OpenText Threat Intelligence File Reputation Service

Dynamic file reputation intelligence to stop malware distribution

Overview

- As malware continues to proliferate, organizations of all sizes need additional layers of defense within their security infrastructure
- Network-based malware detection technologies can be overwhelmed and bypassed
- File intelligence can quickly identify malware and trustworthy files so potential threats can be investigated

Malware hides within the sheer volume of files companies encounter. In fact, the AV-TEST Institute registers more than 350,000 new malicious programs every day. This volume of malware makes the need for strong file reputation capabilities critical in combating threats, as well as freeing up valued security resources by allowing known good files to bypass sometimes over-taxed security infrastructure.

The OpenText™ Threat Intelligence (BrightCloud) File Reputation Service provides up-to-the-minute file intelligence derived from millions of real-world sensors. Each file is analyzed by the latest machine learning techniques and vetted through years of threat expertise. This real-time lookup service of known malicious and allowed file identifiers helps to effectively stop the distribution of threats through networks. This verification significantly reduces the amount of "noise" by enabling policies to automatically determine which files to allow, block or investigate further, allowing security administrators to focus on unknown potential threats.

This service uses industry standard file hashes as fingerprints to uniquely identify files, regardless of filename, platform, encryption or password protection. It responds to authorized requests to look up the reputation of the file hash in the OpenText Threat Intelligence Services Platform.

The service then responds with a determination of Good, Bad or Unknown/Unclassified, as well as several other security attributes associated with the file, including:

- The type of malware it contains
- The number of times the file has been seen across the OpenText Threat Intelligence Services Platform
- When it was first detected
- The date of its classification or most recent determination

86% of malware is unique to a single PC.[1]

The OpenText Threat Intelligence Services Platform is updated via millions of enterprise and consumer endpoints and network security devices around the globe, continuously receiving the latest information on emerging threats. In addition, file data is correlated with URLs, IPs and mobile apps to provide a comprehensive view across the threat landscape. Mapping the relationships between these different data points enables OpenText Threat Intelligence to provide partners with highly accurate intelligence that is always up to date. This automated network dramatically reduces the time to detect for emerging threats and provides real-time protection to prevent malicious files from entering networks and spreading to unsuspecting users. To date, OpenText Threat Intelligence contains more than 38 billion detailed file behavior records and grows more intelligent by the day.[2]

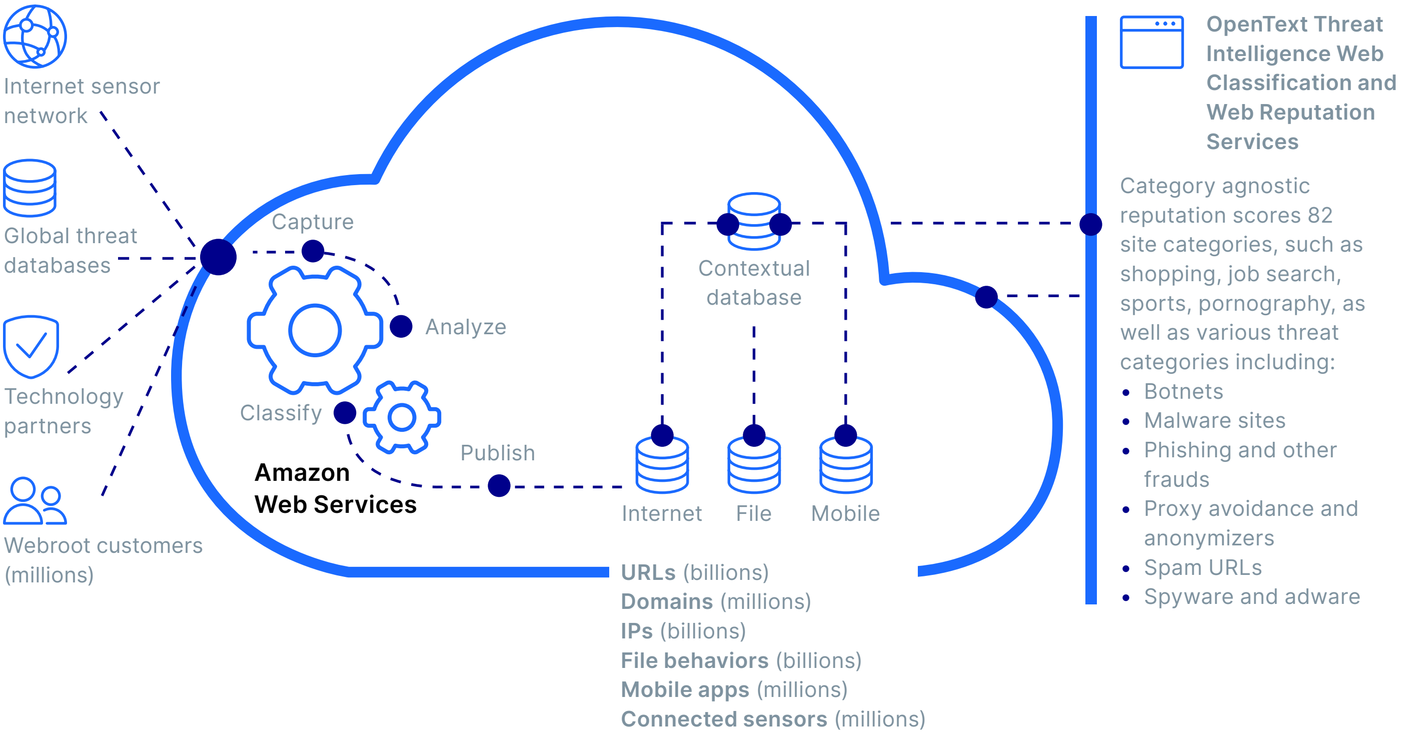
Partner benefits

- **Differentiate yourself from your competition**
  Reduce noise at the network edge, freeing up your customers' security resources to focus on the most pressing threats
- **Leverage the OpenText Threat Intelligence Services Platform**
  Harness collective threat intelligence from millions of sources via the world's most powerful cloud security platform
- **Take advantage of easy integration**
  Simple integration through RESTful API and an SDK into your solution
- **Experience no network impact**
  Protects through your network devices and increases user capacity by eliminating unwanted traffic

[1] 2022 BrightCloud® Threat Report

[2] Ibid.

OpenText Threat Intelligence Platform



OpenText Threat Intelligence API

OpenText Threat Intelligence Web Classification and Web Reputation Services

Category agnostic reputation scores 82 site categories, such as shopping, job search, sports, pornography, as well as various threat categories including:

- Botnets
- Malware sites
- Phishing and other frauds
- Proxy avoidance and anonymizers
- Spam URLs
- Spyware and adware

Figure 1. OpenText Threat Intelligence File Reputation Service

The OpenText Threat Intelligence File Reputation Service in action

The OpenText Threat Intelligence File Reputation Service helps network edge appliances, such as next-generation firewalls and intrusion detection/prevention devices, determine whether files are trustworthy, malicious or require further investigation. Additionally, it helps cloud-based storage providers ensure customers' stored files are free from malware. It also enables web and email hosting providers to scan hosted files to ensure that both the website/email owner and provider are aware of any hosted or queued malware.

OpenText Threat Intelligence File Reputation Service data is backed by more than 95 million real-world endpoints and their encounters with everyday applications, including malware.[3] Because of the constantly updated feed, the OpenText File Reputation Service is often much faster than other leading services in discovering zeroday threats.

Additionally, when coupled with OpenText Threat Intelligence Streaming Malware Detection, the File Reputation Service makes an especially effective tool against traditional and modern malware.

Designed to combat the challenges of polymorphic malware, OpenText Threat Intelligence Streaming Malware Detection allows our partners' devices to make determinations at the network level enabling users to quickly allow, block or flag files for investigations. Since the files often don't need to be fully downloaded, this service frees up network bandwidth by dropping malware at the perimeter and eliminates the need to re-inspect benign files.

Easy integration

Traditional antivirus solutions offer a heavy and rigid approach to integration, sacrificing usability and performance for companies trying to integrate them. The OpenText Threat Intelligence File Reputation Service provides an easy-to-integrate API so partners can use the extensive OpenText Threat Intelligence database to build malware detection into products and better protect users. Additionally, this service combines with existing security solutions through the same SDK as other OpenText Threat Intelligence services, making integration as simple and straightforward as possible.

[2] 2022 BrightCloud® Threat Report