How Menlo Security supports the National Cybersecurity Authority (NCA) framework for the Kingdom of Saudi Arabia

This document provides a summary of how the Menlo Secure Enterprise Browser solution helps organizations improve their security posture and reach NCA compliance with the latest NCA recommended security strategies.

Secure Cloud Browsing for any enterprise

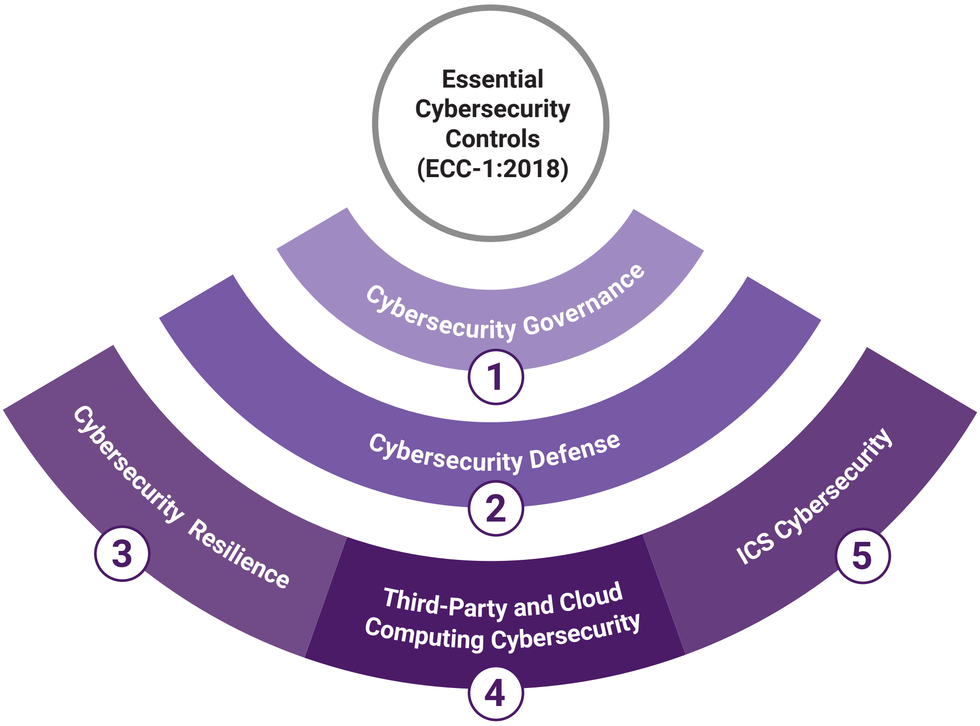
Browsers have become the application enterprises can't live without, but remain a security blind spot. They operate without the necessary protections from cyber threats, exposing users to attacks. The Menlo Secure Enterprise Browser solution helps enterprises better manage browsers, protect their users, and secure application access and enterprise data. Menlo Security provides a secure browsing experience from any browser while preserving user choice and providing a familiar, easy-to-use experience.

To ensure a secure cloud browsing experience, The National Cybersecurity Authority (NCA) of KSA has developed essential cybersecurity controls (ECC) to help organizations meet compliance and minimize the cybersecurity risks that originate from internal and external threats. The NCA strongly encourages all government and private organizations in the Kingdom to leverage these controls to implement best practices to improve and enhance their cybersecurity. The ECC consists of the following:

5 Core Cybersecurity Main Domains

29 Cybersecurity Subdomains

114 Cybersecurity Controls



When considering the NCA framework, Menlo Security directly supports Cybersecurity Defense, specifically preventing evasive phishing and malware threats and limiting the extent of cyber security incidents. For the purpose of this summary, we will discuss how Menlo is compliant with the NCA framework in the core Cybersecurity Domain, Cybersecurity defense and its subcomponents.

Essential Cybersecurity Controls(ECC):

✓ 1. Email Protection

Objective

To ensure the protection of an organization's email service from cyber risks.

Menlo Security benefits

Menlo Security executes all documents from email and the web in a hardened digital twin browser in the cloud. Office documents can be viewed inside our Secure Document and Archive viewer, and a SafePDF copy may also be generated which has all active content and macros removed. No macros would be able to run on user devices if viewed via our isolated container or SafePDF.

Description	How Menlo Security addresses strategy
Must include the following: • Analyzing and filtering email messages (specifically phishing emails and spam) using advanced and up-to-date email protection techniques. • Multi-factor authentication for remote and webmail access to email service. • Email archiving and backup. • Secure management and protection against Advanced Persistent Threats (APT), which normally utilize zero-day viruses and malware. • Validation of the organization's email service domains (e.g., using Sender Policy Framework (SPF)).	Menlo Email Isolation technology assumes all web content and email attachments are potentially malicious, adopting a Zero Trust approach that isolates all web traffic and renders high-risk content in read-only mode. The Menlo Secure Cloud Browser prevents any malicious content from reaching users' devices, ensuring that only safe content is delivered through the Secure Cloud Browser. Menlo integrates seamlessly with existing mail servers like Exchange, Office 365, and Gmail, preserving the native user experience without disrupting workflows. This allows users to click without worry and open anything without the potential risk of phishing or malware. The Menlo Secure Cloud Browser integrates with leading Identity Providers (IDPs) to provide secure access to web and email applications. The Menlo Secure Enterprise Browser solution provides advanced threat prevention for zero-hour phishing, evasive ransomware, and web exploits. By executing all web requests and email attachements inside the Secure Cloud Browser, Menlo Email Isolation technology provides provides a layered approach to security delivering only clean, sanitized content down to the endpoint. While Menlo Security does not provide direct validation of email service domains using SPF, DKIM, or DMARC, its solutions can complement other security tools that handle email authentication, forming part of a broader, integrated security strategy for organizations and protecting users from fileless attacks, APTs, and zero-day exploits.

2. Networks Security Management

Objective

Patch applications (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with ‘extreme risk’ security vulnerabilities within 48 hours. Use the latest version of applications.

Menlo Security benefits

The Secure Cloud Browser runs within an elastic and orchestrated cloud-native platform, fetching content and delivering safe, decomposed and reconstructed, content to a local browser. This enables the Secure Cloud Browser to scale globally and deliver a risk-free local-browsing experience for every user, every tab, and every web session within and across your enterprise.

Description	How Menlo Security addresses strategy
Must include the following: • Logical or physical segregation and segmentation of network segments using firewalls and defense-in-depth principles • Network segregation between production, test and development environments • Secure browsing and Internet connectivity including restrictions on the use of file storage/sharing and remote access websites, and protection against suspicious websites. • Wireless network protection using strong authentication and encryption techniques. A comprehensive risk assessment and management exercise must be conducted to assess and manage the cyber risks prior to connecting any wireless networks to the organization’s internal network. • Management and restrictions on network services, protocols and ports. • Intrusion Prevention Systems (IPS). • Security of Domain Name Service (DNS). • Secure management and protection of Internet browsing channel against Advanced Persistent Threats (APT), which normally utilize zero-day viruses and malware.	The Menlo Secure Enterprise Browser solution ensures network security through logical and physical segregation, using firewalls and defense-in-depth principles to separate network segments, including production, test, and development environments. It provides secure browsing by isolating internet traffic inside the Secure Cloud Browser and restricting access to file storage/sharing and remote access websites, while protecting against suspicious sites. By analyzing browser sessions away from the endpoint, Menlo prevents zero day exploits and highly evasive threats because we analyze data and information in the Secure Cloud Browser. This allows us to use advanced AI techniques, cloud content inspection capabilities, and secure document and archive viewers to identify and block unknown phishing attacks or evasive malware. By rendering the web page in the Secure Cloud Browser, Menlo is able to see exactly what’s happening on the webpage and prevent malicious, dynamic content or payloads, such as javascript or smuggled code, from executing locally on the endpoint. Using Menlo Computer Vision, a leading object detection model, the Menlo Secure Cloud Browser can identify and locate images and identify logos within web content making it possible to identify evasive techniques. Menlo Computer Vision is able to perform logo detection in real-time with high accuracy and then adds the classification from this layered model to the larger Menlo Cloud platform, which makes decisions about how to protect users. The Menlo Secure Cloud Document and Archive Viewer and Archive Viewer enables users to safely view password protected files without ever downloading them to the endpoint. This enables security teams to block evasive techniques used to evade traditional content inspection and close the window of exposure from zero-day exploits. Menlo Security addresses the protection of wireless networks by focusing on securing web and cloud interactions, enforcing strong authentication through integration with IAM systems, and ensuring that data is encrypted during transmission. While Menlo Security does not directly manage wireless network security, it plays a critical role in supporting a broader security strategy that includes strong authentication, encryption, and risk management for wireless networks. By doing so, Menlo also manages network services, protocols, and ports, employs Intrusion Prevention Systems (IPS), secures DNS, and safeguards browsing channels against Advanced Persistent Threats (APT), including zero-day viruses and malware.

3 Mobile Device Security

Objective

To ensure the protection of mobile devices (including laptops, smartphones, tablets) from cyber risks and to ensure the secure handling of the organization's information (including sensitive information) while utilizing Bring Your Own Device (BYOD) policy.

Menlo Security benefits

The Menlo approach enables you to adopt browser security measures, not only on your managed endpoints, but also untrusted endpoints. Continuously access and enforce zero trust access policy for contractors and BYOD users while defending against threats and protecting data down to the last mile.

Description	How Menlo Security addresses strategy
Must include the following: • Separation and encryption of organization's data and information stored on mobile devices and BYODs • Controlled and restricted use based on job requirements • Secure wiping of organization's data and information stored on mobile devices and BYOD in cases of device loss, theft or after termination/separation from the organization • Security awareness for mobile device users	The Menlo Security approach secures data and information in the context of mobile devices and Bring Your Own Device (BYOD) environments by using its cloud-based isolation technology rather than directly storing or managing data on the devices themselves. This enables security teams to adopt browser security measures, not only to managed endpoints, but also to untrusted endpoints for contract workers and BYOD users to help mitigate risk. It enforces controlled and restricted use of data based on job requirements, limiting access to necessary resources only. In cases of device loss, theft, or employee termination, it supports secure wiping of organizational data from mobile devices and BYODs. While Menlo Security focuses on isolating content away from the endpoint rather than encrypting data on the device, any communication between the device and the Menlo Secure Cloud Browser is encrypted. This ensures that data in transit is protected from interception or eavesdropping. The Menlo Secure Cloud Browser stands between any endpoint device and Internet web sites as well as enterprise applications. Users accessing applications inside your own corporate data centers or cloud deployments are protected. And the applications you operate get protected, too. Menlo Browsing Forensics also provides a comprehensive record of browser sessions and user interactions within web sessions so analysts can understand what happened or trace a data leak without delay. While Menlo Security itself does not directly offer security awareness training specifically for mobile device users, it supports security awareness through its policies, integrations, and educational resources. Organizations using Menlo Security's platform can implement these resources as part of a broader security strategy that includes training and awareness programs for mobile device users.

4. Data and Information Protection

Objective

To ensure the confidentiality, integrity and availability of organization’s data and information as per organizational policies and procedures, and related laws and regulations.

Menlo Security benefits

Menlo Security provides a wide range of data-security controls ranging from web security controls to data-security measures, such as copy and paste, upload download controls, read only policy, watermarking, data redaction and data masking to the endpoint.

Description	How Menlo Security addresses strategy
Must include the following: • Data and information ownership • Data and information classification and labeling mechanisms • Data and information privacy	Menlo Security addresses data and information ownership by ensuring that organizations maintain full control over their data while leveraging the Menlo Secure Enterprise Browser solution to protect that data from external threats. Through secure access controls, policy enforcement, and transparency, Menlo Security helps organizations protect their data while retaining full ownership and control. It supports data classification and labeling mechanisms by allowing organizations to enforce policies that categorize and protect sensitive information. Additionally, the browser enhances data privacy by rendering all web content in the Menlo Secure Cloud Browser, ensuring that user data and browsing activity remain private and protected from potential threats. By executing all content inside the Secure Cloud Browser, policies can be applied based on user, group, file type, website category, or cloud application to determine when content is blocked, rendered in read-only mode, or accessible in its original form. The Secure Cloud Browser provides a wide range of data-security controls ranging from web security controls to data-security measures, such as: • Copy and paste • Upload/download controls • Read only policy • Watermarking • Data redaction • Data masking to the endpoint In addition, Menlo Secure Application Access provides further access controls, enabling least-privileged access on a resource by resource basis to support data protection and information leakage. Menlo Browsing Forensics helps responders to understand a user’s activity within a browser by preserving a comprehensive record of web sessions and user interactions so analysts can understand what happened or trace a data leak without delay.

5 Web Application Security

Objective

To ensure the protection of external web applications against cyber risks.

Menlo Security benefits

Menlo Secure Application Access gives remote users secure connectivity to private applications, including web applications and legacy applications. In addition to providing simple-to-deploy, clientless ZTNA, Secure Application Access and the Menlo Secure Cloud Browser protect applications from Internet threats and provide granular controls for added protection of the application and associated data.

Description	How Menlo Security addresses strategy
Must include the following: • Use of web application firewall • Adoption of multi-tier architecture principal • Use of secure protocols • Clarification of secure usage policy for users • Multi-factor authentication for users' access	Menlo Secure Application Access capabilities further cement enterprise defenses by extending secure access to SaaS and private applications without exposing them to threats. The Menlo Secure Cloud Browser together with Menlo Secure Application Access have gone beyond identity verification, to provide a zero trust solution that works everywhere, for managed and unmanaged devices. Menlo Secure Application Access enables least-privileged access to both private and SaaS applications on a resource-by-resource basis, ensuring data security and information leakage protection. It provides secure intranet access for contractors and supports native RDP or SSH clients while keeping private applications hidden from the public Internet, protecting against threats like DDoS and code injection. Access is granted only to necessary applications for a user's job function, based on zero trust principles, allowing for granular and conditional policies. Additionally, it includes endpoint posture checks for non-browser-based access and uses the Menlo Secure Cloud Browser to safeguard applications from evasive threats and infected endpoints. By integrating with leading Identity Providers (IDPs), Menlo provides seamless access for a native user experience, enhanced security against evasive threats, centralized management for security teams and helps meet regulatory NCA compliance requirements.

Preventing evasive threats before they reach the endpoint

Menlo Security demonstrates compliance with the NCA through several key aspects of its cybersecurity solutions and practices:

1. **Alignment with NCA framework principles:** The NCA outlines key principles and guidelines for cybersecurity practices, such as risk management, incident response, and regulatory compliance. Menlo Security aligns with these principles by offering a comprehensive security solution that addresses multiple aspects of cybersecurity threat prevention.

2. **Advanced threat detection and prevention:** Menlo Security incorporates advanced threat detection and prevention capabilities, including real-time analysis of web traffic and proactive protection against evasive cyber threats. These capabilities are crucial for safeguarding critical infrastructure and sensitive information as per the NCA guidelines.

3. **Superior scalability with native user experience:** The Menlo Secure Enterprise Browser solution scales seamlessly across any size organization, with zero impact on end user performance regardless of user count or number of browsing sessions. Menlo Security supports automated workflows and provides customizable reporting, ensuring that it dynamically adapts to customer needs. This flexibility extends to deployment options, including cloud, hybrid, and on-premises models, allowing organizations to choose the setup that best aligns with their existing infrastructure and business requirements.

Conclusion

The Menlo Secure Enterprise Browser solution protects your users, and secures access to applications and associated enterprise data, providing a complete enterprise browser solution. Menlo Security secures existing browsers while preserving the ability for users to keep the browsers they're familiar with. You can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. This helps meet NCA compliance, and in doing so, helps organizations on their Essential Cybersecurity Controls journey. Secure your digital transformation with trusted and proven cyber defenses, on any browser, with Menlo Security.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling Zero Trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.