e., knowledge of who owns the data, who uses the data, and who should and shouldn't have access.

Forrester states, "To manage and protect information effectively, particularly from insiders and business partners, information risk and security professionals must integrate identity and access management with data life-cycle management. Forrester refers to this as protecting information consistently with identity context (PICWIC)."[5]

The central idea of PICWIC is that you should assign data to business owners at all times. When you combine identity context with data management, you can properly provision new user accounts with correct levels of access, recertify access entitlements regularly, and take the appropriate actions when an employee changes roles or is terminated. By following these best practices, you will reduce the chances of accidental data leakage while lifting a substantial burden from IT.

SOUNDS GREAT; SIGN ME UP!

The concept of PICWIC and the resulting policies and procedures that it enables sound very promising, but how do we actually implement PICWIC in the real world? The key to providing the necessary context lies in metadata: to collect and analyze required metadata non-intrusively, to automate workflows and auto-generate reports, and have a reliable operational plan to follow. The Varonis® Metadata Framework™ was purpose-built for metadata collection and analysis.

Companies deeply rely on shared folders and SharePoint sites to store critical data assets, but don't have a grasp on what it takes to manage these containers with identity context in mind. One of the PICWIC best practices that Forrester recommends is to "Bidirectionally map shared folders and AD and LDAP groups to eliminate chaos." Forrester says, "Successful companies report that they have cleaned up and standardized naming conventions and mapping rules between shared folders and AD groups. This way it's clear which AD and LDAP groups drive what level of access to a shared folder."[6] Access activity is one metadata stream that Varonis® uses to facilitate PICWIC by showing data owners who is accessing data. Varonis® also aggregates metadata required to attain a bidirectional mapping of your shared folders and AD and LDAP groups, so you have a crystal clear view into who can access data.

Varonis® identifies those containers (e.g. folders/directories, SharePoint sites) that contain large amounts of sensitive data, are exposed to many people and are heavily utilized, and prioritizes them in order of risk. Then, Varonis® identifies data owners and involves them in managing and protecting their data at the appropriate container level, where most access control decisions are made. Managing containers instead of individual files drastically reduces the number of individual decisions that need to made (often by a factor of 10 or more[7]). Once owners are identified, they can then limit access to only those who require access. Additionally, by tracking and analyzing access activity, Varonis® is able to identify when access is being abused, and identify access infringements before data leaks occur.

While Varonis® is not a DLP product, Varonis' IDU Data Classification Framework®(DCF) provides the ability to include classification results from other DLP products, and/or scan the files itself. Because DCF is a part of the Metadata Framework™, its metadata is fully integrated with its audit trail of access activity to provide true incremental scanning–only scanning new and modified content.

DLP solutions alone do not provide enough context to systematically and sustainably address fundamental problems in data management and protection: individuals in organizations have access to data that they do not need and should not have, and their use of data is not monitored. Enterprise context awareness is a problem in the domain of Metadata Framework™ technology—not data loss prevention. When access controls are optimized, use of data is monitored, and abuse is flagged, the possibility of data loss decreases greatly. In order to maximize security, corporations will have to apply complementary technologies, not to eliminate, but to accelerate their existing DLP solutions. The most secure banks have tellers that give out the right money and diligent guards at the door.

[1]*Your Data Protection Strategy Will Fail Without Strong Identity Context, Forrester Research, Inc., July 29, 2011 (Forrsights Security Survey, Q3 2010)*

[2]*Your Data Protection Strategy Will Fail Without Strong Identity Context, Forrester Research,Inc., July 29, 2011 (Poneman Institute, 2010 Annual Study: U.S. Cost of a Data Breach)*

[3]*Your Data Protection Strategy Will Fail Without Strong Identity Context, Forrester Research,Inc., July 29, 2011 (Forrsights Security Survey, Q3 2010)*

[4]*Your Data Protection Strategy Will Fail Without Strong Identity Context, Forrester Research, Inc., July 29, 2011*

[5]*Your Data Protection Strategy Will Fail Without Strong Identity Context, Forrester Research, Inc., July 29, 2011*

[6]*Your Data Protection Strategy Will Fail Without Strong Identity Context, Forrester Research, Inc., July 29, 2011*

[7]*If there is an average of 1 million files in a terabyte of data and .5% are sensitive, that amounts to 5,000 decisions. In contrast, there are typically 2,500 folders in a terabyte that have unique permissions and usually only 5-10% of them need to be managed.*

ABOUT VARONIS

Varonis is the leading provider of software solutions for unstructured, human-generated enterprise data. Varonis provides an innovative software platform that allows enterprises to map, analyze, manage and migrate their unstructured data. Varonis specializes in human-generated data, a type of unstructured data that includes an enterprise's spreadsheets, word processing documents, presentations, audio files, video files, emails, text messages and any other data created by employees. This data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property and numerous other forms of vital information. IT and business personnel deploy Varonis software for a variety of use cases, including data governance, data security, archiving, file synchronization, enhanced mobile data accessibility and information collaboration.

Free 30-day assessment:

WITHIN HOURS OF INSTALLATION

You can instantly conduct a permissions audit: File and folder access permissions and how those map to specific users and groups. You can even generate reports.

WITHIN A DAY OF INSTALLATION

Varonis DatAdvantage will begin to show you which users are accessing the data, and how.

WITHIN 3 WEEKS OF INSTALLATION

Varonis DatAdvantage will actually make highly reliable recommendations about how to limit access to files and folders to just those users who need it for their jobs.

WORLDWIDE HEADQUARTERS

1250 Broadway, 31st Floor, New York, NY 10001 **T** 877 292 8767 **E** sales@varonis.com **W** www.varonis.com

UNITED KINGDOM AND IRELAND

Varonis UK Ltd., Warnford Court, 29 Throgmorton Street, London, UK EC2N 2AT **T** +44 0207 947 4160 **E** sales-uk@varonis.com **W** www.varonis.com

WESTERN EUROPE

Varonis France SAS 4, rue Villaret de Joyeuse, 75017 Paris, France **T** +33 184 88 56 00 **E** sales-france@varonis.com **W** sites.varonis.com/fr

GERMANY, AUSTRIA AND SWITZERLAND

Varonis Deutschland GmbH, Welserstrasse 88, 90489 Nürnberg **T** +49 (0) 911 8937 1111 **E** sales-germany@varonis.com **W** sites.varonis.com/de