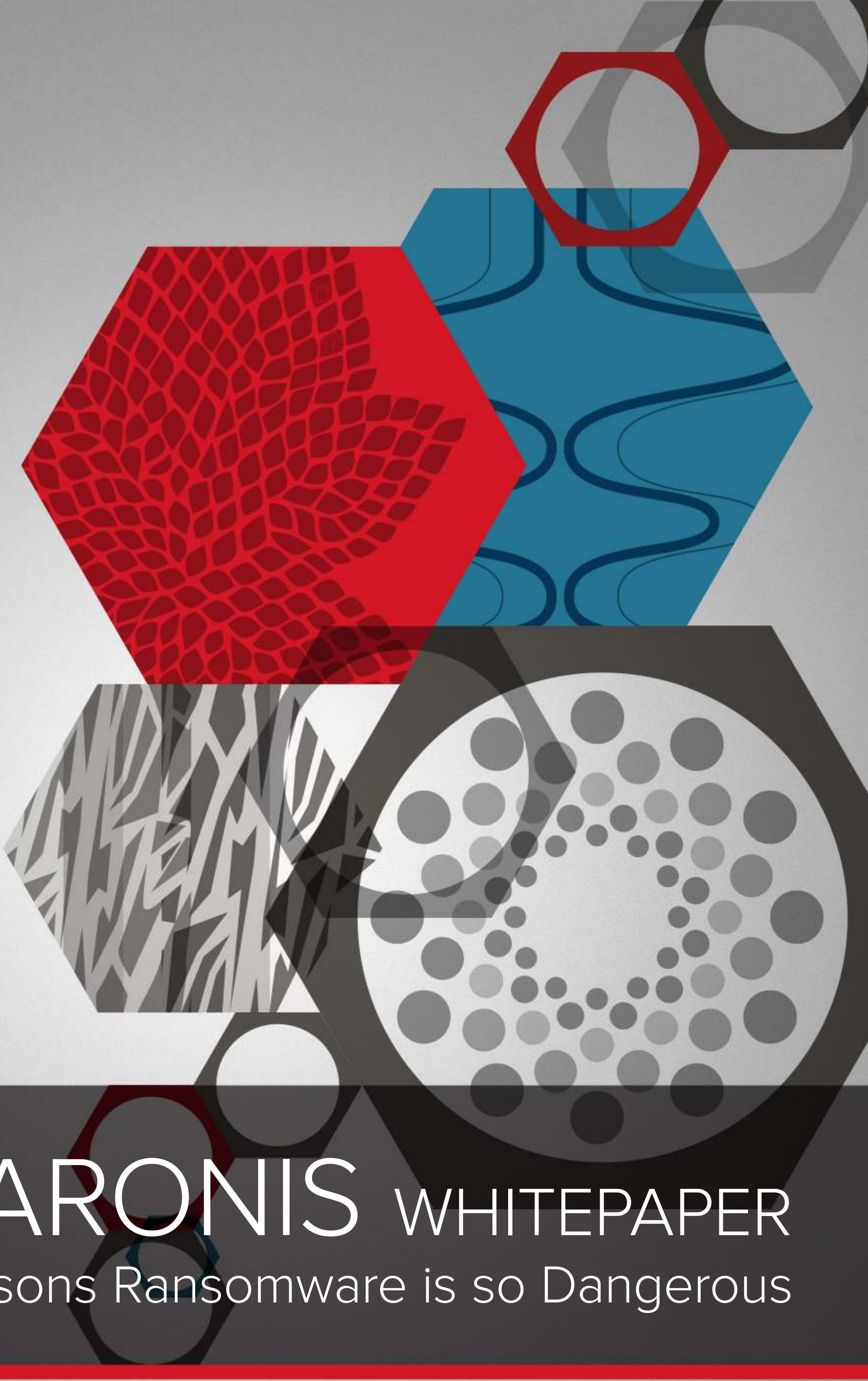

VARONIS WHITEPAPER

3 Reasons Ransomware is so Dangerous

3 REASONS RANSOMWARE IS SO DANGEROUS

STORIES FROM THE FIELD

“WE JUST WALKED DOWN THE HALL AND UNPLUGGED THE MACHINE,”

Said the Director of Information Security for a Timber Production company in the Pacific Northwest. It wasn’t the most technically sophisticated way to stop the in-progress ransomware infestation, but it stopped the threat in its tracks.

> *“It got through our [new, next-generation] firewall, IDS, and alerts on our SIEM. We also had two separate [malware detection] agents running on the workstation.”*

The signatures for this particular variant weren’t yet known, so the code passed through the perimeter of the network, slipped right by their endpoint security and began encrypting files on their network shares.

> *“A Varonis alert triggered within three minutes of the outbreak. We had enabled alerting but had yet to configure any kind of automatic response,” he continued, “so we just walked down the hall and unplugged the machine.”*

In this case, the user was the head of the legal department, who had access to huge amounts of extremely sensitive information. Luckily, the attack was stopped before the malware could contact the command and control (C&C) server and confirm that an infestation had taken place. They were also able to use the DatAdvantage access log to list the files that needed to be restored.

This is just one example of the many ransomware success stories Varonis is hearing from customers and prospects all over the world. Organizations in all verticals, from healthcare to government to financial services and manufacturing are getting attacked daily by new and more insidious flavors of ransomware like CryptoLocker. Varonis performs hundreds of evaluations per month and is installed in thousands of enterprise environments. For many of these customers, Varonis is now critical in the prevention, detection, mitigation and recovery from these kinds of attacks.

What makes ransomware so insidious is that it so easily exploits vulnerabilities on the inside of the security perimeter, a weak spot for so many organizations.

Here are 3 reasons ransomware is so dangerous:

1. Many organizations aren't monitoring how employees use file shares at all —the huge repository of files that newer ransomware strains target. You can't catch what you can't see, so it's extremely difficult to catch ransomware without monitoring file share use.

2. What's worse is that users typically have access to far more files than they need, and a lot of files are accessible to any employee. This means that once ransomware gets in it can wreak all kinds of havoc. Even a single compromised user can lock up huge amounts of data.

3. Finally, since most have no record of who modified (or encrypted) which files when, huge recovery exercises are needed to make sure that nothing was missed. Recovery from these attacks can often mean bringing entire file shares down while backups are restored.

In January, 2016, the County Council in Lincolnshire in the U.K. was hit by a strain of ransomware that forced it to bring down the entire network for more than 24 hours, making news all over the country. A nearby town was put immediately on alert and took a close look at its own systems to see if they were as vulnerable.

> *"Following what happened in Lincolnshire, we are now ever more vigilant."*

This town installed Varonis and was able to alert and lock down a recent infection immediately, without causing widespread damage and keeping them out of the news.

The best way to combat ransomware is to make sure that users only have access to what they need and that all access is monitored and analyzed. What's driving so many Varonis installations in response to ransomware is that Varonis software does both: Varonis monitors and analyzes all activity so you can detect ransomware and other insider threats, and it lets you lock down access by eliminating global access and intelligently reducing excessive individual permissions.

Customers have been surprised at just how effective Varonis has been, especially compared with the other solutions they've invested in. A major Western Canadian Bank got an object lesson in this over the last six months when they realized that after spending more than $500,000 on new security tools from different vendors, they weren't any closer to detecting or preventing these kinds of attacks.

> *"Of all the expensive security products we've purchased," they told us, "DatAlert is the solution that has done, and is doing, all of the alerting and notification of anomalous behavior, especially ransomware."*

ABOUT VARONIS

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Varonis empowers enterprises to stop ransomware in its tracks, discover where sensitive data is overexposed, prioritize vulnerable and stale data, and lock it down without interrupting business. Varonis builds context around the content of data and activity; automates threat detection with predictive threat models built on advanced analytics, user behavior, and machine learning; and monitors critical assets for suspicious activity, including unusual access to sensitive data, abnormal user behavior and file activity to protect against potential exploitation.

All Varonis products are free to try for 30 days. Our systems engineering team will get you up and running in no time.

FAST AND HASSLE FREE

Our dedicated engineer will do all the heavy-lifting for you: setup, configuration, and analysis - with concrete steps to improve your data security.

FIX REAL SECURITY ISSUES

We'll help you fix real production security issues and build a risk report based on your data.

NON-INTRUSIVE

We won't slow you or your system down. We can monitor millions of events per day without impacting performance.

START YOUR FREE TRIAL