

# RANSOMWARE FEARS VERITAS REDLAB

Keeping you resilient, compliant, and secure.



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**.

## Real-World Threat Testing in Real-Time

Cybersecurity **red teams** test an organization's defenses by pretending to be an enemy.



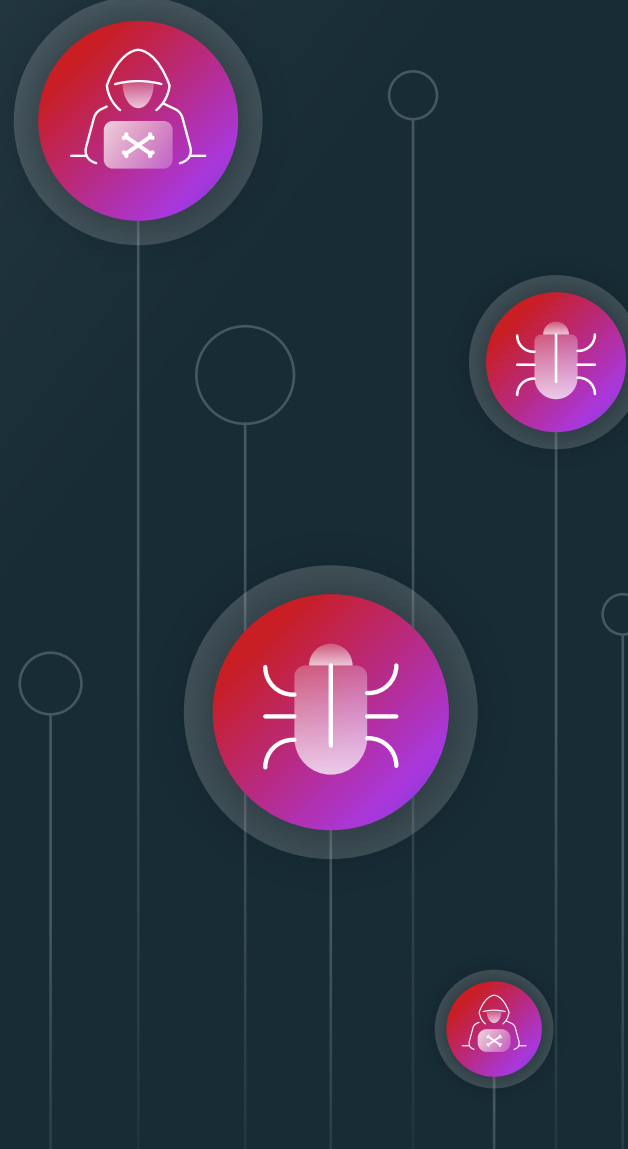
## REDLAB IS BUILT TO BE RELENTLESS. BECAUSE RANSOMWARE IS RELENTLESS.

**6.3 Trillion**

Total intrusion attempts in 2022.<sup>1</sup>

**5.5 Billion**

Total malware attacks in 2022.<sup>1</sup>



## TOP 6 REASONS

### Why Ransomware Feels Veritas REDLab

- 1 Laser Focused**  
REDLab fosters a culture of continuous improvement, providing insights to refine 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 known attack vectors and searches for previously unknown or "zero-day" vulnerabilities. Uncovering them reinforces the need for new defenses and rapid response strategies to mitigate risks.
- 4 Unconventional**  
REDLab employs creative thinking to devise attack strategies, exploring unconventional 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 Test, Deliver & Repeat**  
REDLab uses live malware and ransomware variants to simulate real-world scenarios, test our products' capabilities, and inform future functionality.

WHITE PAPER  
**Developing and Validating Malware Defense**

[Download Now >](#)

