



Ransomware Defense Validation

PROVE YOUR SECURITY INVESTMENTS ARE PROTECTING YOU RIGHT NOW

SECURE EMAIL GATEWAY VALIDATION

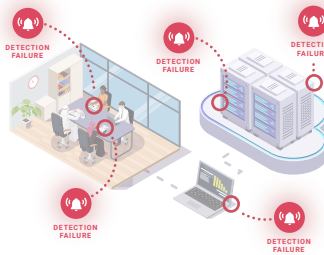
IS YOUR EMAIL FILTER BLOCKING EMAILS?



FILTER FAILURE

THREAT DETECTION VALIDATION

ARE YOUR SECURITY TOOLS DETECTING ATTACKS?



ALERTING FAILURE

THREAT RESPONSE VALIDATION

WILL YOUR MONITORING PROVIDER RESPOND?



RESPONSE FAILURE

Ransomware Defense Validation (RDV) simulates real-world cyber-attacks to consistently ensure your **secure email gateway** is effectively filtering malicious emails, **threat detection tools** are detecting attacks, and **threat response teams** are neutralizing threats in real-time.



Gain Operational Assurance

- ✓ Continuously confirm your defenses are optimally protecting your organization.



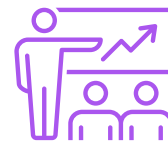
Proactively Reduce Risk

- ✓ Consistently test and validate your defenses before your cyber adversaries do.



Ensure Vendor Efficacy

- ✓ Trust but verify your security providers are meeting their SLA requirements.



Prove Investment ROI

- ✓ Present current investment ROI and justify any need for additional funding.



Demonstrate Readiness

- ✓ Visualize organizational preparedness for industry-specific adversarial threats.



Exceed Industry Standards

- ✓ Functionally prove your security controls are working as intended all year.

Discover the impact of RDV through our case study [here](#).