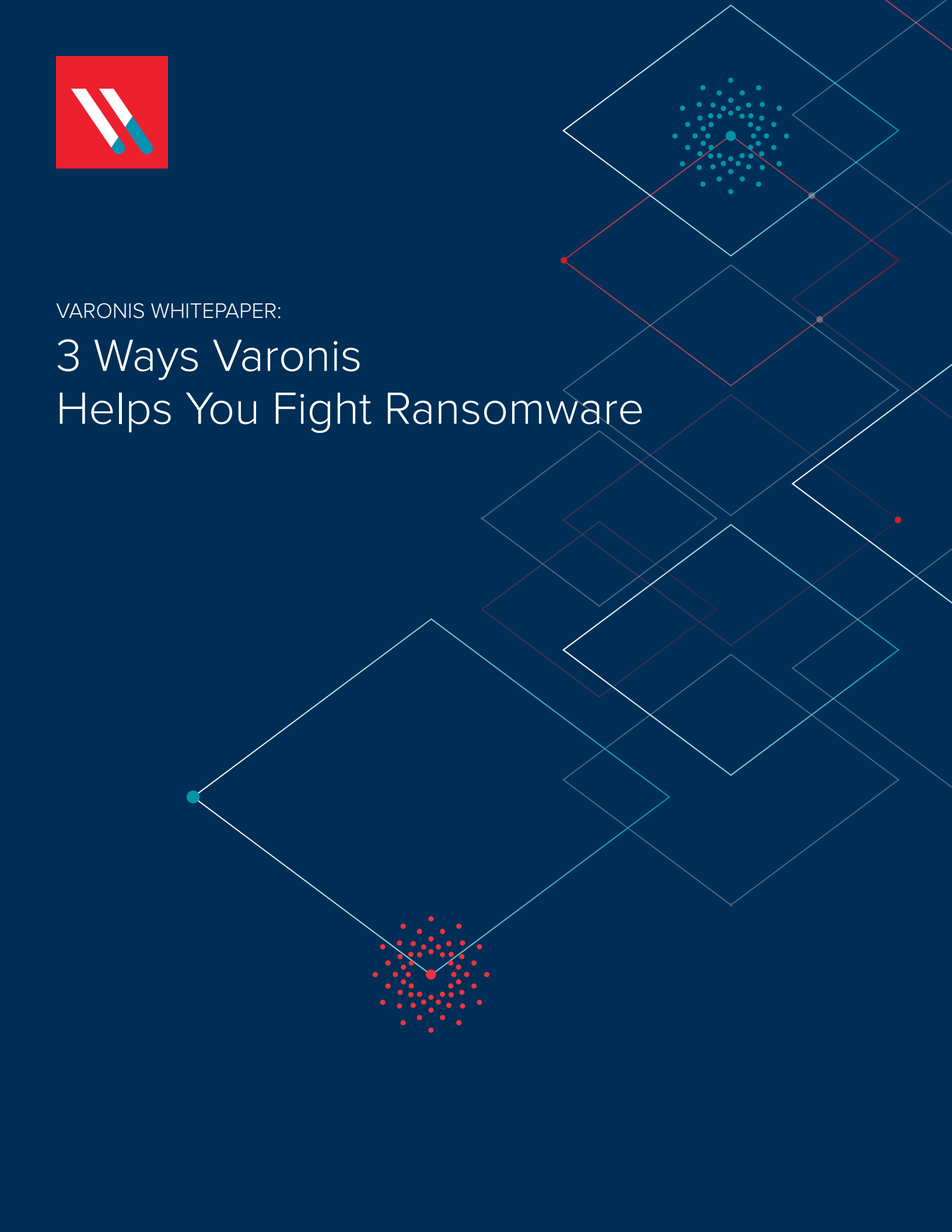


VARONIS WHITEPAPER:

3 Ways Varonis Helps You Fight Ransomware

The Canary in the Coal Mine

Ransomware can be devastating, but it doesn't have to be.

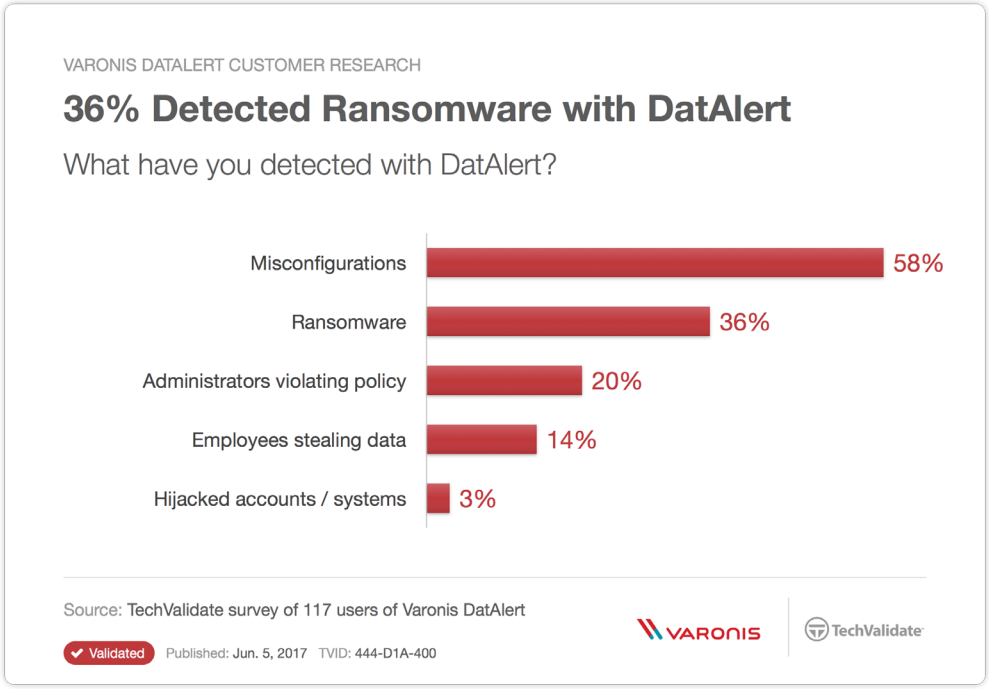
- It's one of the easiest insider threats to catch and stop if you're looking at the right things, as it's a very noisy intruder, especially when compared with other threats.
- It's possible to limit the damage a ransomware infection can do by reducing the attack footprint for compromised users.
- Recovery can be much easier if you know which users have been compromised and which files have been encrypted.

Here's how Varonis helps with all three areas:

Rapid Detection and Response

Varonis DatAdvantage captures more information about how users interact with data than any other technology – it analyzes file system activity on platforms that provide adequate auditing through their APIs, like those from NetApp and EMC, and uses file system filters to capture metadata for platforms where native auditing is lacking, like Windows, Unix, Exchange, and SharePoint.

Varonis DatAlert analyzes the file system activity collected by DatAdvantage to detect when an attack is underway – looking for both known variants, as well as 0-day attacks with sophisticated user behavior analytics. Once ransomware moves past an endpoint and starts encrypting files on core IT systems, DatAlert triggers an alert and can shut down compromised accounts automatically – before they do serious damage.



▲ *In a recent survey, 36% of Varonis DatAlert customers have detected ransomware.*

Prevention

The highest concentration of data targeted in ransomware attacks is usually on the shared folders, with 10 to 1,000 times more data than on a laptop or a workstation. In the 2017 Varonis Data Risk Report, we found that 20% of all shared folders were open to every employee. It only takes one infected user, then, to spread ransomware to 20% of your data – most ransomware attacks run using the credentials of the compromised user.

Varonis DatAdvantage analyzes file system permissions, user and group relationships, and activity to find overly broad access granted through global groups (like Everyone, Authenticated Users, and Domain Users), permissions malfunctions, and excessive group relationships. DatAdvantage also provides the ability to model or sandbox changes to reduce access, and then execute them, safely.

The Varonis Data Classification Framework can help you prioritize remediation efforts by identifying sensitive and regulated content, and the Varonis Automation Engine can safely remove global access groups over entire shares or servers – automatically. By reducing broad access, a ransomware attack can do far less damage.

Recovery

With the detailed audit log captured by DatAdvantage, it's possible to recover from an attack very quickly. Instead of searching through directories for ransom notes, you can run a query for all the modifications made by any user over any time period to pinpoint the affected files, and then restore the correct version of the file.

Summary

By combining sophisticated analytics with permissions management, Varonis protects you from ransomware with rapid detection, optimized access controls, and data-driven recovery. In addition to ransomware, Varonis also protects organizations from insider threats that are much harder to spot and even harder to recover from, like disgruntled employees stealing data, rogue admins reading executive emails, or compromised accounts escalating privileges.

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.

Live Demo

Set up Varonis in your own environment and see how to stop ransomware and protect your data.

info.varonis.com/demo

Data Risk Assessment

Get your risk profile, discover where you're vulnerable, and fix real security issues.

info.varonis.com/rra