Puffin Cloud Isolation: Future-proof Browser Security Against Zero-day Attacks

Protect endpoints web environments from both known and unknown exploits with the latest cloud-based remote browser isolation technology.

Introduction

Since the invention of the web browser 30 years ago, it has become the most critical application on our devices. Many of our daily tasks, from work to entertainment, rely on web browsers. As a result, they have become one of the most popular targets for cybercriminals. In 2020, the estimated monetary loss from global cybercrime was $945 billion USD. Whenever a web browser announces a security fix, the vulnerability being addressed may have already been exploited by hackers. Modern web browsers and operating systems are so sophisticated that the likelihood of zero-day vulnerabilities are inevitable.

A traditional secure web gateway uses URL filtering or content inspection to block malicious web pages and protect endpoints. However, these pattern-matching-based algorithms can only stop known exploits and might unintentionally block harmless web pages. It cannot detect sophisticated attacks that hide their signature in dynamic content or unrecognized exploits that target zero-day vulnerabilities. Hence, web browsers are still at great risk.

Unlike other traditional solutions on the market, Puffin Cloud Isolation uses an entirely different approach to stop all forms of web threats. Instead of blocking exploits, we developed the Puffin Remote Browser technology to isolate and nullify them. In conjunction with Puffin Remote Browser, unsafe web pages are fetched, rendered, and executed within a cloud sandbox on remote servers. All dynamic content from external sources will not come into contact with internal endpoints. Through this technology, no malicious content will be able to exploit users' web browsers. Clean web pages will also not be mistakenly blocked.

[1] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Figure 1: Puffin Cloud Isolation Architecture

Puffin Remote Browser first isolates and disarms insecure web pages, then converts them to a display-only remote browser graphics language format. Puffin Cloud Isolation then constructs new web pages from it so that endpoint web browsers can present identical visuals, only this time without the harmful content of the original. Our proprietary remote browser graphics language functions as the air gap dividing external hazardous Internet content and internal secured web environments.

Puffin Cloud Isolation and Puffin Remote Browser work together to deliver a seamless web isolation experience that protects endpoints from current and future web threats without changing user behavior. Neither additional applications nor browser extensions are needed to use Puffin Cloud Isolation; its zero-footprint architecture allows users to effortlessly access protected web environments with their preferred web browsers.

Puffin Remote Browser

Puffin Remote Browser is the core Browser-as-a-Service platform used in all CloudMosa remote browser solutions. It is a large-scale, multi-data center, and high availability cloud service that supports over 10 million monthly active users around the world. An endpoint first connects to Puffin Remote Browser to create a remote user session and forward user events and gestures. Each session has its sandbox processes for web, JavaScript, and Flash Player engines. The remote browser user session issues HTTP requests on the user's behalf and handles HTTP responses in isolated sandboxes. After the sandbox parses, renders, and executes web content, it uses our proprietary remote browser graphics language to present the web page exterior, free of untrusted web data. During the user session, the sandboxes receive user events from the endpoint and continuously update the graphic language data based on web page visual changes.

Puffin Remote Browser can handle different types of web content, including HTML, CSS, JavaScript, and Flash. It also supports various multimedia resources, including still and animated images, audio/video clips or streams, SVG, web fonts, and more. Standard web resources are processed in a sandbox environment with our proprietary remote browser engine derived from Blink. Flash content is handled on a different sandbox with Flash Player and our proprietary remote PPAPI implementation.

Web threats do not only reside in web pages. Malicious web sites can exploit endpoints via downloading files containing malware or viruses. Puffin Remote Browser works with 3rd party cloud storage services such as Dropbox, Google Drive, and OneDrive to isolate downloaded files from endpoints by directly transferring them into the user's cloud storage space. Users can view or edit downloaded documents and files in the cloud storage without physically storing documents in their local device. Puffin Remote Browser can also be integrated with 3rd-party virus scanning services to verify downloading files on-the-cloud. There is also a document preview feature that converts DOC, PPT, XLS, and PDF documents into a read-only web page to avoid unnecessary file downloads.

Puffin Remote Browser not only function as an isolation layer for individual endpoint web security but also as a simple, efficient and comprehensive browser management layer for enterprises. For Puffin Remote Browser Enterprise Edition, we offer an admin interface for monitoring service status, auditing user access logs, and enforcing enterprise web security policies (web filtering, clipboard operation, file uploading, file downloading, virus scanning, document previewing, etc). With Puffin Remote Browser, enterprises can deploy a secured and managed web environment across all endpoints.

Remote Browser Graphics Language

The Remote Browser Graphics Language is an API and network protocol used between Puffin Remote Browser and Puffin Cloud Isolation. It uses hierarchical layers and vector-based drawing commands to represent the web page's appearance.

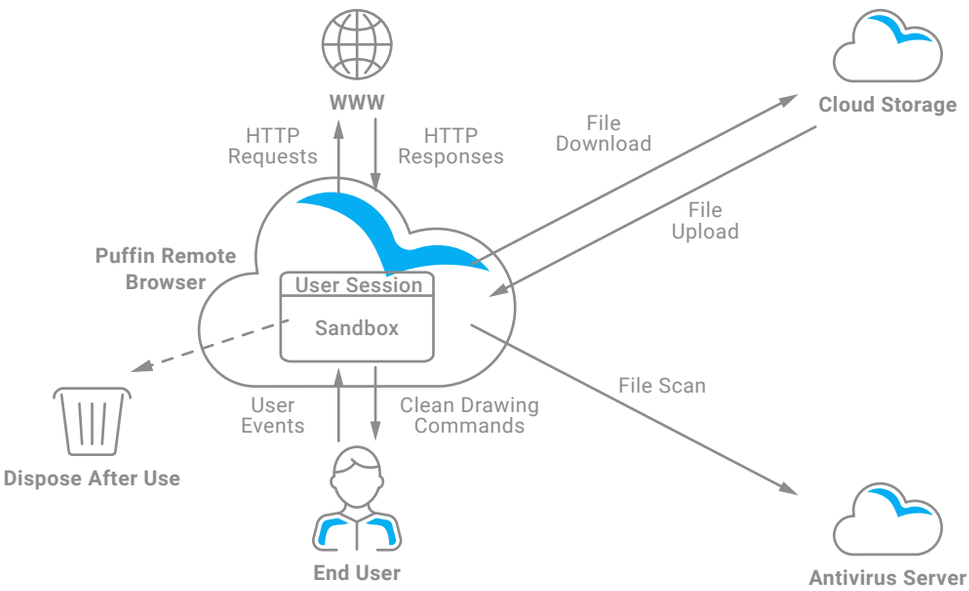

Figure 2: Puffin Remote Browser Platform

Generic web contents, including text and images, are defined by content layers with vector-based drawing commands in Remote Browser Graphics Language. Special web elements such as video streaming, Flash content, HTML canvas, and WebGL canvas are defined in separate layers. Remote Browser Graphics Language is designed to efficiently represent dynamic web content, as the Puffin Remote Browser doesn't need to send fully rendered data for each web page change. On web page scrolls, only the attributes of corresponding layers need to be updated. On web page content changes, only the difference in their drawing commands needs to be sent.

Compared with other pixel-based web isolation solutions, Puffin's Remote Browser Graphics Language provides exceptional visual quality and uses less data to render remote web pages. The vector-based drawing commands preserve original text and graphics quality, adapting to various endpoint screen dimensions and resolutions. The heterogeneous layers optimize content streaming based on the each layer's characteristics, and the hierarchical layer structure increases remote content scrolling performance.

The Remote Browser Graphics Language is an intermediate data format used in all our remote browser products. It transmits the web page's appearance and behaviors losslessly without any web technologies like HTML, CSS, JavaScript, and Flash so that no browser exploits can apply. Remote Browser Graphics Language is a comprehensive, efficient, and secure format to present web content post-isolation.

Puffin Cloud Isolation

Puffin Cloud Isolation is the web gateway for endpoints to use Puffin Remote Browser Server's web isolation service from browsers. Compatible platforms include the latest version of Google Chrome and Microsoft Edge; Safari and Firefox support to be added at a later date.

Puffin Cloud Isolation provides a native user experience on isolated web pages, supporting most web browser functionality. This includes, but is not limited to the following; page navigation, browser history, keyboard and mouse events, file upload and download, clipboard copy, cut and paste, context menu, open dialogs and windows, and geolocation services. Users do not need to install extra software or learn how to use Puffin Cloud Isolation. The zero-footprint architecture and native user experience let users adapt to Puffin Cloud Isolation effortlessly.

Puffin Cloud Isolation provides public cloud service and private deployment. Users can subscribe to CloudMosa's Puffin 365 subscription service to use Puffin Cloud Isolation via the "i.puffin.com" prefix in front of web page URLs for their current web browsers. i.puffin.com also has a special shared-computer mode for users to protect their privacy on a public or shared computer. Puffin Cloud Isolation will not store user credentials, website cookies, or local storage data on the web browser in shared-computer mode. It will also automatically log out user sessions after a specific idle time and wipe out all user data.

Puffin Cloud Isolation also comes with an optional browser extension, Puffin Cloud Isolation Assistant. Users can enable or disable the current tab's web isolation function with a single click. This extension can, by user preference, enforce browsers to open new tabs in web isolation automatically.

Puffin Cloud Isolation can be installed in a private cloud or on-premises. Enterprises and organizations can deploy a packaged Puffin Cloud Isolation and Puffin Remote Browser solution inside their network and integrate with other network security components. Puffin Cloud Isolation can be configured as a TLS-interception web proxy to intercept insecure web pages into secure isolated pages in a private deployment. In this web proxy mode, the IT admin needs to configure Puffin Cloud Isolation as a transparent proxy or explicit proxy for endpoints. The TLS-interception certificates also need to be installed on endpoints for the Puffin Cloud Isolation proxy server to detect HTTPS requests and rewrite HTTPS responses.

Puffin Cloud Isolation as a web proxy or web server is easy to integrate with other network security components in enterprises. A recommended architecture for Puffin Cloud Isolation with other secure web gateways is to deploy Puffin Cloud Isolation between the Internet and SWG. Puffin Cloud Isolation is the first tier of defense against the external network to maximize the web environment protected by web isolation and keep other network security features like malware/anti-phishing URL filtering, content inspection, virus scanning, etc.

The high availability and load balanced architecture of Puffin Cloud Isolation make it reliable and easy to expand. Enterprises can dynamically create Puffin Cloud Isolation server nodes and adjust isolation cluster size as necessary.

Conclusion

Zero-day exploits are among the most severe threats to cybersecurity and traditional web security technologies. Only remote browser isolation tactics can stop zero-day attacks permanently. This technology isolates all web contents making any web threats unable to reach the endpoints, guaranteeing a secure web environment.

Based on CloudMosa's market-proven remote browser technology, Puffin Cloud Isolation is the most advanced remote browser isolation solution for both individuals and enterprises. Its exceptional vector-based graphics format delivers lossless web pages at superior quality and efficiency. Our unique remote browser graphics language provides an absolute insulation layer that divides untrusted external web content from now-protected endpoints. The high availability and load balanced cloud architecture make it suitable for deployments of varying scales.

Visit https://www.puffin.com/cloud-isolation/ to learn more about Puffin Cloud Isolation.