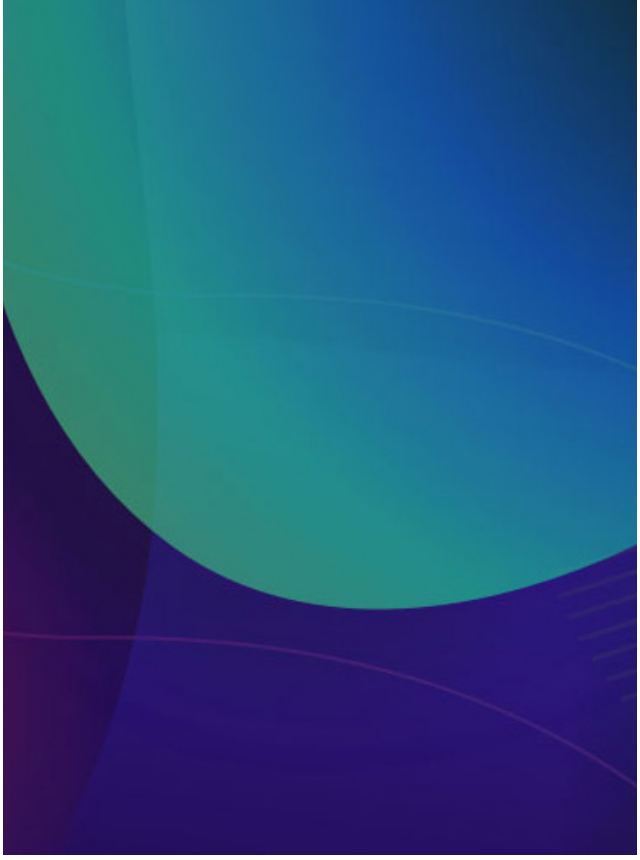
SLASHNEXT

URL Scanning vs. URL Analysis and Enrichment

What's the Difference and Why it Matters



42%

Security professionals report using URL scanning services

In a survey of security professionals, many reported using different types of methods to research and determine if suspicious URLs are malicious. The most popular methods used by nearly half of the respondents were commercial phishing URL databases and commercial real-time URL scanning services.*

*SlashNext engaged Survata, an independent research company, to conduct a survey of cybersecurity professionals in the United State in late 2019.[1]

Introduction

Most security teams, security vendors, MSSPs, and ISPs seek to know if URLs in their emails, network, or endpoint traffic are malicious. In many cases, they use URL scanning services. These typically involve a look-up against a curated database of known threats. In other cases URL scanning may involve a check of the reputation of the domain hosting the URL. Security analysts and threats researchers performing phishing incident response and threat hunting may also utilize URL enrichment services, either manually or through automated playbooks.

Advanced Evasion Tactics to Avoid Detection

Lightweight URL scanning services provide relatively accurate verdicts on known threats or obvious phishing pages. However, they are often not updated quickly enough, or fail to detect, the growing number of more sophisticated, fast-moving phishing threats. More advanced threat actors use multiple evasion tactics to avoid detection by the average URL inspection and domain reputation analysis services. Most commonly, this is done through a combination of dynamic URL re-directs and phishing pages on compromised websites that are hosted on legitimate infrastructure. Sites that typically aren't blacklisted. Some attackers also evade detection by serving up benign pages to traffic from IP blocks associated with different security vendor's cloud infrastructure that inspect their sites. Attackers also use latently weaponized webpages to avoid detection at time of delivery. They prop up phishing pages and take them down within a few minutes to hours to avoid detection and blacklisting. This means that many phishing threat databases and scanning services return false negatives on more elusive, previously unknown threats. Unfortunately, these tend to be the most dangerous kind.

Stay Ahead of the Threats

Robust detection methods are essential to stop elusive, short-lived threat tactics. Accurate phishing URL analysis on-demand and at scale is key. Automating phishing URL analysis services can provide accurate, definitive results and enrichment to speed execution of phishing IR playbooks, analysis, and reporting. However, it's critical to use intelligence that can detect multiple payloads with accuracy and provide detailed forensics, including screenshots, HTML, and rendered text.

Here are some fundamental differences between URL scanning and URL analysis.

URL scans may return false negatives when the threat database is not updated with accurate, real-time phishing threat intelligence.

Scans relying on domain reputation analysis typically fail to detect phishing sites hosted on legitimate (but compromised) websites or legitimate hosting infrastructure.

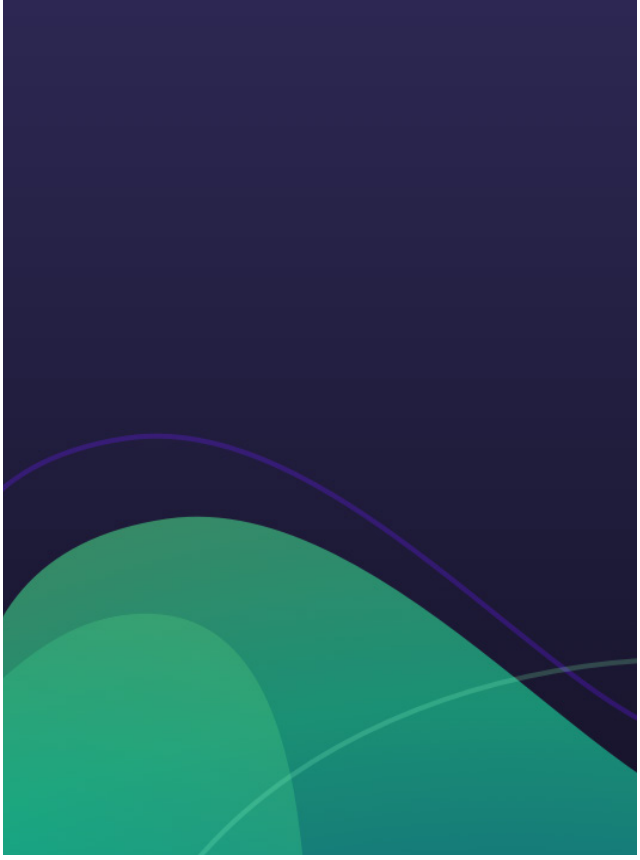
Many phishing attacks use links with multiple URL redirects. The initial URL is often not the ultimate destination page, so scans against a threat database may not find a match.

Scanning technologies often fail to overcome advanced evasion tactics and cannot detect multistage tactics that require user interaction, such as popups and Captchas.

Some URL scanning and domain reputation services deliver arbitrary threat risk scores rather than definitive verdicts. Without definitive, binary verdicts, more manual research may be required, making automation actions difficult.

Scans focus on fake log-in pages for major brands but can return false negatives on many other types of dangerous phishing and social engineering payloads.

Lack of enrichment. While some scans return verdicts plus first seen and basic Geo IP data, most lack more detailed forensics data such as screenshots and HTML.



40%

Lack definitive, accurate verdicts from their security systems and/or URL look-up resources

When determining if a suspicious phishing URL is malicious, the top 3 challenges cited by security professionals were: 1) URL redirection / forwarding when the initial URL directs to a safe unblocked page or site and automatically re-directs users, through a series of re-directs, to the ultimate malicious page destination. 2) Identifying previously unknown suspicious URLs. 3)Lack of definitive, accurate verdicts – from their security systems and/or URL look-up resources.

*SlashNext engaged Survata, an independent research company, to conduct a survey of cybersecurity professionals in the United State in late 2019. [1]

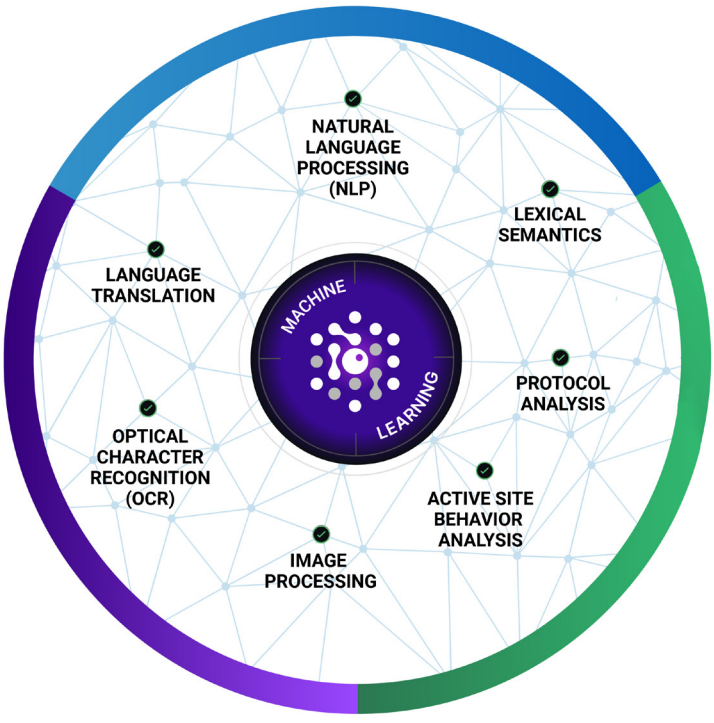
The Bottom Line

It may seem like a small difference in semantics when talking about URL scanning vs. URL analysis, but the differences and benefits can be critical to helping security teams protect their organization against threats. The use cases for more accurate URL analysis are many. SOAR playbooks for automated phishing IR and threat hunting can now get more accurate threat intelligence and forensics. Email security solutions can achieve greater efficacy, particularly for previously unknown and more elusive threats. Service providers can provide better, more automated services to their customers.

Advanced Evasion Tactics to Avoid Detection

Detecting sophisticated, elusive, and short-lived threats requires a more robust phishing URL analysis and enrichment method. To address this need, SlashNext pioneered and patented an approach called SEER™. It uses millions of virtual browsers to click on links (as a user would) to follow through on re-directs, and do more thorough run-time analysis of final page contents. Instead of relying on domain reputation or doing a scan to compare against log-in pages of major brands, it does deeper analysis of the page using computer vision, NLP, site behavior analysis, and machine learning. The SEER approach offers many advantages over light weight URL scanning methods. This includes overcoming evasion tactics and producing more accurate, definitive verdicts on a wider variety of phishing threats. It also produces a wealth of artifacts, enriching URLs with forensics data which can be used for further analysis and reporting.

SEER™ Threat Detection Technology



The SlashNext Advantage

Phishing URL Analysis and Enrichment powered by SlashNext SEER technology goes much further than the average URL scanning technologies. By using millions of browsers to dynamically analyze page contents and site behavior, it delivers highly accurate, definitive verdicts and rich forensics data to power security technologies and automated playbooks. Together with a broad, multi-vector, global sensor network, SlashNext real-time phishing threat intelligence detects thousands of threats missed by other URL intelligence services.

The advantages of SlashNext-powered URL analysis include:

Broader, high-fidelity, real-time intelligence on the latest phishing threats.

Highly accurate, definitive, binary verdicts (not threat scores), enabling better automation and a block-ready threat feed (blocklist) for phishing protection solutions and network controls.

Overcoming numerous evasion tactics such as shortened URLs, multiple re-directs, and multi-stage attacks that require user interaction, such as Captchas.

Detection of phishing pages hosted on both compromised websites and legitimate hosting infrastructure.

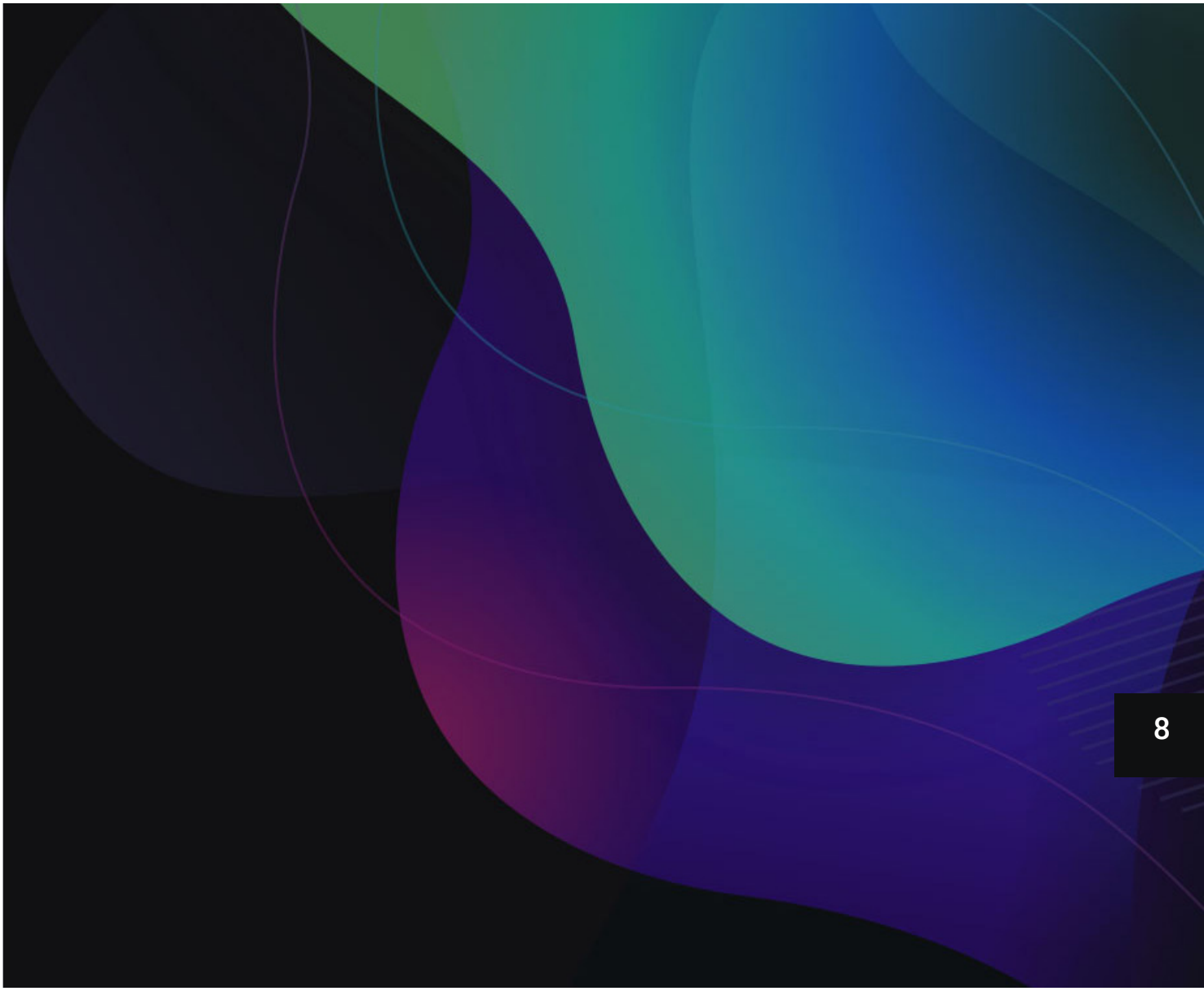
Rich forensics data for further analysis and reporting. In addition to verdicts and threat status, users can access threat type, first seen / last seen data, Geo IP, screen shots, HTML, and text.

Pre-Built Integrations for Phishing IR, Threat Research, and More

URL Analysis & Enrichment is easily accessed via integration apps with leading SOAR, SIEM, and TIP solutions. Add automated phishing URL analysis to your phishing IR playbooks, network log threat hunting, and more. Just check out our Technology Partners list at www.slashnext.com/technology .

About SlashNext

SlashNext helps organizations close the gaps in their existing defenses against today's—and tomorrow's—more advanced phishing and social engineering threats. SlashNext provides IT security teams with a range of real-time phishing protection, phishing incident response, and threat hunting solutions to protect users, both inside and outside network perimeter protections.



Survey Methodology

[1]SlashNext engaged Survata, an independent research company, to conduct a survey of cybersecurity professionals in the United State in late 2019. Respondents came from a certified panel of security decision-makers working for large organizations with security operations centers (SOCs). They were required to currently be a part of their organization's enterprise cybersecurity team, which had a SOC, and used at least one threat intelligence feed.