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

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

Introduction

Since the web browser's invention 30 years ago, it has become the most critical application on our computers. Many of our daily tasks, from work to entertainment, rely on web browsers. That makes browser attacks one of the most popular ways for cybercriminals to inflict damage. In 2020, the estimated monetary loss from global cybercrime was $945 billion. Whenever a web browser announces a security fix, hackers might already use that vulnerability for some time. Modern web browsers and operating systems are so sophisticated that the existence of zero-day vulnerabilities is inevitable.

Traditional secure web gateway uses technologies like URL filtering or content inspection to block malicious web pages and protect endpoints. But these pattern matching-based algorithms can only stop known exploits and might block harmless web pages on a false alarm. It cannot detect sophisticated attacks hiding their signature in dynamic contents or exploits targeting zero-day vulnerabilities. Hence, web browsers are still under threat.

Unlike previous technologies, Puffin Cloud Isolation uses a different method to stop all web threats eternally. Instead of blocking web threats, we developed the Puffin Remote Browser technology to isolate and nullify them. Puffin Cloud Isolation uses Puffin Remote Browser to fetch, render, and execute unsafe web pages in a cloud sandbox on remote servers. All dynamic contents from external sources will not contact internal endpoints. Therefore, none of the malicious content will exploit users' web browsers. This isolation technology will not obstruct an innocent web page nor miss malicious content.

[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 isolates and disarms insecure web pages and converts them into a display-only remote browser graphics language format. And then, Puffin Cloud Isolation constructs new clean web pages out of the graphics data from Puffin Remote Browser so that web browsers on endpoints can present identical web content visuals without the questionable content. The proprietary remote browser graphics language between Puffin Remote Browser and Puffin Cloud Isolation plays as the air gap dividing external hazardous Internet and internal secured web environments.

Puffin Cloud Isolation and Puffin Remote Browser work together to deliver a seamless web isolation experience that can protect 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 lets users access protected web environments with preferred web browsers straightforward.

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, high availability cloud service that can support over 10 million monthly active users globally. An endpoint first connects the Puffin Remote Browser to create a remote user session and forward user events and gestures. Each user session has its sandbox processes for the web engine, JavaScript engine, and Flash Player engine. The remote browser user session issues HTTP requests on the user's behalf and handles the HTTP responses in isolated sandboxes. After sandbox parses, renders, and executes web content, it uses a proprietary remote browser graphics language to present the web page exterior without untrustworthy web data. During the user session, the sandboxes receive user events from the endpoint and continuously update the graphic language data responding to web page visual changes.

Puffin Remote Browser can handle different 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, etc. Standard web resources are processed in a sandbox environment with our proprietary remote browser engine derived from Blink. Flash contents are handled in a different sandbox with Flash Player and our proprietary remote PPAPI implementation.

Web threats reside not only in the 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, including DropBox, GDrive, and OneDrive, to isolate download files from endpoints by directly transferring them into the user's cloud storage space. Users can view or edit downloaded documents and files in cloud storage without physically storing documents in the local device. Puffin Remote Browser also can integrate with 3rd-party virus scanning services to verify downloading files on-the-cloud first. Besides download isolation and download scanning, Puffin Remote Browser also has a document preview feature that can convert DOC, PPT, XLS, and PDF documents into a read-only web page to avoid unnecessary file downloads.

Puffin Remote Browser is an isolation layer for endpoints web security and a simple, efficient, and comprehensive browser management layer for the enterprise. Puffin Remote Browser Enterprise Edition provides an admin interface for monitoring service status, auditing user access log, and enforcing enterprise web security policies including web filtering, clipboard operation, file uploading, file downloading, virus scanning, document previewing, etc. Enterprises can leverage Puffin Remote Browser to 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 Remote Browser Server and Puffin Cloud Isolation. It uses hierarchical layers and vector-based drawing commands to represent the web page's appearance.

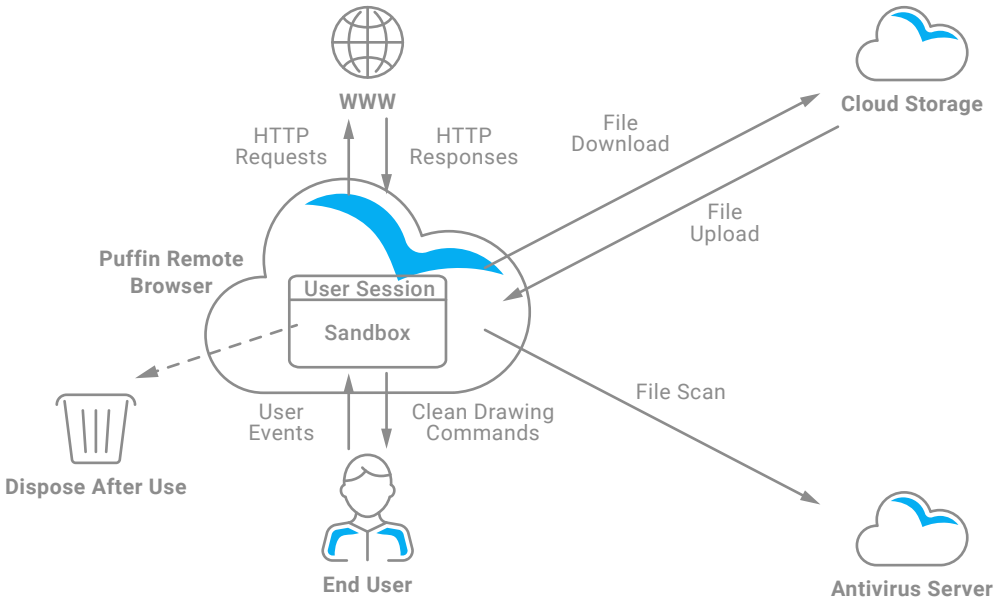

Figure 2: Puffin Remote Browser Platform

The generic web contents, including text and images, are defined by content layers with the vector-based drawing commands in Remote Browser Graphics Language. Special web elements like video stream, Flash content, HTML canvas, and WebGL canvas are defined in separated layers. Remote Browser Graphics Language is designed to represent dynamic web content efficiently. Remote Browser Server doesn't need to send the whole render data on web page changes. 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, the Remote Browser Graphics Language provides exceptional visual quality and uses fewer data to render remote web pages. The vector-based drawing commands preserve original text and graphics quality and adapt to various endpoint screen dimensions and resolutions. The heterogeneous layers optimize content streaming based on the layers' 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 so that no browser exploits can apply. Remote Browser Graphics Language is a comprehensive, efficient, and secure format to present web content after web isolation.

Puffin Cloud Isolation

Puffin Cloud Isolation is the web gateway for endpoints to use Puffin Remote Browser Server's web isolation service from web browsers. Puffin Cloud Isolation supports the latest Google Chrome and Microsoft Edge currently, Safari and Firefox support to be added later.

Puffin Cloud Isolation provides a native user experience on isolated web pages. It supports most web browser functionality, including 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 service. 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 service and use the Puffin Cloud Isolation public service on the i.puffin.com from current web browsers. The 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 save any user credentials, website cookies, and local storage data on the web browser in the 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 on this extension. The extension also can enforce browsers to open new tabs in web isolation automatically.

Puffin Cloud Isolation can be installed in a private cloud or on-premises, too. Enterprises or organizations can deploy a complete Puffin Cloud Isolation and Puffin Remote Browser solution inside their network and integrate its web isolation function 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 Gateway is to deploy Puffin Cloud Isolation between Internet and SWG. Puffin Cloud Isolation is the first tier defender for 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. Enterprise can dynamically create Puffin Cloud Isolation server nodes and adjust Puffin Cloud Isolation cluster size as necessary.

Conclusion

The zero-day exploit is one of the most severe threats to cybersecurity and traditional web security technologies can not protect web browsers from it. Only the emerging remote browser isolation can stop zero-day attacks permanently. This technology isolates all web contents outside, making any web threats unable to reach the endpoints, guaranteeing a secure web environment for its users.

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 page quality at greater 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 scale.

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