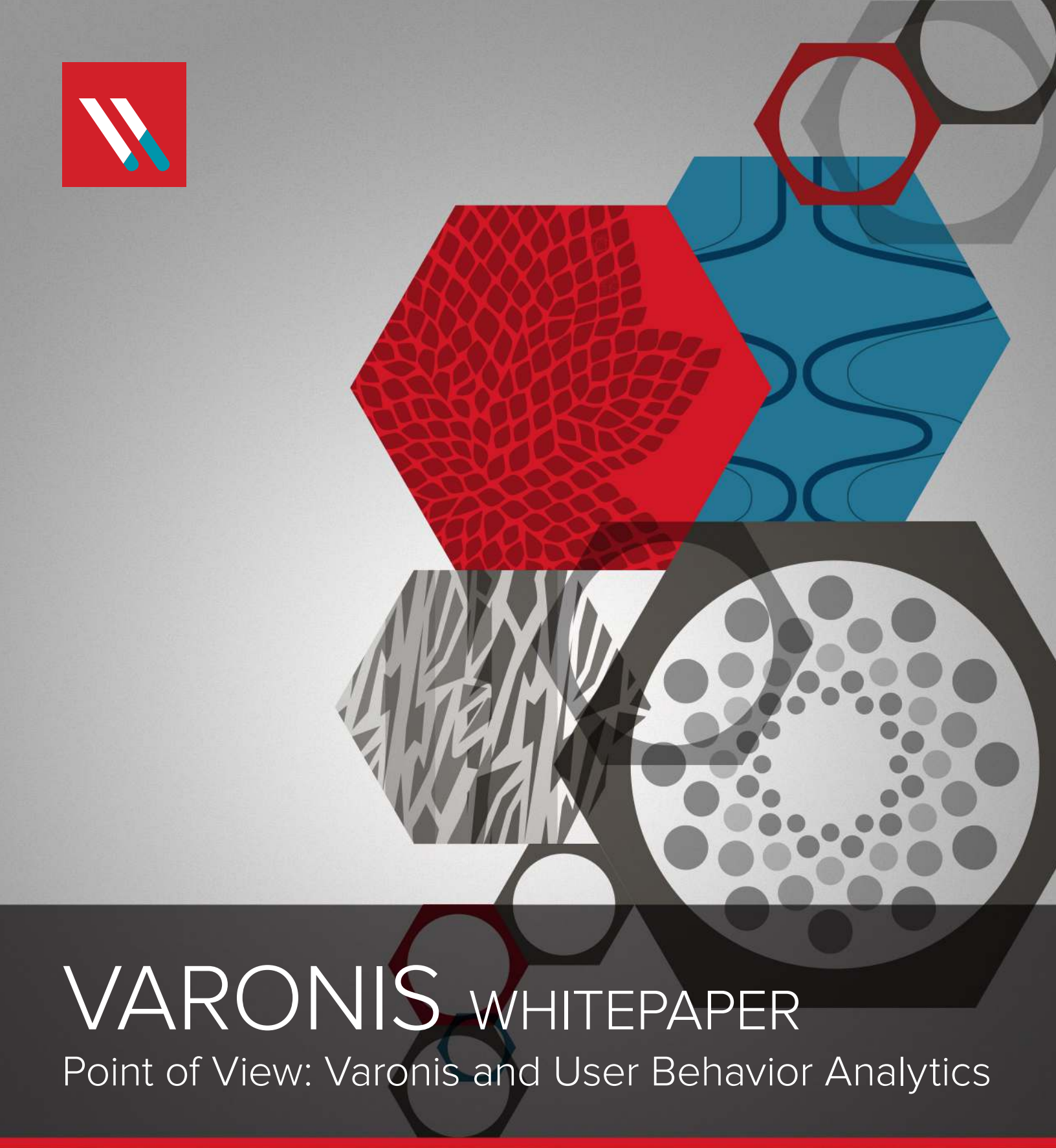

VARONIS WHITEPAPER

Point of View: Varonis and User Behavior Analytics

CONTENTS

POINT OF VIEW: VARONIS AND USER BEHAVIOR ANALYTICS

OVERVIEW

Security has become a business problem. Though organizations have invested in security, they know they're not really protected. The recent string of headline-making breaches has not been lost on the C-level suite. Security personnel, for the most part, know their biggest areas of risk, know they have a short window to get something done and know they have a limited budget.

So what to do? The answer is surprisingly simple: protect unstructured data!

UNSTRUCTURED, ACCESSIBLE, AND OUT OF CONTROL

Many breaches (if not most) involve the theft of unstructured data. Most CISOs know this is their biggest vulnerability. On the federal side, consider Snowden and Manning in the US, Israel's Anat Kamm, and the hackers behind the Office of Personnel Management. In all these cases, what was taken? Files. Emails. Unstructured data. The attackers had too much access to sensitive data, nobody was watching them, and, even worse, no one even noticed the data had been copied and exfiltrated.

The damage is still being felt, and the ultimate cost remains unknown.

On the commercial side, unstructured data is just as valuable and vulnerable. In the Sony incident, exposed internal emails and files led to one of the most sensational breaches in recent history. And in February of 2014, Indiana University announced that 146,000 students' and recent graduates' data, including social security numbers, had been exposed, not because of hackers but because someone accidentally saved a file in the wrong public folder. The list of breaches where unstructured data is carelessly handled goes on.

Bottom line: If an organization has unstructured data and they don't have a Varonis solution, then they're almost certainly a breach waiting to happen. Breaches, by the way, are very expensive. A Ponemon Institute study tell us that in 2015 the average cost of a breach runs around $3.7 million.

At Varonis, we have a great first step. Our Express Risk Assessment can you tell whether your unstructured file data has any security holes.

THE PERIMETER IS IRRELEVANT

It's too easy for an attacker to get "inside" the network. They walk in as contractors, they steal credentials, or they compromise an insider's account or system through a phishing attack, as was the case with the Anthem.

Phishing works: The 2015 Verizon DBIR claims that a phishing campaign of just 10 emails has a better than 90% chance of getting a click.

For most organizations, once an attacker is inside, it's game over.

According to a Varonis-sponsored Ponemon study, 71% of employees have access to more data than they need (much of which turns out to be sensitive), and only 21% of organizations seem to be watching what employees are doing with data. Files and emails are over-exposed gold mines that aren't being watched.

It's not surprising then that organizations discover breaches long after they happen (if ever) and don't know the extent of them. The Verizon DBIR researchers have also been tracking the time it takes for companies to discover a breach: their unit of measurement is in *months*, not weeks or days.

We know the hackers are going around perimeter defenses and then going after unstructured data. So instead of fighting the last war with more firewalls and anti-virus software, organizations need to modernize their defenses by directly fortifying the controls around assets they need to protect.

That's where Varonis comes in.

DETECTING BREACHES IN TWO HOURS.

There's a new category of security software out there that's getting a lot of attention: User Behavior Analytics, or UBA. Security folks are talking about it. Analysts are talking about it. It's in the news. The idea is that UBA software watches and baselines what users are doing to detect things that don't look normal. Sound familiar?

Varonis has been doing User Behavior Analytics for years, and we track behavior that no one else sees: user access to unstructured file data.

Varonis' comprehensive audit record of all access to unstructured data across multiple platforms is difficult to capture and harder to store and analyze. DatAdvantage recommendations and alerts are two examples of User Behavior Analytics that have been proving themselves for ten years.

With DatAlert, IT security teams can immediately begin to detect the things they're most worried about, like:

- Mass deletions and modifications
- Malware and Ransomware that affects files or emails (e.g., CryptoLocker)
- Administrative group changes (privilege escalations)
- Administrative access to user data
- Mass failed login attempts
- Monitoring email attachments sent to personal accounts (gmail, yahoo, etc.)
- Mailbox activity by accounts other than those of the mailbox owner
- Activity on sensitive data
- Changes made outside of change control windows

Whether an IT group integrates DatAdvantage/DatAlert with a SIEM, another UBA system, or receives alerts directly from Varonis, they immediately make progress in solving their business problem: securing unstructured data from attackers.

VARONIS DOES FAR MORE THAN DETECTION: IT'S AN INVESTMENT IN PREVENTION AND FAST RECOVERY.

For years we've been helping organizations classify and archive data, optimize their permissions, and sustain a least privilege model. It's really an application of Privacy by Design (PbD) principles, which researchers, government regulators, and security personnel agree is a more practical and realizable way to achieve data security.

They also know that security improvements based on PbD will take time, even with Varonis (though Varonis accelerates these improvements). In the meantime, by focusing on UBA, not only do security teams get a quick win but they're setting their organizations up for strategic improvement going forward.

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.

START YOUR FREE TRIAL