MANDIANT

MANDIANT ADVANTAGE DATA SHEET

RANSOMWARE DEFENSE VALIDATION

Evaluate whether your security controls can prevent the latest ransomware

HIGHLIGHTS

- Safe and daily tests of your production security controls against the latest ransomware
- Automated, continuous and delivered via the Mandiant Advantage SaaS platform
- Validations based on active, relevant ransomware informed by Mandiant frontline intelligence
- Concise reports to help prove your ability to withstand the most likely ransomware attacks

Daily headlines highlight victims of increasingly frequent and widespread modern ransomware attacks. Organizations of all sizes and industries struggle to know whether they are prepared for a ransomware attack. With the right preparation and resources, you can dramatically reduce your organization's risk of falling victim to ransomware attacks and multifaceted extortion campaigns.

Mandiant Advantage Ransomware Defense Validation enables organizations to quickly understand their ability to prevent ransomware grinding their business to a halt. This solution, delivered through the Mandiant Advantage SaaS platform leverages Mandiant threat intelligence, ransomware repurpose capabilities and automated validation infrastructure. Most importantly, leaders will be able to more confidently and concisely present evidence to answer the question: "Will our security controls prevent our data from being encrypted by ransomware?"

Intelligence-led validation

Mandiant experts curate the latest ransomware families from frontline threat intelligence and repurpose them to run safely within your organization's production environment. Daily evaluations are based on active ransomware Mandiant sees targeting your industry and peers.

Rapid time-to-value

Ransomware Defense Validation conducts automated, daily evaluations of your critical production security controls with ransomware content relevant to your organization. Continuous evaluations provide daily feedback about whether your organization can withstand attacks from the latest and most relevant ransomware.

Reports and readouts

Reports are based on continuous ransomware evaluations and deliver concise details on your ability to prevent ransomware. Automated reports are augmented by discussions with Mandiant experts who review your progress and share insights on curated ransomware evaluations planned for your organization (Fig. 1).

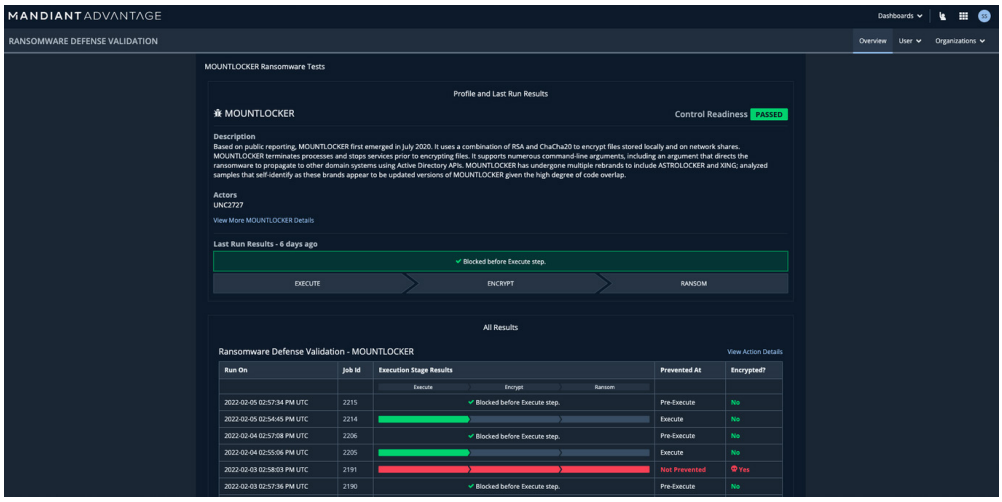

FIGURE 1. Detailed report on an organization's ability to prevent a specific ransomware family, including at which stage they failed or succeeded in prevention.

Dashboards and quantifiable data

Ransomware Defense Validation enables your team to proactively drive change with data points on how your security controls respond to ongoing ransomware attacks. A personalized dashboard presents a live graphical display of evaluation results. Quantifiable results arm your security team with the ability to track improvements over time and help prove your security controls prevent your data from being encrypted by ransomware (Fig. 2).

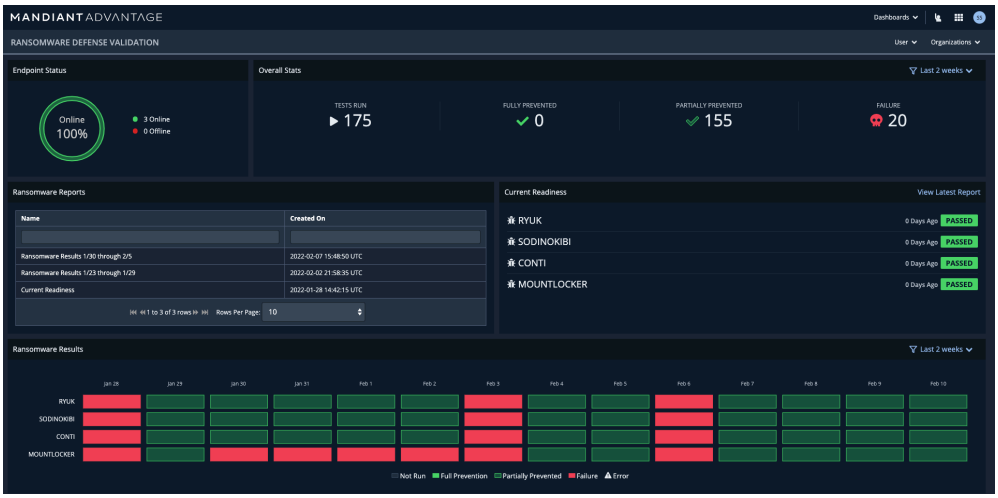

FIGURE 2. Ransomware Defense Validation dashboard.

Ransomware Defense Validation ultimately gives security leaders the evidence required to better show whether they can prevent the next big ransomware attack.

Learn more at **www.mandiant.com**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT