Veritas REDLab is a fully isolated, in-house security lab where we proactively test our products against the latest malware and ransomware to validate our cyber-resiliency capabilities.

Validates products with the latest threat intelligence.

Provides documented proof for business needs.

Goes beyond detection to deliver dynamic actions.

Keeping you resilient, compliant, and secure.

REDLab is built to be relentless. Because ransomware is relentless.

Total intrusion attempts in 2022: 6.3 Trillion

Total malware attacks in 2022: 5.5 Billion

TOP 6 REASONS Why Ransomware Fears Veritas REDLab

1. Laser Focused
   REDLab fosters a culture of continuous improvement, providing insights into new security policies, procedures, and incident response plans.

2. Independent
   REDLab utilizes cybersecurity research to validate assertions on ransomware resiliency and identify potential areas of attack.

3. Cyber Sleuth
   REDLab studies the top threats to provide insights to proactively improve our security solutions and identify potential areas of attack.

4. Unconventional
   REDLab analyzes emerging threats to devise attack strategies, exploring previously uncharted avenues of attack that automated security tools might miss.

5. Forward-Looking
   REDLab identifies vulnerabilities that help us organize, prioritize, and optimize security features across our portfolio and offers ways to speed recovery.

6. Text, Deliver & Repeat
   REDLab uses live malware and ransomware variants to simulate real-world scenarios, test our products’ capabilities, and inform future functionality.