



Varonis Data Security Platform — Cyber Catalyst 2020 Designation

The Varonis Data Security Platform helps organizations:

- Detect insider threats and cyberattacks by analyzing data, account activity, and user behavior;
- Prevent and limit disaster by locking down sensitive and stale data; and
- Efficiently sustain a secure state with automation.

Data today is largely overexposed and under protected, which can open companies up to a number of risks: increased attack surfaces, loss of IP, privacy violations, and more damaging cyberattacks.

Varonis helps organizations manage the difficult and ever-growing challenge of securing vast enterprise data stores both on premises and in the cloud that hold their most valuable assets. With Varonis, customers can confidently detect security incidents and cyberattacks, and reduce their risk and exposure.

The Varonis Data Security Platform helps companies to:

- **Know where sensitive data is and where exposures are.** Varonis enables organizations to say “show me every sensitive folder open to too many people, in order of risk” and get an instant answer, with highly accurate data classification and deep visibility into data access and activity.
- **Put data protection on autopilot:** Varonis uses behavior-based automation to intelligently remediate risk on a massive scale without disrupting business.

- **Keep risk low while automating thousands of manual tasks:** Varonis makes it possible to enforce retention policies consistently across the organization’s environment, simplify entitlement reviews and save hours of back/forth, and streamline access governance.
- **Detect and respond to threats:** Varonis uses sophisticated behavioral analytics to catch potential threats like malware, ransomware or malicious insiders. The platform combines and enriches logs to produce a handful of high-fidelity, context-rich alerts that are meaningful and actionable. Built-in automated responses can stop cyber threats, and a free Incident Response team can help investigate any incident.

The Varonis Data Security Platform serves more than 7,000 customers worldwide across a range of industries, including financial services, public, healthcare, industrial, insurance, energy and utilities, consumer and retail, technology, media and entertainment, and education.

**Product information provided by Varonis*

For more information about Varonis Data Security Platform, visit www.varonis.com.

Why Varonis Data Security Platform is a 2020 Cyber Catalyst Designated Solution

ADDRESSES A TOP 5 CYBER RISK:

The 2020 program encouraged the submission of solutions that targeted the top five cyber risks identified by participating insurers: ransomware, supply chain/vendor management, cloud migration/management, social engineering, and privacy regulation/data management.

Varonis Data Security Platform specifically targets ransomware, but also has wider utility and applicability in addressing other types of cyber risk.

INSURER RATINGS AND COMMENTARY:

Cyber Catalyst participating insurers rated Varonis Data Security Platform highest on the criteria of cyber risk reduction, efficiency, and differentiation.

In their evaluation, the insurers commented:

- “A fantastic piece of software that definitely fulfills a broad use case for auditing data availability and protective provisions. Arguably best-in-class when monitoring for PII data within an organization.”
- “Intuitive dashboard and covers the majority if not all current data stores used by organizations. This will help administrators get out in front of the issue.”
- “A good product that would work well as companies, including small and medium enterprises, move increasingly to the cloud.”

Insurance Policies and Implementation Principle

Organizations that adopt Cyber Catalyst designated solutions may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers.

Those insurers, when considering potential policy enhancements, will expect organizations to deploy Cyber Catalyst designated products and services in accordance with certain “implementation principles” that have been developed by the insurers and product vendors.

The implementation principle for Varonis Data Security Platform is:

- A designated individual works with Varonis to install the software and perform a Data Risk Assessment; the software will begin to immediately identify unusual activity that could signal a potential ransomware attack in the environment and in approximately 30 days the platform builds profiles for users and devices and alerts individual(s) on potential threats when activity deviates from normal.

Evaluation Process

Applications for evaluation of cybersecurity products and services were accepted from March 10 to May 15, 2020. More than 90 offerings, spanning a broad range of categories, were submitted.

The insurers evaluated eligible solutions along six criteria:

1. Reduction of cyber risk.
2. Key performance metrics.
3. Viability.
4. Efficiency.
5. Flexibility.
6. Differentiation.

Cyber Catalyst designation was awarded to 15 solutions receiving positive votes from at least six of the eight insurers, which voted independently. Marsh did not participate in the Cyber Catalyst designation decisions.

More Information on Cyber Catalyst

The next Cyber Catalyst program will occur in 2021.

For more information on the 2020 Cyber Catalyst designated solutions, or the 2019 class of Cyber Catalyst solutions, visit the Cyber Catalyst pages on the Marsh website: www.marsh.com/cybercatalyst.

For more information about Marsh’s cyber risk management solutions, email cyber.risk@marsh.com, visit www.marsh.com, or contact your Marsh representative.

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the “Marsh Analysis”) are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.