



# EMAIL RISK ASSESSMENT

The most accurate email risk assessment in the industry. For free.

## CHALLENGE

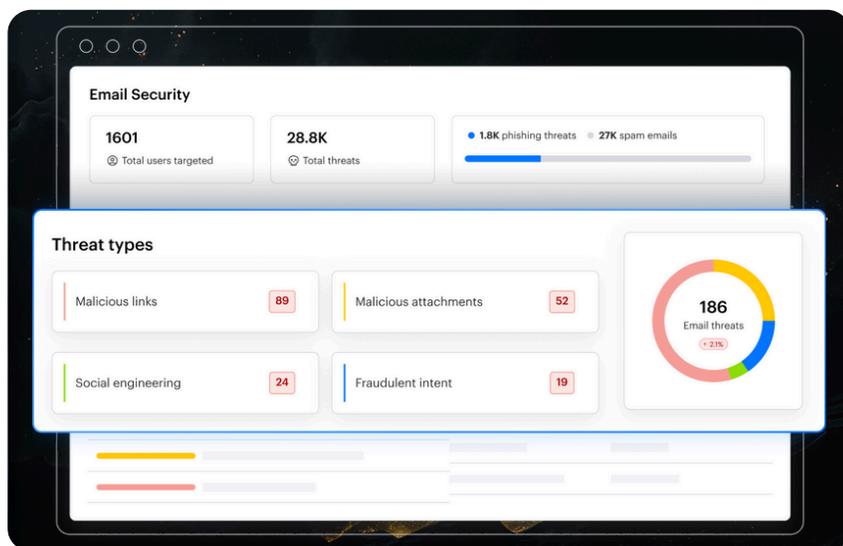
Bad actors are no longer hacking computers. They're hacking trust. AI has enabled a new breed of email threats that are more deceptive than ever, making malicious messages difficult for both humans and legacy security tools to detect.

These threats also blend text, images, links, and behavioral cues in ways that require more sophisticated, layered defenses.

## SOLUTION

Varonis Interceptor replaces ineffective API-based solutions and augments legacy SEGs with a true multimodal AI strategy. It combines numerous sources of AI-powered analysis to achieve a higher rate of detection and deliver superior protection. See for yourself.

Start a free email risk assessment and see firsthand what is being missed. It takes 5 minutes to set up, and our team of analysts will show you what threats are getting through and how. Gain a full 90-day look back and a real-time view of present threats.



## KEY BENEFITS

**90**

Day look-back of missed threats

**5**

Minute install for speedy deployment

**1,000's**

Of threats in your inboxes distilled into a single, easy-to-consume report

## THREATS COVERED

- Phishing Link and QR-Code Attacks
- Targeted BEC Threats
- Malicious Attachments
- Social Engineering Attacks
- Invoice Fraud
- Credential Phishing  
*and much more*

# HOW AN EMAIL RISK ASSESSMENT WORKS



## STEP 1 \ \ INSTALL VARONIS INTERCEPTOR ON YOUR INBOXES

- + The engagement begins with a personalized readiness call to understand your success criteria, existing tools, and scope.
- + Next, our skilled deployment engineer leads the installation process
- + Varonis is API-based and installation takes minutes

## STEP 2 \ \ EXAMINE INITIAL FINDINGS AND COMPARE EXISTING SOLUTIONS

- + The Email Risk Assessment runs over the course of 1-2 weeks depending on scheduling.
- + Assessment results identify types of threats currently reaching mailboxes with specific examples and a breakdown detailing how Interceptor found them.
- + Organizations also receive a business impact summary to understand the ROI of switching.

## STEP 3 \ \ BUILD A PLAN TO MIGRATE OR INTEGRATE

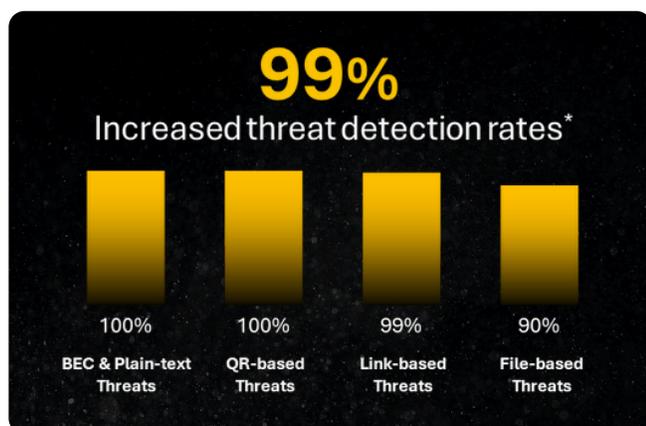
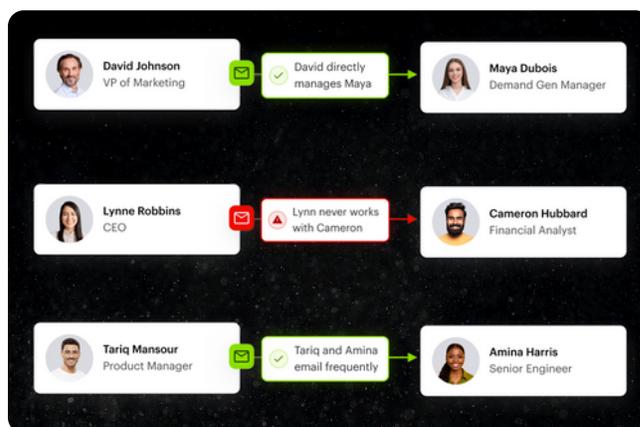
- + With risks identified, our expert team creates a prioritized plan for installation, remediation, and migration.

## INTERCEPTOR IN ACTION

Watch this short [video](#) showcasing the power and distinct capabilities of Varonis Interceptor.

## Most attacked users

See the top recipients of phishing emails within your organization, along with details on the type of threats common among them and where messages originated.

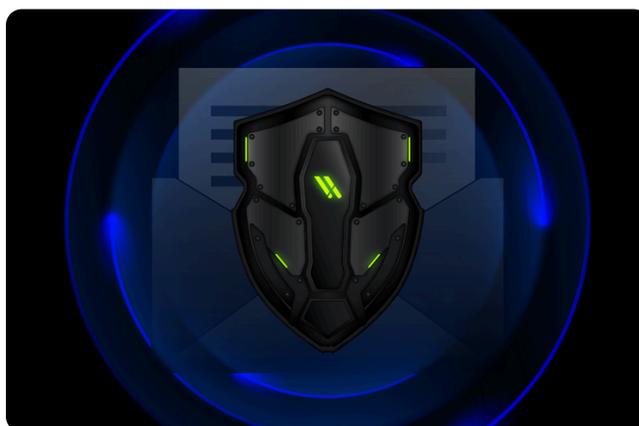


## Efficacy comparison

Understand what threats are leaking through. Security teams and leaders alike will see live and historical data without any tailoring or favorable filtering. The data will speak for itself.

## Business impact report

Gain insights on how identified threats can impact your business, where phishing is leading to identity and data compromise, and why Interceptor will achieve greater protection and ROI.



## STATE OF PHISHING REPORT

Uncover what Varonis Interceptor is catching for other organizations and the leading trends [here](#).

