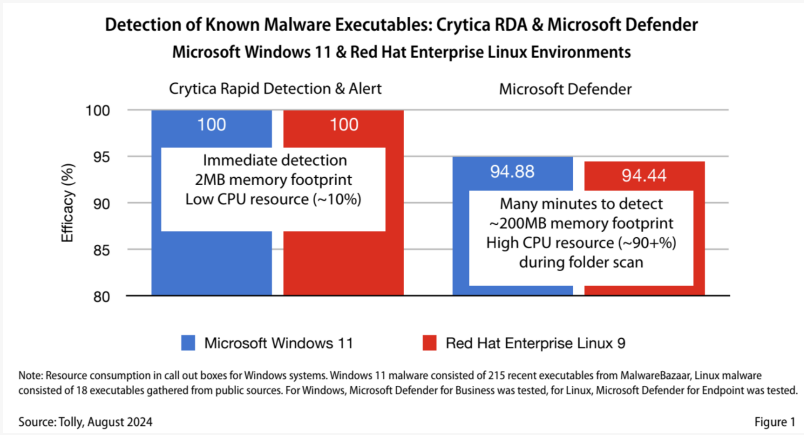
Tolly Group Report: Crytica Security Rapid Detection & Alert vs. Microsoft Defender

Crytica RDA Rapidly Detects Malware in Mission-Critical Operational Technologies



Crytica Security Tolly Group Report Figure 1

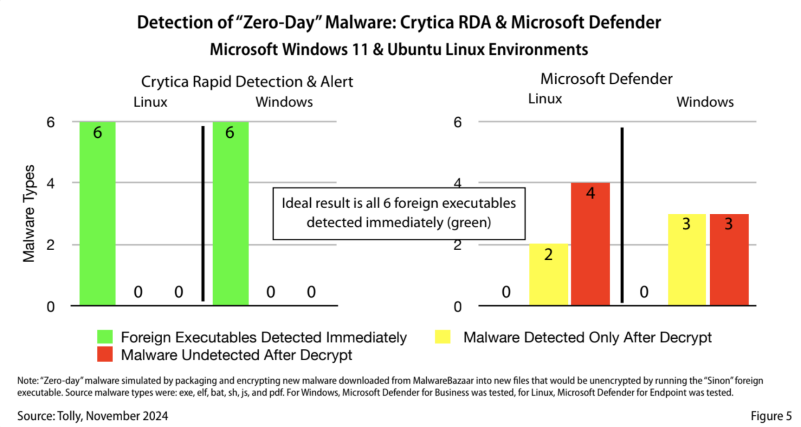
RENO, NV, UNITED STATES, January 15, 2025 /EINPresswire.com/ -- Crytica Security, a pioneer in next-generation cybersecurity, has received third-party validation for its patented Rapid Detection & Alert (RDA) technology. The Tolly Group, a leader in independent verification and validation services for information technology solutions, conducted rigorous testing to evaluate Crytica RDA's capabilities, and the results underscore Crytica's impact on advancing cybersecurity solutions.

> The findings in the Tolly Group Report showcase Crytica RDA's unprecedented ability to safeguard mission-critical infrastructure."
>
> *Kenneth Bible, former CISO for the Department of Homeland Security*

Kevin Tolly, Founder of the Tolly Group, shares, "Our testing found Crytica's technology exceptionally effective at detecting malware with speed and precision, even in resource-constrained environments like Operational Technologies and the Internet of Things. Crytica RDA addresses pivotal security challenges faced by mission-critical industries."

Kenneth Bible, former Chief Information Security Officer (CISO) for the Department of Homeland Security and a member of Crytica Security's board, also commented on the significance of these results: "Crytica's Rapid Detection & Alert technology is a game changer for cybersecurity. The findings in the Tolly Group Report showcase Crytica RDA's unprecedented ability to safeguard mission-critical infrastructure. It's a privilege to serve on the board of a company that is making such a major impact on Operational Technologies and Internet of Things cybersecurity. As we like to say at Crytica, 'If you can't detect, you can't protect.'"

The testing compared Crytica RDA with Microsoft Defender across Windows and Linux platforms, focusing on malware detection rates, speed, and resource efficiency. Crytica RDA detected 100% of both known and zero-day (previously undocumented) malware, identifying threats within seconds of injection. Microsoft Defender, by comparison, detected 94.4% of known malware but only between 33% and 50% of zero-day malware, with detection occurring only after the malware was decrypted and executed. Crytica RDA also outperforms Microsoft Defender in resource efficiency, using just 2MB of memory and minimal CPU usage (~10%), compared to Defender's significantly higher memory consumption (200–368MB) and CPU usage peaking at 96%.



Crytica Security Tolly Group Report Figure 5

C. Lloyd Mahaffey, former head of Apple Federal Systems and Executive Chairman of Crytica Security, explains, "What sets Crytica Security apart from other cybersecurity solutions is its innovative approach and patented design that allows it to uniquely fit into the myriad of Operational Technologies deployed within mission-critical environments like public utilities."

Unlike traditional cybersecurity solutions that rely on threat intelligence databases, Crytica RDA focuses on identifying unauthorized changes to a device's internal instruction sets. This method allows Crytica to detect previously undocumented malware in real time, which significantly reduces the risk of advanced persistent threats and zero-day attacks. Additionally, Crytica RDA does not generate false positives, ensuring accurate alerts that help organizations concentrate their resources on addressing actual threats.

For the first time in its history, Crytica Security has third-party validation of its technology and capabilities. This milestone affirms the benefits Crytica brings to essential sectors, such as public utilities, healthcare, and government agencies. In 2025, Crytica is poised to expand its impact, offering industries a proven solution that enhances cybersecurity defenses while minimizing resource consumption.

For a detailed overview of the testing and results, refer to the full Tolly Group report.

About Crytica Security:
Crytica Security is the first patented, multi-mesh, survivable Rapid Detection & Alert™ (RDA™) solution for malware that can be embedded in industrial control system Operational Technologies (OT), Internet of Things (IoT) devices, and Information Technologies (IT) to complement and dramatically improve existing XDR, MDR, and EDR cyber defense stacks within government agencies, companies, healthcare institutions, and public utilities. For more information, please visit www.cryticasecurity.com.

Crytica Security — If you can't detect, you can't protect.

Dr. Kerry Nemovicher
Crytica Security
+1 775-762-2627
email us here
Visit us on social media:
LinkedIn
