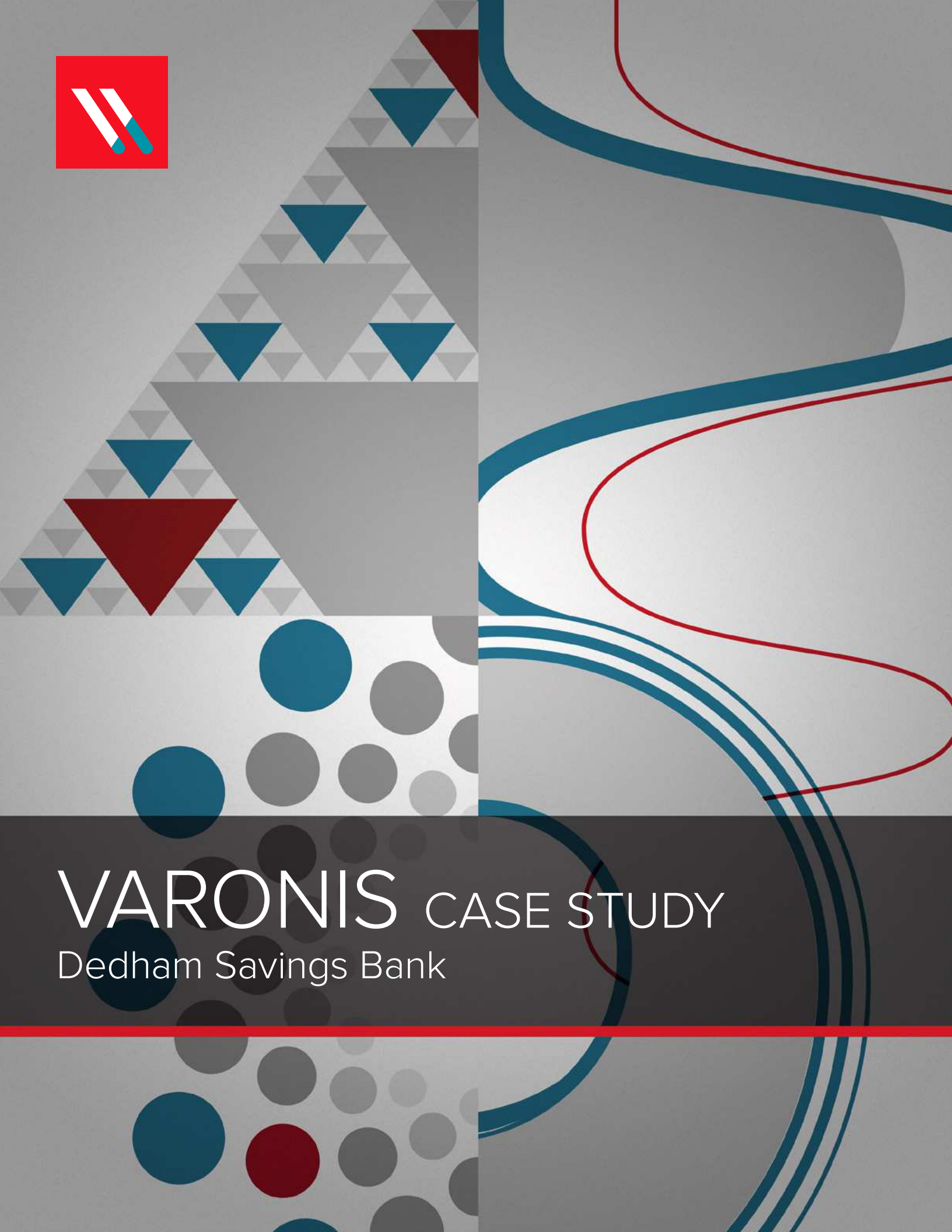

VARONIS CASE STUDY

Dedham Savings Bank

Dedham Savings

"Cryptolocker is a huge security threat, so having Varonis DatAlert in place to help prevent attacks is a no brainer for us. When anyone from the outside tries to encrypt a file on the network or use a compression tool like WinZip, DatAlert will let us know in real time. Also, we can receive alerts about suspicious internal activity. It's nice to know Varonis is looking out for us and will be able to catch things and help us proactively prevent internal and external data breaches."

—Jim Hanlon – SVP & CTO, Dedham Savings Bank

THE CUSTOMER

Dedham Savings Bank

LOCATION

Massachusetts, USA

INDUSTRY

Financial Services

PRODUCTS

DatAdvantage for Windows, DatAdvantage for Directory Services, DatAdvantage for SharePoint, DatAlert, Data Classification Framework, Data Transport Engine, Varonis Professional Services

Founded in 1831, Massachusetts-based Dedham Savings Bank has 14 locations in the Boston area.

BUSINESS REQUIREMENTS

PEACE OF MIND KNOWING DOCUMENTS ARE SAFE FROM INSIDER THREATS

Dedham Savings Bank wanted a solution that could monitor insider behavior to detect suspicious activity such as mass deletions and employees accessing data they shouldn't.

GET AHEAD OF POTENTIAL DATA BREACHES

Malware and ransomware are on the rise, so the bank required a solution that could quickly alert the IT staff to unusual file access behavior, like rapid encryption of files stored on its servers.

REDUCE RISK

The bank needed a solution in place that could protect its growing set of unstructured corporate and customer data.

ENSURE COMPLIANCE

The bank is regulated and must follow certain policies and federal guidelines for data retention.

DATA CLASSIFICATION

The bank needed a solution that could help it classify its terabytes of unstructured data across its network.

THE VARONIS SOLUTIONS / RESULTS

Implementation Process

The actual implementation took half a day.

According to Jim Hanlon, SVP & CTO, Dedham Savings Bank, *"The implementation process went terrifically. Varonis' support folks were really responsive. They worked with us on the phone, reported in, did the training sessions, demonstrated the tools, and got us up and running in no time."*

VARONIS DATADVANTAGE

Bank Data is Now Safe and Sound

Varonis DatAdvantage for Windows, SharePoint, and Directory Services ensures that only the right people at Dedham Savings Bank have access to the right data at all times, all access is monitored, and any abuse is flagged. DatAdvantage also helps keep track of which files employees view, move and copy.

These capabilities also help ensure the bank meets compliance requirements regarding data loss prevention and having the ability to identify all data owners.

According to Jim, *"One of the biggest regulatory requirements right now is to be totally confident about where customer information resides on your network. When you know where it is, then there are no surprises."*

VARONIS DATALERT

Varonis DatAlert detects and alerts on potential security breaches by analyzing file activity, Active Directory changes, permissions changes, and other events. Alert criteria and output are easily configurable so that the right people and systems can be notified about the right things, at the right times, and in the right ways.

Jim also reported, “Cryptolocker is a huge security threat, so having DatAlert in place to help prevent attacks is a no brainer for us. When anyone from the outside tries to encrypt a file on the network or use a compression tool like WinZip for example, DatAlert will let us know in real time. Also, we can receive alerts about suspicious internal activity. It’s nice to know Varonis is looking out for us and will be able to catch things and help us proactively prevent internal and external data breaches.”

VARONIS DATA TRANSPORT ENGINE

Easy and Secure Data Migration

The bank added Data Transport Engine to help it migrate data from its file service to SharePoint without the hassle and downtime, permissions, translation issues or cross-platform challenges.

VARONIS DATA CLASSIFICATION FRAMEWORK

Understand and Find Sensitive Content

An organization like Dedham Savings Bank has terabytes of data, much of which is comprised of files that are considered sensitive. Finding them is a challenge, and so is figuring out who has access to them. With Varonis Data Classification Framework, the bank now understands how sensitive data is being used, including who has access, who's using it, and to whom it belongs.

"Varonis Data Classification Framework has helped us solve a major ongoing business challenge, which is identifying and classifying the unstructured data on our file systems. It's not a flip-the-switch project from the perspective of folks within IT, because you have to work with so many different business units and departments throughout the organization to identify the data and justify multiple instances of the data, how old it is, and whether it's necessary to keep it live or archive it. Thanks to Data Classification Framework, we were able to determine that about three-quarters of our data was stale and needed to be archived."

Jim continued, *"Identifying customer data on the network is critical, and so is the sensitive internal data on the network that we may have never thought of before that may have been left behind by former employees. Take Target and Sony Pictures, for example, where the hackers found administrative credentials on their networks. You won't have any insight to that unless you have a solution like Varonis to help you out."*

VARONIS RISK ASSESSMENTS QUICKLY SHOW YOU WHERE YOUR MOST VULNERABLE DATA IS STORED, WHO IS ACCESSING IT, AND WHAT NEEDS TO BE DONE TO SECURE IT. FIND OUT MORE HERE.

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