VARONIS WHITEPAPER:

Defeat Ransomware with Varonis and NetApp

The Canary in the Coal Mine

Ransomware attacks have become a major security threat. It feels like each week a new variant is announced, and with the global impact made by WannaCry ransomware is now on everyone's radar as it has indeed become a universal problem.

However, there's no need to panic. We offer the following security advice:

- It's possible to limit the damage a ransomware infection can do by reducing the attack footprint for compromised users.
- Ransomware that encrypts files with known extensions can be blocked.
- 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.
- Recovery from current backups can be much easier if you know which users have been compromised and which files have been encrypted.

Here’s how Varonis and NetApp help:

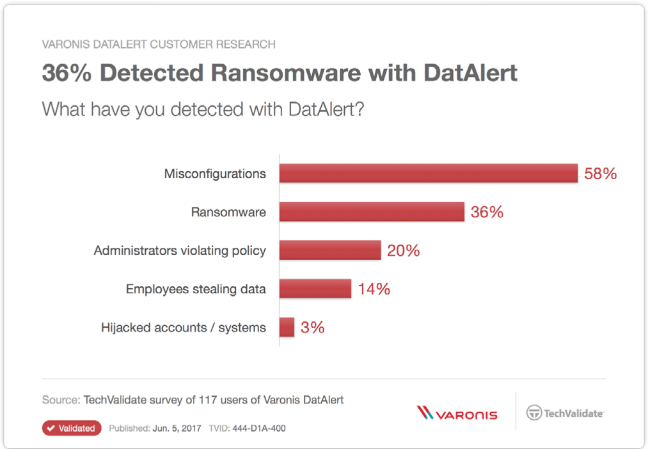
Prevention

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. This is also why we constantly tout the value of access control, a key value that the DatAdvantage solution provides.

The more folders that are available to an average user, the greater the overall damage of a ransomware attack!

To help you find and limit excessive access rights, Varonis DatAdvantage analyzes the file system permissions, user and group relationships, and activity. It can then find overly broad or general 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, while the Varonis Automation Engine can safely remove global access groups over entire shares or servers – automatically. By reducing broad access, the scope of a ransomware attack can be severely limited.


VARONIS DATALERT CUSTOMER RESEARCH

36% Detected Ransomware with DatAlert

What have you detected with DatAlert?

Source: TechValidate survey of 117 users of Varonis DatAlert

✓ Validated Published: Jun. 5, 2017 TVID: 444-D1A-400

▲ *Figure 1 In a recent survey, 39% of Varonis DatAlert customers have detected ransomware.*

Blocking

Is it possible to simply stop ransomware from doing its work in the first place? The NetApp ONTAP FPolicy solution provides a file-blocking methodology that allows organizations to filter or block traffic based on file extensions and file metadata. Common ransomware includes, but is not limited to, the following file types:

- .micro
- .encrypted
- .locked
- .crypto
- .crypt
- .crinf
- .r5a
- .XRNT
- .XTBL
- .crypt
- .R16M01D05
- .pzdc

Rapid Detection and Response

Varonis DatAdvantage and DatAlert can form the basis of your next layer of defense. DatAdvantage captures more information about how users interact with data than any other technology. It analyzes file system activity on platforms that can provide adequate auditing through their APIs, such as those from NetApp ONTAP and uses file system filters to capture metadata for those platforms where native auditing is lacking, including Windows, Unix, Exchange, and SharePoint.

Varonis DatAlert then analyzes the file system activity collected by DatAdvantage to detect when an attack is underway – looking for both known variants, as well as zero-day attacks with sophisticated User Behavior Analytics (UBA). 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.

Recovery and Remediation

Let’s say the ransomware has not been caught in time—your files are encrypted. There’s a still a way out. Varonis and NetApp solutions provide a speedy route to recovery.

With the contextual information provided from NetApp ONTAP FPolicy and the detailed audit log captured by DatAdvantage, 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.

What about restoring from the most recent back-up?

That’s where NetApp Snapshot technology comes into play. Snapshot produces point-in-time copies that protect data with no performance effect and minimal storage space consumption. Snapshot technology provides the granularity to create images of a single file copy or a complete disaster recovery solution.

Summary

By combining sophisticated analytics with permissions management and contextual information, Varonis and NetApp protect you from ransomware with rapid detection, and optimized access controls. Combining Varonis and NetApp, you can achieve fast data-driven recovery.

About NetApp

NetApp is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation and optimize their operations. For more information, visit www.netapp.com. #DataDriven

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.

Additional Resources/Information

In addition to ransomware, Varonis also protects organizations from insider threats that are much harder to spot and even harder to recover from, such as disgruntled employees stealing or deleting data, rogue admins reading executive emails, or compromised accounts escalating privileges.

See our Case Studies to see how we continue to help customers manage and protect their data!

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