Menlo Security

NEXT-GEN SECURE WEB GATEWAY URL-FILTERING

ACCEPTABLE USAGE POLICY WITH ISOLATION

It's no secret that business today is conducted over the internet. Yet, the internet is fraught with malicious content from fake login portals to malware-infected sites that look legit and are designed to trick users into providing access to corporate systems. Legacy Secure Web Gateway solutions give enterprises the ability to allow or block internet content based on policies, but how do you know what to block and what to allow? Evidently, you can't block all internet access. Nor can you simply allow unfettered access. The answer? Adopt a Block and Isolate AUP with Menlo Security Isolation Secure Web Gateway.

Existing Solutions Not Keeping Pace with the Dynamic Internet

Traditional Secure Web Gateways solutions do not have the capacity to evolve quickly enough to protect users from advanced web-based attacks. These detect and resolve solutions too often rely on out-of-date, inaccurate risk data from threat intelligence databases or use behavior monitoring on websites to detect anomalies. The problem with the latter approach is that the changing nature of the internet makes it virtually impossible to monitor everything, especially dynamic and active content--which makes up the majority of the most commonly-visited sites today.

The result is that web-based attacks are far too common and too successful. Clearly, a new approach is needed.

Menlo Security Next-Gen Secure Web Gateway - Web Isolation

Rather than determining what web content is legitimate, organizations should just assume that all web content is risky and hosts potentially malicious content. The resulting zero trust approach eliminates the need to make an allow or block determination based on coarse categorization. An Isolate or Block policy is needed instead. Menlo Security enables this approach by intercepting all web browsing sessions so acceptable use policies can be applied to each session.

USE CASE

Today's Threat Landscape

1. The internet is constantly evolving with old sites coming down and new sites being spun up every day.
2. This constant evolution makes it impossible to keep blacklists and whitelists up to date and accurate.
3. Needing the internet to do their jobs, users are falling prey to phishing, social media attacks, credential theft, and other advanced web malware threats.

USE CASES

What You Can Accomplish with Menlo Security AUP

1. Safely and confidently allow users unrestricted access to unknown/uncategorized websites without impacting productivity or risking malware attacks by implementing an "Isolate" instead of "allow" web filtering policy

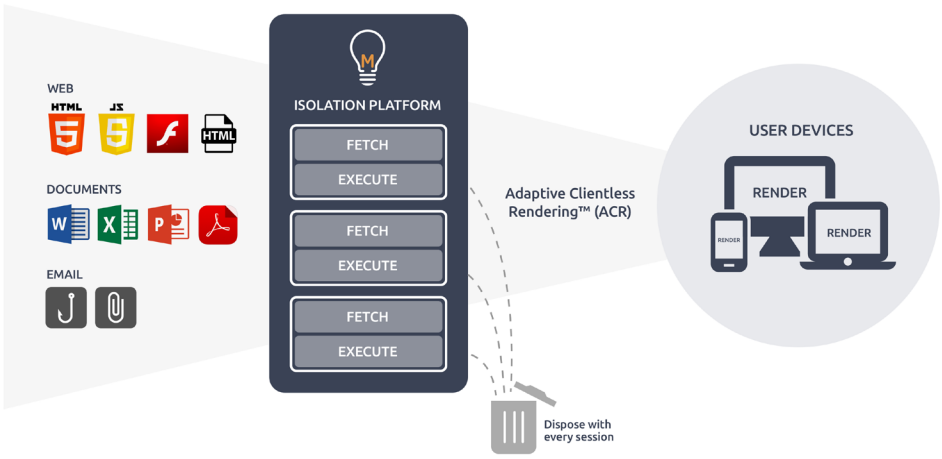
2. Allow granular access to all documents on the web without worrying about malware being downloaded on the user's machine

3. Enforce a set of rules and regulations by blocking access to inappropriate or offensive content on the web using categorization

4. Prevent users from entering credentials or exposing personally identifiable information (PII) on suspicious webforms by making the site read-only

5. Granularly monitor user access to websites and documents on the Internet

NEXT-GEN SECURE WEB GATEWAY URL-FILTERING
ACCEPTABLE USAGE POLICY WITH ISOLATION



With Menlo AUP, all web content is fetched and executed in the Menlo Security Cloud instead of on users' browsers. It is here that acceptable use policies can be enforced, authorizing or blocking web interactions at a granular level.

For content that is allowed, Menlo Adaptive Client Rendering (ACR) efficiently delivers authorized content to the end user's browser with no impact on user experience or productivity nor special client software/plug-ins.

This restores 100 percent confidence in security posture for security teams and worry-free and productive clicking, downloading and browsing experience for end users.

Menlo Security AUP allows organizations to implement a comprehensive and powerful acceptable use policy for web browsing that is completely configurable. This provides powerful protection from web-born threats and attacks like malware, phishing, credential theft and data loss.

Menlo Security - AUP Key Features and Benefits

Acceptable Use Policies (AUP)

Web usage policy enforcement

- Allows unacceptable content to be blocked through URL categorization and filtering based on exceptions and threats
- Ensures adherence to web browsing rules and regulations using granular policies like isolate/allow/block/isolate + read-only
- Detects and prevents access to risky, uncategorized, typosquatting sites
- Blocks access to non-certified versions of browsers

User or role based privileges

- Allows granular specification of both allowed and blocked content based on role

Read-only mode

- Prevents credential theft and data loss of PII
- Prevents posting sensitive information on social sites

Optional "safe", read-only or original downloads

- "Safe" downloads remove and execute any dynamic content, such as JavaScript, within the isolation platform, ensuring safe documents are used inin Adobe Acrobat client
- Read-only documents can be viewed for complete isolation
- Original downloads may be required, and are offered as an authorized option, on a per user basis
- Blocks uploads for isolated sites

HTTPS traffic insight

- Provides better insight into and control of HTTPS traffic coming into your network

HTTPS document rendering

- Protects the user and their endpoint device from encrypted documents harboring malware

Flexibility of deployment options

The Menlo Security Isolation Platform (MSIP) can be deployed in a variety of different customer environments.

Cloud Service

Deploying Menlo Security as a cloud service reduces infrastructure management requirements and ensures service availability and platform upgrades.

MSIP is hosted on an industry leading public cloud, high-availability platform with a global footprint, geo-redundancy and "least latency" based routing.

A web-based administration console provides granular control over configuration features, security policies and access rule settings. Traffic analysis, reporting and logs are available through the administration portal as well and can also be downloaded via an API.

Enable protection no matter where you do business

Menlo Security's Global Elastic Cloud provides high-availability, auto-scaling and bandwidth management that is completely transparent to the user with fixed pricing irrespective of bandwidth or CPU utilization.

Rather than let the platform's performance be tied to a Service Level Agreement (SLA) from a public cloud provider, Menlo measures the platform's reliability and uptime against those of Cloud Service Providers. With more than 20 ISO27001 and SOC2-certified data centers worldwide, Menlo achieves 99.995% global availability with transparent and automatic failover between data centers--making it possible to fully protect your users no matter where they do business around the world.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents and email.

Menlo Security's cloud-based and on-premise Isolation platform scales to provide comprehensive web, email and document protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience.

Menlo Security is trusted by major global businesses, governments and verticals, including Fortune 500 companies and financial services institutions, and backed by leading venture capital firms and banks.

Menlo Security is headquartered in Palo Alto, California.

To learn more, visit **menlosecurity.com** or contact **sales@menlosecurity.com**