Menlo Security

MENLO SECURITY NEXT-GEN SECURE WEB GATEWAY

SECURE WEB TRAFFIC AND ELIMINATE MALWARE

Growing Sophistication and Volume of Threats in a Dynamic Internet

Now, more than ever, today's business is conducted on the internet especially with increasing adoption of mobile and cloud. However, the internet is fraught with malicious content from fake login portals to malware-infected sites that look legitimate. Virtually any website, link or web advertisement can be used to deliver malware today, launching an attack on a user's endpoint device that quickly spreads throughout your organization, infecting any device it can reach.

However, opening access to everything on the web or limiting access to the internet is both counterproductive and stretches an already overburdened IT support team. There is no simple way for security professionals to differentiate safe content from malicious content--putting the organization at risk while inhibiting the productivity of users.

Existing Solutions Not Keeping Pace with Cyber Threats

Traditional Secure Web Gateway (SWG) solutions give enterprise's the ability to allow or block internet content based on policies but how do you know what to block and what to allow? In addition, legacy SWG's are based on detect and respond approach to security identifying only known threats and are not able to keep up with increasingly sophisticated cyberattacks. They rely on inaccurate risk data or signatures from threat intelligence databases or use behavior monitoring to detect anomalies resulting in false positives and negatives and delayed detection. Dynamic and active content--which makes up the majority of commonly-visited sites today make it impossible to keep up.

Additionally, protecting the enterprise from today's cybersecurity threats requires deep insights and context into threats and vulnerabilities as well as user web and email behavior. Security analysts and threat detection and response teams need to know exactly what users were doing at the moment an attack occurs. However, visibility into user behavior is difficult to come by if it exists at all.

The existing approach to web security and malware prevention results in tools sprawl and overburdened security teams and is ineffective and expensive. Web-based attacks are far too common and successful. Clearly, a new approach to security is needed.

The answer? Menlo Security's Next-Gen Secure Web Gateway that allows you to block specific and isolate all other websites ensuring complete protection for web browsing.

Today's Threat Landscape and Dynamic Internet

1. The Internet is constantly evolving making it impossible to keep blacklists and whitelists updated while website reputation history is limited and inaccurate
2. Users are falling prey to phishing, social media attacks, credential theft, and other advanced web malware attacks.
3. Safe, legitimate websites can be hijacked with malware
4. Legitimate looking URLs are really spoofed

USE CASES

1. Protect users from all malware hosted on hijacked websites
2. Prevent users from entering credentials or exposing personally identifiable information (PII) on suspicious webforms by making risky sites read-only and restricting uploads to prevent data loss
3. Enforce a web access policy using a set of rules and regulations by limiting and blocking access to inappropriate or offensive content on the web
4. Monitor user access to websites and documents on the Internet and generate detailed reports that gives insights into threats, vulnerabilities and web activity for improved security investigations, remediation and compliance
5. Isolate ALL websites for all users without compromising security, productivity or performance

Next-Gen Secure Web Gateway features and Benefits

Advanced Threat Protection with web isolation

- Web and document Isolation
- Eliminate all malware, ransomware and emerging zero-day threats from web traffic and documents
- Eliminate false positives and false negative alerts eliminating website re-categorization and re-imaging of endpoints

URL Filtering and Acceptable Use Policy (AUP)

- Enable, isolate, block and restrict access to the web using categorization and exception based policies
- Control employee web browsing via granular policies (user, group, IP …)
- Document access controls including view only, safe or original downloads specified with granular policies based on file type
- Limit user interaction for specific categories of websites

Content and Malware Analysis

- Integrated file analysis using file hash check, antivirus, and sandboxing
- Integration with existing 3rd party AV and sandboxing solutions
- Inspect risky content and detect malicious behavior of all original documents downloaded

Logging, Analytics and Reporting

- Gain visibility and insights into users browsing behavior and threat activity including threats mitigated
- Built-in and custom reports and alerts
- Detailed event logs and built-in traffic analysis
- Built-in and custom queries for flexible exploration and analysis of data
- Configurable data retention period for compliance
- Export log data using API to 3rd party SIEM's and BI tools
- Accelerate threat detection, IR and forensic operations for security teams.

User/Group Policy and Authentication

- Fine-tune policies for specific users or groups
- Integrates with SSO and IAM solutions with SAML support
- Integrates with Active Directory Federation services (ADFS)

Encrypted Traffic Management

- Intercept and inspect TLS/SSL encrypted web browsing traffic
- Provisionable SSL inspection exemptions ensuring privacy for certain categories of websites
- Expose hidden threats in encrypted sessions

Data Loss Prevention (DLP)

- Render websites in read-only mode
- Ability to block file uploads
- Integration with 3rd party DLP (both on-premise on cloud based) maintains optimal visibility
- Limit user interaction on risky or specific categories of websites like social sites
- Prevent data loss and credential theft

Cloud Access Security Broker (CASB)

- Deep visibility and control of Cloud and SaaS application traffic to protect information and ensure compliance
- Integration with 3rd party CASB solutions (both on-premise and cloud-based)

MENLO SECURITY NEXT-GEN SECURE WEB GATEWAY

SECURE WEB TRAFFIC AND ELIMINATE MALWARE

Menlo Security

Web and Document Isolation features and Benefits

Web Isolation and ATP

- Safe viewing of websites by executing all active and risky web content (ie. JavaScript and Flash)
- All native web content is discarded in disposable containers using stateless web sessions
- Adaptive clientless Rendering (ACR) optimally renders safe content on endpoint
- Native and seamless user experience

Document Isolation / Access Control

- Safe viewing of documents by executing all active or risky active content in the cloud away from the endpoint
- Option to download safe cleaned or original versions of documents
- Broad file type support
- Granular policies to limit document access based on file type and user
- Restrict document upload to the Internet

Cloud Delivery and Endpoint Support features and Benefits

Connection Methods and Endpoint Support

- Proxy Automatic Configuration (PAC) automatically configured on endpoints
- Proxy chaining from existing proxy device and IPSEC VPN
- Works with native browsers with broad browser support
- Supports all OS and devices types
- No endpoint software or browser plug-ins

Cloud Delivery with Universal Access

- Global Elastic Cloud with autoscaling and least-latency based routings
- ISO27001and SOC2 certified data centers
- High Availability and Service Level Agreements
- Allows connectivity from any location
- Secure and optimal web access for remote sites and mobile users

Menlo Key Differentiators

Web Isolation Technology

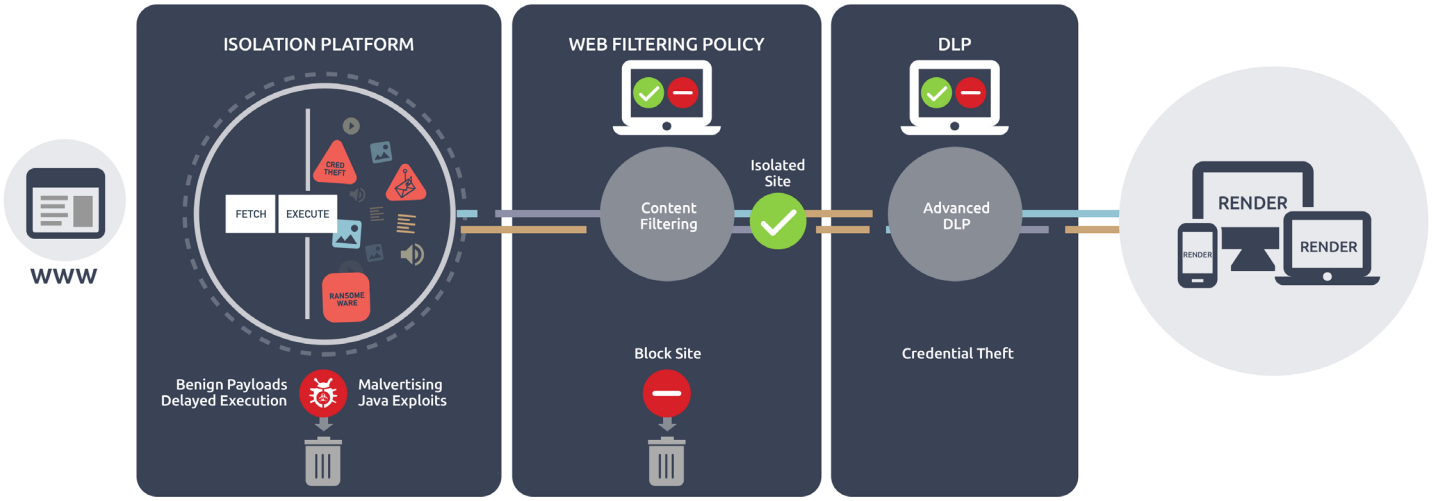
- Industry leading web isolation technology with no impact on user experience or productivity and no need for endpoint software
- Protects users and endpoints from all active and malicious content
- Optimal usage of endpoint and network resources
- Recognized as a Visionary in the 2018 Gartner Magic Quadrant for Secure Web Gateways

Global Elastic Cloud

- High performance and low latency cloud service
- Scales to 1000's of users in 'Isolate All' deployments
- Security Hardened platform

Advanced Threat Protection

- 100% protection against all web and document borne threats including zero-day malware
- Assumes all content is risky
- No endpoint or user infections



Menlo Security Next-Gen Secure Web Gateway with 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. This approach eliminates the need to make an allow or block determination based on coarse categorization and detailed analysis. Customers should employ an Isolate or Block policy instead. Menlo Security enables this approach by intercepting all web browsing sessions preventing malicious content from reaching endpoints and enforcing acceptable use policies and data loss prevention for each session in the cloud.

Our Next-Gen Secure Web Gateway uses state-of-the-art web isolation technology, protecting organizations from cyber attacks by eliminating the threat of malware and phishing attacks from the web and email. The Menlo Security Next-Gen Secure Web Gateway isolates all active content in the cloud, enabling users to safely interact with websites, links and documents online without compromising security.

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.

The Menlo Security Next-Gen Secure Web Gateway is delivered from a global elastic cloud as a service, protects enterprises from web based cyber threats, enforces granular access and security policies, controls, monitors and protects web traffic, prevents data leaks and credential theft, secures cloud apps and ensures compliance across all devices and locations. It does this with unmatched performance and scale.

The Menlo Security solution provides powerful protection from web-born threats and attacks like malware and data loss. The best part is that the user's web browsing experience is not impacted at all, giving them unrestricted yet safe and transparent access to all web content.

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 next-generation 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. Recognized as a visionary in the Gartner Magic Quadrant for Secure Web Gateways, Menlo Security is a leader in web security innovation.

Menlo Security is headquartered in Palo Alto, California.
To learn more, visit **menlosecurity.com** or contact **sales@menlosecurity.com**