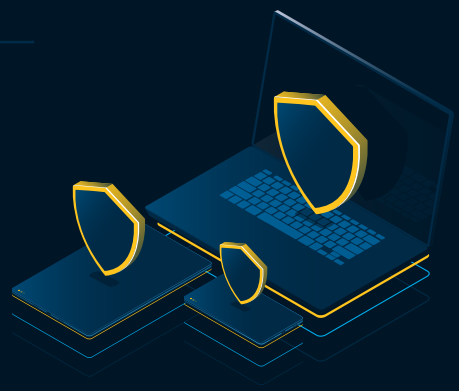
VMRAY Life Fitness

How VMRay helps Life Fitness
ANALYZE EDR/XDR ALERTS



CASE STUDY – SPORTS & LEISURE

> With a small team, our processes were **time-consuming and ineffective**. With VMRay's auto-forwarding feature, the **time our analysts needed is nearly halved**, which saves us precious time to focus on our strategic tasks on improving our defenses.
>
> **Brad Marr**
> Senior Director & CISO

2x
Faster analysis with Auto-Forwarding

Life Fitness, a U.S.-based company dedicated to creating innovative fitness solutions that benefit facilities and health conscious consumers.

With 75% of organizations in the US experiencing a successful phishing attack in 2020 – and 96% of those threats arriving by email – CISO Brad Marr has made it a priority to strengthen anti-phishing protections.

As Senior Director and CISO at Life Fitness, Brad Marr is responsible for keeping the company's security systems in fighting form with a small staff. As with many organizations, phishing is the top attack vector for Life Fitness. **Only 7% to 15% of incoming email is considered clean.**

The company's core phishing defense platforms detect and stop a high percentage of tainted emails and related malware and malicious links. But where detection results are inconclusive, a small percentage of suspect messages get through.

"When that happens — whether we see it ourselves or it's reported by an end-user – we need to determine, with a **high level of confidence**, whether the email is malicious or not," Brad says. "VMRay is our source of truth for that."

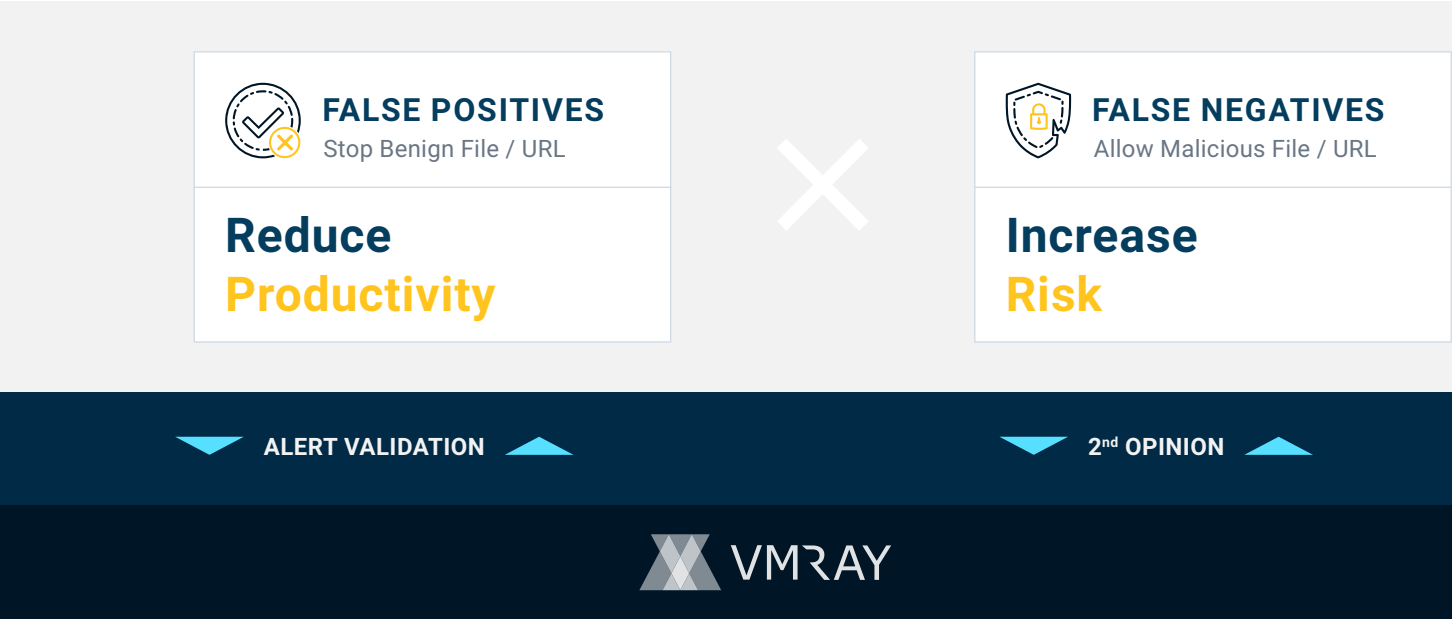
PROBLEM
Small team of analysts
Manual phishing analysis
Looking for ways to automate

IMPACT
Time-consuming process
Delays in notifying users
No time for strategic tasks

SOLUTION
Automated detonation
Less time spent on analysis
Focus on improving defenses

Brad and his team use VMRay to vet likely false positives (FPs) generated by Endpoint Detection and Response (EDR) systems, which are notorious for being over-sensitive. It becomes trickier especially when it comes to Macro-enabled files and Powershell scripts that used by both adversaries and legitimate programs.

> We'll see files that EDR says are malicious and should be blocked. But when we look at the surface information, they sometimes appear to be benign.
>
> If you get an ambiguous result for a Powershell script — and you assume it's malicious and block it — you're going to stop the business. On the other hand, if you treat those scripts as if they're benign and allow them through, that also puts you at risk.



Not stopped by the Hop-Hop-Hop

Adversaries eventually catch on to the evolving techniques used in phishing analysis, and they develop countermeasures to evade detection. A common technique is to create an attachment with an embedded link that redirects the user to a final, malicious destination that is 3 or 4 hops away.

> "Often, the first 2 or 3 links are harmless. Some tools don't dive in enough. They'll only go to the first or second hop and then say, 'It's clean.'
>
> VMRay follows those redirections **all the way to the end** so malicious activity can be identified and mitigated.

When VMRay determines an email is malicious, that information can be used to identify other users who have received the same message. A company-wide block can then be put in place so they're not affected. "If 50 people are at risk, catching that one message spares the other 49 from a potential credential harvesting threat.".

What Auto-Detonation Looks Like

> The process was time-consuming and ineffective, and it caused delays in notifying users about whether a message was safe or not.
>
> VMRay not detects where that link goes, and with screenshots it enables our analyst to determine if the credentials page is safe, **at a glance**.

In June 2019, to supplement the company's existing defenses, Brad's team deployed VMRay's **cloud-based** threat detection solution. Previously, they had used an on-premises sandbox lab to manually detonate and analyze each message that was submitted.

While 70% of the company's security workload is handled by a managed services provider, Brad has kept responsibility for phishing analysis in-house, with the workload split between him and his analyst. They set up auto-forwarding from the existing phishing mailbox to the VMRay environment, which automatically detonates each email to detect indicators of compromise (IOCs).

SENDER CHECK

VMRay looks at senderinformation and the originating **IP and mail server**.

URL CHECK

VMRay determines whether the **external sites** that attachments and links reach out to are malicious.

IN-DEPTH VISION

The system generates an analysis report, which includes **screenshots** of potentially harmful activity.

NOISE-FREE REPORT

Analysts can **quickly scan** through clear reports to determine if any follow-up action is required.

RESULTS

> With VMRay, our analyst has carved out a daily time saving of 1 to 2 hours.
>
> This freed him to focus on bigger things like making sure our businesses are being supported, managing risk, and tuning our phishing defenses to catch new threats

BEFORE	AFTER
4 hours/day **SPENT** analysis with previous solution	**1-2** hours/day **SAVED** for strategic tasks with VMRay

Contact Us

Email: sales@vmray.com
Phone: +1 888 958-5801

VMRay GmbH

Universitätsstraße 142
44799 Bochum • Germany

VMRay Inc.

22 Boston Wharf Road, 7th Floor
Boston, MA 02210 • USA

VMRAY