Yakima Valley Farm Workers Clinic

we are family

REQUEST FOR PROPOSAL

Secure Access Service Edge (SASE)

07/09/2025

RFP Response Contact
ISRFP@yvfwc.org
Attn: Jeremy Staab
IS Security Manager, IT Dept.

Document History

Revision	Date	Description of Change	Author / Editor
1.0	10/01/2024	Initial Draft	Jeremy Staab, Nicholas Bierman, & John Bronk
2.0	11/01/2024	Second Draft	Jeremy Staab
3.0	11/15/2024	Third Draft	Jeremy Staab
4.0	06/06/2025	Fourth Draft	Jeremy Staab
5.0	07/02/2025	Fifth Draft	Jeremy Staab

Table of Contents

1 Solicitation Introduction

Yakima Valley Farm Workers Clinic (YVFWC) is issuing this Request for Proposal (RFP) for Vendors to submit proposals for implementation of a new Secure Access Service Edge (SASE). The following document provides instructions on the preparations of a proposal that will enable you to address the business, technical, financial, security, and legal requirements in this bid.

1.1 General Information

The Yakima Valley Farm Workers Clinic (YVFWC) is seeking a robust, multi-functional Secure Access Service Edge (SASE) solution to serve as the foundation of its network and security infrastructure. This solution must integrate key capabilities such as Wide Area Networking (WAN), Dedicated Internet Access (DIA), commodity internet, VPN, and cloud application access to support the organization's evolving connectivity and security needs.

A core requirement is the deployment of Software-Defined WAN (SD-WAN) with Firewall as a Service (FWaaS) across 45 locations, supporting 5,000 endpoints, 2,500 staff, and 200–400 remote VPN users. The solution must also include Data Loss Prevention (DLP), a Secure Web Gateway (SWG), and a Cloud Access Security Broker (CASB) to ensure secure, seamless access to applications and resources regardless of location.

To meet the highest security standards, the solution must implement Zero Trust Network Access (ZTNA), enforcing identity- and context-based access to all network and cloud resources. The architecture should be cloud-native, identity-driven, and globally scalable to support secure access at all network edges.

YVFWC's Information Services Department includes 87 team members supporting approximately 2,800 users across nearly 50 sites in Washington and Oregon. The organization operates 12 vendor site-to-site VPNs terminating in Azure, supports 250 concurrent VPN users, and manages four datacenters (two physical, Azure, and DRaaS). The environment includes Microsoft 365, various SaaS applications, 3,000+ laptops/desktops, 1,000 iPads, and 175 servers.

The current infrastructure includes Palo Alto Networks Next-Generation Firewalls (NGFWs) (physical and VM series) managed via Panorama, and Meraki MX/MS appliances in a hub-and-spoke SD-WAN overlay. This overlay runs over diverse, multi-carrier internet circuits with primary 1Gbps synchronous and secondary asynchronous coaxial uplinks for redundancy.

While most core applications are cloud-based, some legacy systems remain on-premises. The IS department oversees end-user computing, LAN/WAN, wireless, security, business intelligence, and mission-critical application performance under defined SLAs.

The ideal SASE solution will:

- Simplify IT operations through service convergence (SD-WAN, FWaaS, SWG)
- Enhance user experience while maintaining strict security controls
- Support agile, scalable, and secure infrastructure aligned with healthcare delivery needs

YVFWC seeks a solution that not only meets today's requirements but also provides a flexible, future-ready platform to support its mission of delivering exceptional healthcare services.

1.2 About YVFWC

Originally established as a provider of health care for migrant and seasonal farm workers, the Yakima Valley Farm Workers Clinic (YVFWC) is a not-for-profit 501(c)(3) organization incorporated in 1978.

Today the Yakima Valley Farm Workers Clinic has locations throughout Washington and Oregon providing healthcare to thousands of adults and children each year. Services are provided without regard to an individual's ability to pay. A sliding-fee scale is available for those without health insurance.

The list of services includes medical and dental care, behavioral health and counseling, pharmacy, substance abuse treatment, community health and nutrition and optometry. There are also educational and employment training programs. YVFWC has over 2,500 full time employees and impacts the lives of over 180,000 adults and children each year through our services in Washington and Oregon.

The Mission:

The mission of the Yakima Valley Farm Workers Clinic, its Board of Directors, and its employees, is to improve the quality of life for farm workers, the underserved, and others as we work to strengthen the health of our communities.

We believe in the right to wellness for all in a comprehensive, preventive approach to health. We value cultural diversity and teamwork. We respect the dignity of our clients and employees.

Many of the communities we serve have significant populations of farm workers and low-income families. Services are provided without regard to an individual's ability to pay, and a sliding-fee and nominal-fee scale is available for those without health insurance. More information about YVFWC is available at http://www.yvfwc.com/.

YVFWC will be using the SASE system to help facilitate the mission statement above, and the business goals and objective enumerated in section 4. YVFWC expects vendors to provide an effective system that is both cost effective and whose implementation is compatible with the functional requirements detailed below.

This Request for Proposal is the first step in a process that is designed to select a highly qualified vendor. The full process is outlined below:

1| Letter of Intent: Interested Vendors are invited to submit a brief letter to inform YVFWC of the Vendor's intent to respond to the RFP. A letter of Intent must be submitted in accordance with the schedule laid out in section 2.1.
2| Questions and Answers: Vendors that submit a letter of intent may submit questions in accordance with the schedule described in section 2.1.
3| Written Proposal: Vendors wishing to do so are required to submit a written response to this RFP in accordance with the schedule laid out in section 2.1.
4| Customer Reference Checks: YVFWC may contact Vendor references to understand prospective Vendors from a customer's point of view. All responses should include contact information for a minimum of two reference checks.
5| Vendor Demonstrations: Vendor will be notified and invited to present to YVFWC via remote Video Conferencing technology (i.e., Zoom, Teams, WebEx, etc.)

2 Proposal Timetable

YVFWC intends to follow a specific schedule in performing the proposal evaluation and vendor selection process. The timetable below identifies key dates, which may be changed at YVFWCs discretion.

RFP Event/Deadline	Date
RFP released to Vendors	July 11th, 2025,
Letter of Intent submitted (required for consideration)	July 16th, 2025
Written questions submitted by Vendors	July 23rd, 2025
Written answers returned to Vendors	July 29th, 2025
Written responses submitted (required for consideration)	August 1st, 2025
Vendor presentations	August 11th – Aug 15th, 2025
Vendor Selected	September 1st – 30th, 2025

2.1 Primary Contact (Delivery of Intent, Questions and Proposals)

All correspondence shall be via electronic communication to:

Yakima Valley Farm Workers Clinic
Attn: Jeremy Staab
603 West Fourth Ave.
Toppenish, WA 98948
ISRFP@yvfwc.org

2.2 Confidentiality

All information presented in this RFP, including information disclosed by YVFWC during the proposal process, is considered confidential. As such, all data and information shall be kept strictly confidential and shall not be disclosed to any third party without the express written consent of YVFWC.

2.3 Proposal Costs

All costs associated with preparing proposals in response to this RFP, and for providing any additional information required, or conducting demonstrations, are the sole responsibility of the vendor.

2.4 News Releases and Marketing

Vendors are not permitted to announce involvement in or release any information regarding this RFP.

2.5 Period of Proposed Validity

All vendors' proposals must remain valid for a minimum of six (6) months from the proposal due date.

2.6 Subcontracting

YVFWC must grant permission to subcontract any work to be performed under this RFP and the subcontractor must be identified before approval.

2.7 Disclaimer

No commitment to purchase or license any product either now or in the future is being made or implied by this RFP. YVFWC will solely determine the success or failure of the evaluation process. The project may be terminated at any time without commitment and without cause. Information provided in the RFP may be used as part of the contractual agreement.

3 Solicitation Overview

3.1 Procurement Goals and Business Objectives

The new SASE solution should address several key goals aimed at enhancing both security and network performance. These goals include facilitating secure and efficient access for remote workers, supporting global operations with consistent security and connectivity, and enabling secure direct internet access (DIA) to optimize connectivity to cloud services. Additionally, a SASE solution aims to improve cloud connectivity performance and security, consolidate vendors to simplify management by integrating networking and security functions into a single platform, and embrace a Zero Trust strategy to ensure all users and devices are authenticated and authorized before accessing network resources. Enhancing the overall security posture by applying consistent policies and controls across the network is also a critical goal. These objectives help organizations achieve a more secure, resilient, and efficient network infrastructure, supporting their digital transformation initiatives.

Goals:

- Facilitate Remote Work and Access: Ensure secure and efficient access for remote workers, enabling them to connect to corporate resources from anywhere.
- Support Distributed Operations: Provide consistent security and connectivity for users and applications across different geographical locations on and off network.
- Enable Secure Direct Internet Access (DIA): Optimize internet connectivity by allowing direct access to cloud services without backhauling traffic through a central data center.
- Unified Monitoring and Reporting: Ability to centralize and visualize traffic flows, application-visibility, network issues and latency, security issues and concerns, alerting and other data into a single cloud-management dashboards for all network and security activity across YVFWC's portfolio.
- Optimize Cloud Connectivity and Observability: Improve performance and security for cloud-based applications and services. Help identify shadow IT.
- Consolidate Vendors: Simplify management by reducing the number of vendors and integrating networking and security functions into a single platform.
- Embrace Zero Trust Strategy: Implement a Zero Trust model to ensure that all users and devices are authenticated and authorized before accessing network resources.
- Enhance Security Posture: Strengthen overall security by applying consistent policies and controls across the network.
- Service Quality: Ensure that IT services are reliable, secure, efficient, and meet user expectations.
- Efficiency: Streamline Information Security and Networking processes to reduce waste and improve productivity.
- Simplify Administration / Ease of Use: The SASE solutions should be designed to be user-friendly, especially for administrators, offer centralized management, and facilitate networking and security functions from a single console.

- User Satisfaction: Focus on delivering a better user experience through highly secure and reliable connectivity that has managed and measurable performance.
- Replicate Existing Workflows and Functionality: The SASE solution should fully replicate existing workflows and functionality by seamlessly integrating with current network and security infrastructures, ensuring smooth access to YVFWC resources for users.
- Ensure Performance: Implemented solution provides real-time insights into network activity, traffic flows, security threats, and application performance, allowing administrators to quickly identify and address issues.
- Regulatory Compliance: Ensure that IT services comply with relevant regulations and standards, and that security measures are robust and up to date.
- Response Times: Ensure that the tools operation and performance is not a roadblock or inhibitor to workflow or usage.
- Stability and Market Leadership: Vendor and product have a track record of stability and solid market leadership.

3.2 Evaluation Process & Criteria

YVFWC will use a structured process to evaluate all RFP responses, to select vendor finalists, and ultimately select the vendor of choice. Only bids that fully respond to all requirements outlined in the RFP will be considered. The exact criteria and weights assigned will not be disclosed; however, high-level criteria that will be used in the evaluation are as follows:

- Pricing – Proposed solutions offer high value and meets YVFWCs budgetary needs
- Functionality – Solutions have all necessary components to ensure on-going and future initiatives are successful and allows integration with other products
- Organization – Vendors have experience implementing solutions with organizations similar to YVFWC
- Technical – The vendor's solution appropriately fits with YVFWC's environment and requirements
- Prior Experience – Successful implementation and adoption in similar and relevant organizations
- Vendor Stability – Vendor can demonstrate and be prepared to discuss medium to long range business objectives and plans.
- Training – Training program is comprehensive
- Support – Vendor offers high level of on-going support
- Usability – Software programs are intuitive and time saving

Each Vendor will be evaluated against the same criteria and will be provided a "score" for each category. YVFWC retains complete discretion in deciding which proposals meet the requirements set out in the RFP and what evidence will be considered adequate to indicate compliance with those requirements. Only top Vendors will be invited to conduct product demonstrations.

4 YVFWC-Specific Requirements

4.1 Key Technical Features & Requirements of the SASE Solution for YVFWC

4.1.1 Centralized Management of All SASE Solutions - Requirements:

Centralized, cloud-based management is a pivotal aspect of the comprehensive Secure Access Service Edge (SASE) solutions per this RFP. Responses must demonstrate how various networking and security functions may be managed by a unified, cloud-native service model. This approach simplifies the administration of security policies and network configurations across all users, devices, and applications, enhancing the overall security posture and operational efficiency. By aligning with SASE initiatives, the organization can ensure a cohesive and agile infrastructure that supports the dynamic needs of modern digital environments.

4.1.2 Next-Generation Firewall-as-a-Service (NGFWaaS) Requirements:

- The FWaaS component shall be a Next-Generation Firewall (NGFW) service.
- The Next-Generation Firewall-as-a-Service (NGFWaaS) would be a sophisticated security system that integrates traditional firewall capabilities with additional features to provide comprehensive network protection. Key components of this cloud-based NGFW shall include deep packet inspection, application-level filtering, intrusion prevention / detection systems, advanced URL filtering, DNS security, threat intelligence, and dynamic content updates including External Dynamic Lists (EDLs) of current global threats or allow lists. These elements will work together to inspect network traffic deeply, block malware, and prevent advanced cyber threats, enhancing the security of an organization's network. The NGFWs shall utilize real-time threat intelligence and identity-based security approaches to create granular "allow/deny" rules for applications and web content, offering more dynamic and adaptive security solutions.

4.1.3 Data Loss Prevention (DLP) Requirements

- The proposed Cloud SASE - Data Loss Prevention (DLP) solutions shall include a comprehensive approach to securing data across cloud environments, ensuring that sensitive information is protected from unauthorized access and exposure. This strategy integrates Secure Access Service Edge (SASE) with DLP systems to provide a unified solution that not only identifies and classifies sensitive data but also applies robust protection policies. By leveraging advanced techniques such as data classification, pattern matching, and machine learning, Cloud SASE DLP solutions can accurately detect and safeguard critical data. This solution would enforce compliance with data protection regulations and organizational policies and protect against both internal and external threats.
- Key features of the DLP solution shall include:
    - Monitor and Prevent Data Loss Through Breach: Implement measures to monitor organizational data and systems, detecting and preventing data exfiltration through data breaches, social engineering, malware, and hacking.
    - Prevent Data Exfiltration: Prevent and detect unauthorized and intentional transfer of critical data beyond the organization's perimeter. Block and alert on illicit movement of sensitive information, carried out by third-parties or malicious insiders who have authorized access.

- Classification & Monitoring of Sensitive Data: Support for automated and manual data classification to identify sensitive data and ensure compliance with data security strategies.
- Detect and Block Suspicious Activity: Monitor all data traffic within the network, cloud, and off-premises environments to prevent sensitive data from exiting via email, USB drives, or other channels.
- Improve Visibility and Control: Provide visibility into sensitive data within the organization and helps identify potential unauthorized data transfers, audit for potential issues, and alert on potential issues or policy violations.
- Regulatory Compliance: Comply with data protection standards, laws, and regulations such as HIPAA, the Sarbanes-Oxley (SOX) Act, and the Federal Information Security Management Act (FISMA).

4.1.4 SSL Decryption Requirements

- The proposed SSL Decryption solutions shall include decryption and inspection of SSL/TLS encrypted data, to identify potentially harmful malware and data loss which could be encrypted in these protocols. The SSL decryption solution shall include consideration of legal and ethical implications, alongside the technical aspects regarding the intercepting and inspecting encrypted traffic across the entire portfolio. Including the ability to decrypt SSL traffic to monitor and protect sensitive data.

  Key features of the SSL Decryption solution shall include:

  - Unlimited and Scalable Capacity:
  - Monitor both on-network and off-network SSL traffic from users using a scalable service that adjusts dynamically to handle varying traffic demands.
  - Conduct a thorough assessment of organizational equipment, capacity, bandwidth, and resources to ensure appropriate allocation for a well-sized deployment of comprehensive SSL decryption across the portfolio.
  - Granular Policy Control: Ability to maintain compliance while allowing flexibility to exclude encrypted user traffic from sensitive website categories, such as healthcare or banking.
  - SIEM Integration: Direct / API integration with the organizations Security & Information Management System (SIEM) with Splunk cloud to provide centralized alerting.
  - Centralized Management of All SASE Solutions
  - Centralized, cloud-based management is a pivotal aspect of the comprehensive Secure Access Service Edge (SASE) solutions per this RFP. Responses must demonstrate how various networking and security functions may be managed by a unified, cloud-native service model. This approach simplifies the administration of security policies and network configurations across all users, devices, and applications, enhancing the overall security posture and operational efficiency. By aligning with SASE initiatives, the organization can ensure a cohesive and agile infrastructure that supports the dynamic needs of modern digital environments.

4.1.5 Network, SD-WAN, and Clinic-Level Firewall Requirements

- Integration and Transition
  - The proposed SASE solution must integrate with existing Meraki MX clinic-level firewalls during transition phases or provide an alternative to replace them. The solution should offer security, visibility and context, integrating with the existing Splunk cloud SIEM. It must enrich security

events, handle errors robustly, and comply with regulations (e.g., HIPAA, GDPR). The solution should ensure encrypted data transmission, high performance, and minimal latency, with comprehensive documentation and support.

- Option 1: Support existing Meraki MX firewalls with SD-WAN and FWaaS, ensuring redundant internet connectivity.
- Option 2: Propose and quote an alternative solution to replace Meraki MX firewalls, supporting SD-WAN and FWaaS, and integrating with the SASE solution.
    - Replacement Requirements
        - If proposing the replacement of all Meraki clinic-level firewalls, the new devices must support:
        - L3 Gateway for all VLANs
        - DHCP Services
        - Captive Portal with Customizable Splash Page
        - 30-day records for connected clients, uplink statistics, and traffic analytics
        - Internet Breakout/Direct to Internet Traffic
        - Dual uplink failover
        - Traffic shaping per uplink
        - VLAN management and distribution across sites
        - Local access lists for network segmentation
        - Dynamic Routing (BGP, etc.)
        - SD-WAN with local internet offloading
        - Packet capture on L3 device and connected clients
        - Local device login for setup
        - Device alerts (temperature, DHCP lease pool, PSU status)
        - Network connectivity tools (ping, tracert, nslookup, ARP table, speed test, iPerf, tcpdump)

- SASE Solution Requirements
    - The proposed SASE solution must support SD-WAN with multiple internet connections, integrating advanced security and network management capabilities. It should provide a centralized platform to manage both SD-WAN and security policies, ensuring consistent enforcement across all connections (MPLS, broadband, DIA, LTE). The solution should dynamically route traffic based on real-time performance metrics, optimize bandwidth use, and improve application performance. It must offer detailed visibility into network traffic, cloud application performance, and user activities, enabling better monitoring and quicker response to security incidents. High availability and redundancy must be ensured, maintaining continuous network operations even if one connection

fails.

- Key Network and SD-WAN Features
  - **Redundant Power Supplies**: Ensure high availability with multiple power supplies.
  - **Application-Centric Networking**: Prioritize and route traffic based on application needs.
  - **Centralized Management**: Simplify network administration with a centralized dashboard.
  - **Optimized Connectivity**: Support multiple transport services (MPLS, LTE, DIA, broadband).
  - **Improved Performance**: Reduce latency and enhance bandwidth usage.
  - **Secure Connections**: Encrypt data across the network.
  - **Integrated Security**: Combine SD-WAN with SWG, CASB, FWaaS, and ZTNA.
  - **Cloud-Native Architecture**: Deliver services from the cloud for scalability.
  - **Dynamic Perimeter**: Accommodate remote workers and branch offices.
  - **Simplified Network Management**: Reduce complexity of managing security devices.
  - **Capacity Requirements**: Route, forward, inspect, and encapsulate traffic at 1Gbps (clinics) and 10Gbps (data centers).
  - **Overlay Transport**: Provide secure connectivity over insecure mediums.
  - **Identity-Based Networking**: Map users to IP addresses across the network.
  - **Application/User Experience Reporting**: Report performance metrics beyond simple ICMP RTT.
  - **Custom Application Definition**: Configure custom applications for routing and policy decisions.
  - **Automatic Route Propagation**: Distribute routing information dynamically using BGP and OSPF.
  - **Embedded Packet Capture**: Capture packets for troubleshooting and analysis.
  - **Basic Network Troubleshooting Tools**: View ARP tables, ping/traceroute, and routing/forwarding table lookups.
  - **Detailed Flow Logging**: Log source/destination IP and ingress/egress interface.
  - **Application-Aware QoS/Traffic Shaping**: Configure traffic shaping and prioritization policies.
  - **DHCP Management**: Configure DHCP scopes, options, and reservations.
  - **Policy-Based Routing**: Route traffic based on defined policies.
  - **Local/Clinic Level Firewall**: Perform packet filtering at the clinic level.
  - **Captive Portal/User Authentication**: Grant network access with a captive web portal.
  - **Link Aggregation**: Provide redundant paths to switching infrastructure.
  - **Serial Console Port**: Advanced troubleshooting and recovery.
  - **Support for Copper Interfaces**: 100/1000Mb RJ45 interfaces for LAN and WAN.
  - **Support for 10Gb Interfaces**: 10Gbps RJ45 and SFP+ interfaces for LAN and WAN.

4.1.6 Zero Trust Network Access (ZTNA) - Requirements

- The SASE - Zero Trust Network Access (ZTNA) solution should enforce strong authentication methods like multi-factor authentication (MFA) or certificate-based authentication for role-based access control, and continuous verification of users and devices. Granular access control is essential, utilizing role-based access control (RBAC) and least privilege principles to minimize unauthorized access. Context-aware policies adapt based on user behavior, device health, and location, ensuring dynamic policy enforcement. Network segmentation, including micro-segmentation, isolates network segments to limit lateral movement of threats. Application and data security measures, such

as application-level access controls and data encryption, protect sensitive information. Continuous monitoring and analytics provide real-time insights into user and device behavior, integrating threat intelligence to detect and respond to incidents. A unified management platform centralizes security policy management, monitoring, and reporting, while ensuring scalability for diverse workforces. Additionally, invisibility and minimal access principles, such as concealing applications from public discovery and using a trust broker for connection requests, reduce attack surfaces and enhance security. These components collectively ensure a secure, adaptive, and efficient ZTNA solution, supporting remote and hybrid work environments.

- Key features of the Zero rust Network Access (ZTNA) solution shall include:
  - Strong Authentication:
    - Multi-factor authentication (MFA)
    - Continuous authentication
  - Granular Access Control:
    - Role-based access control (RBAC)
    - Least privilege access.
  - Context-Aware Policies:
    - Adaptive access policies
    - Dynamic policy enforcement
  - Network Segmentation:
    - Micro-segmentation
    - Perimeter controls around individual assets
  - Application and Data Security:
    - Application-level access controls
    - Data Encryption
  - Continuous Monitoring and Analytics:
    - Real-time monitoring of user and device behavior
    - Threat intelligence integration
  - Unified Management:
    - Centralized platform for managing security policies.
    - Scalability for diverse and remote workforces
  - Invisibility and Minimal Access:
    - Concealing applications from public discovery
    - Trust broker for connection requests

4.1.7 Secure Web Gateway (SWG) - Requirements

- The SASE-ZTNA solution should enforce strong authentication methods, such as multi-factor authentication (MFA) and certificate-based authentication, for role-based access control and continuous verification of users and devices. Granular access control is essential, utilizing role-based access control (RBAC) and least privilege principles to minimize unauthorized access. Context-aware policies adapt based on user behavior, device health, and location, ensuring dynamic policy enforcement.

- Network segmentation, including micro-segmentation, isolates network segments to limit lateral movement of threats. Application and data security measures, such as application-level access controls and data encryption, protect sensitive information. Continuous monitoring and analytics provide real-time insights into user and device behavior, integrating threat intelligence to detect and respond to incidents. A unified management platform centralizes security policy management, monitoring, and reporting, while ensuring scalability for diverse workforces.
- Additionally, invisibility and minimal access principles, such as concealing applications from public discovery and using a trust broker for connection requests, reduce attack surfaces and enhance security. These components collectively ensure a secure, adaptive, and efficient ZTNA solution, supporting remote and hybrid work environments.
- Key Features of the ZTNA Solution
    - Strong Authentication: Multi-factor authentication (MFA), continuous authentication.
    - Granular Access Control: Role-based access control (RBAC), least privilege access.
    - Context-Aware Policies: Adaptive access policies, dynamic policy enforcement.
    - Network Segmentation: Micro-segmentation, perimeter controls around individual assets.
    - Application and Data Security: Application-level access controls, data encryption.
    - Continuous Monitoring and Analytics: Real-time monitoring of user and device behavior, threat intelligence integration.
    - Unified Management: Centralized platform for managing security policies, scalability for diverse and remote workforces.
    - Invisibility and Minimal Access: Concealing applications from public discovery, trust broker for connection requests.

4.1.8 Cloud Access Security Broker (CASB) - Requirements

- The proposed SASE solution will include a Cloud Access Security Broker (CASB) to enhance cloud security and management. The CASB must provide comprehensive visibility into all cloud services, including both sanctioned and unsanctioned applications, to identify potential risks. It should offer robust Data Loss Prevention (DLP) capabilities to protect sensitive information from unauthorized access and sharing, and detect and prevent threats such as malware, ransomware, and compromised accounts by analyzing cloud traffic and user behavior.
- The CASB must enforce granular access controls based on user identity, device, location, and other contextual factors to ensure secure access to cloud services. It should help organizations comply with regulatory requirements by enforcing policies that prevent the use of non-compliant cloud services and ensure data protection. Additionally, the CASB should identify and manage the use of unsanctioned cloud applications, providing insights into potential risks and enabling the enforcement of security policies.
- Integration with other SASE components like secure web gateways (SWG), zero trust network access (ZTNA), and firewall as a service (FWaaS) is essential for a unified security posture. The CASB must offer real-time monitoring and analytics to detect and respond to security incidents promptly and be scalable to manage high volumes of cloud traffic without performance degradation, ensuring a seamless user experience.
- Key Features of the CASB Solution
    - Visibility: Comprehensive visibility into all cloud services, including sanctioned and unsanctioned applications.
    - Data Loss Prevention (DLP): Protects sensitive information from unauthorized access and

sharing.
- Threat Detection and Prevention: Detects and prevents threats such as malware, ransomware, and compromised accounts.
- Access Control: Enforces granular access controls based on user identity, device, location, and other contextual factors.
- Compliance: Helps organizations comply with regulatory requirements by enforcing policies that ensure data protection.
- Shadow IT Management: Identifies and manages the use of unsanctioned cloud applications, providing insights into potential risks.
- Integration with Other Security Services: Seamlessly integrates with other SASE components like SWG, ZTNA, and FWaaS.
- Real-Time Monitoring and Analytics: Offers real-time monitoring and analytics to detect and respond to security incidents promptly.
- Scalability and Performance: Scalable to handle high volumes of cloud traffic without performance degradation, ensuring a seamless user experience.

4.1.9 SASE for Remote Users

- Effectively support all end-user / endpoints, securing workflows both on and off the VPN. This integration ensures that users have secure access to corporate resources from any location, enhancing productivity and maintaining security standards. Additionally, SASE provides the flexibility needed for future growth, allowing the organization to scale its network and security infrastructure as needed. This approach not only secures current operations but also prepares the organization for evolving demands and expanding user bases.
- For off VPN remote users, the benefits must include enhanced security through continuous verification of user identity and device health, ensuring that only authorized users can access corporate resources, and protect users through the Secure Web Gateway (SWG). This approach provides seamless access, allowing users to securely connect to applications and data without the need for a traditional VPN, thereby improving user experience and productivity. Additionally, by applying security policies at the edge, threats are mitigated before they reach the corporate network, significantly reducing risk.

4.1.10 SIEM Integration, Monitoring, & Alerting:

- The proposed SASE system must integrate with the organization's Splunk Cloud SIEM, preferably via API, to send logs, alerts, and other security data. The system should enrich security events with contextual information before sending them and include robust error handling and retry mechanisms. The integration must be scalable, secure, and compliant with relevant regulations, ensuring encrypted data transmission and high performance with minimal latency. Comprehensive documentation and technical support should be provided for setup, troubleshooting, and maintenance.
- Key Features
  - Functional Requirements:
    - Data Ingestion: Send logs, alerts, and security data to Splunk Cloud SIEM in real-time.

        - Event Enrichment: Enrich security events with contextual information (e.g., user identity, device details) before sending.
        - Error Handling: Implement robust error handling and retry mechanisms for reliable data transmission.
        - Security: Ensure data transmission is encrypted using industry-standard protocols (e.g., TLS).
    - Performance Requirements:
        - Latency: Minimize data transmission latency for timely detection and response to security incidents.
    - Maintenance and Support:
        - Documentation: Provide comprehensive documentation for API endpoints, data formats, and the integration process.
        - Support: Offer technical support for integration setup, troubleshooting, and maintenance.

4.1.11 Secure Browser Requirements:

- A secure browser is a desired but optional component of this RFP. Vendors who offer a secure browser should quote based on a 3,000-user license count. The secure browser, if available, should prioritize privacy

and security, with the following key features. Vendors who do not offer a secure browser will not be penalized in the evaluation process.

- Key Features
  - Privacy Protection
  - Block third-party trackers
  - Customizable privacy settings
  - Privacy-focused search engines
  - Cookie management
  - Ad and tracker blocking
  - Pop-up blocking
  - Security Features
  - Automatic HTTPS encryption
  - Anti-phishing protection
  - Sandboxing technology
  - Key-logging and screen scraping protection
  - Sensitive data masking
  - Control over file movements and transfers
  - Centralized or User Control
  - Permission management
  - Browser extensions restriction and control
  - Password management
  - Integrated VPN restriction and blocking
  - Identity-based access control
  - Granular control over browser components
  - Maintenance and Updates
  - Regular and automatic updates
  - Reporting capabilities for browsing history, risk scoring, and metrics
  - Additional Security Measures
  - Multi-factor authentication
  - Certificate protection
  - Browser DLP (Data Loss Prevention) features for alerting and blocking
  - Visibility and control over user browsing behavior
- This secure browser should ensure encrypted data transmission, high performance, and minimal latency, with comprehensive documentation and support for setup, troubleshooting, and maintenance.

4.2 Key Vendor Support Features

- Comprehensive Security Suite:
  - Next-Generation Firewall-as-a-Service (NGFW)
  - Secure Web Gateway (SWG)
  - Cloud Access Security Broker (CASB)
  - Data Loss Prevention (DLP)
  - Zero Trust Network Access (ZTNA)
  - Secure Browser Solutions
  - Physical Security Appliances*

        - For possible clinic-level firewall replacement.
- Cloud-Native Architecture:
    - Built for scalability and performance in the cloud.
- Zero Trust Network Access (ZTNA):
    - Strong identity verification and access control.
- Network Performance Optimization:
    - SD-WAN capabilities for optimized traffic management.
- Advanced Threat Defense:
    - Real-time threat detection and response.
- User-Friendly Management Tools:
    - Centralized policy control and network visibility.
- Vendor Reputation and Support:
    - Well-known and reputable vendors.
    - 24/7 availability and technical expertise.
        - 24/7 Customer Support with expert.
        - Availability of round-the-clock support to address any issues promptly.
        - Ability to call support 24x7x365 and contact support.
    - Technical Expertise:
        - Access to knowledgeable support staff who can provide detailed technical assistance.
    - Proven Track Record:
        - A history of successful deployments and satisfied customers in similar industries.
    - Comprehensive Documentation:
        - Availability of detailed guides, FAQs, and troubleshooting resources.
    - Training and Onboarding:
        - Provision of training sessions and onboarding support to ensure smooth implementation.
    - Regular Updates and Patches:
        - Commitment to providing regular software updates and security patches.
    - Customer Feedback and Improvement:
        - Mechanisms for collecting customer feedback and continuously improving the service.
    - Scalability and Flexibility:
        - Ability to scale the solution as your organization grows and adapt to changing needs.
    - Vendor Stability:
        - Financial stability and longevity of the vendor to ensure long-term support.
    - Integration Support:
        - Assistance with integrating the SASE solution with existing IT infrastructure.

4.3 Required Vendor Features:

- Organization – Vendors have experience implementing solutions with organizations similar to YVFWC
- Technical – The vendor's solution appropriately fits with YVFWC's environment and requirements
- Implementation Speed – Vendor will commit to fully install solution starting on November 1st 2025 with all sites and features fully deployed on or before August 1st, 2026.
- Prior Experience – Successful implementation and adoption in similar and relevant organizations.
- Vendor Stability – Vendor can demonstrate and be prepared to discuss medium to long range business objectives and plans.
- Training – Training program is comprehensive.
- Support – Vendor offers high level of on-going support.
- Usability – Solution is intuitive and time saving.

4.4 Technical and Interfacing Requirements

The technical response must be written in sufficient detail to permit YVFWC to conduct a meaningful evaluation of the SASE capabilities, support features, functionality, and ability to directly integrate the data sources as itemized. Some of the desired (but not required) integrations include:

1. Palo Alto – Next Generation Firewalls (NGFW) – Physical & Virtual including Azure-based.
2. Palo Alto Global Protect VPN – (or suitable replacement for VPN)
3. Meraki MX Security Appliances – Site-to-Site VPNs
4. Critical Start SOC API integration with Zero-Trust Analytics Platform (ZTAP)
5. Cloud Splunk (SIEM) API integration
6. Active Directory – Azure AD / Microsoft Entra ID
7. Microsoft Authenticator – MS Auth

4.5 General Security Requirements

YVFWC is committed to maintaining a highly secure and available environment for the safety of our patients while maintaining usability and accessibility for our users. Vendors will be required to provide a detailed plan in their response for appropriately addressing the security and privacy provisions (Including Authentication, Integrity, Confidentiality, Auditing, High Availability, and Disaster Recovery) of HIPAA, HITECH, The Omnibus Rule, The Joint Commission, Washington/Oregon Regulations and all other regulatory bodies under which YVFWC falls. Some of these specific requirements are listed in Sections 7 and 8, but the vendor must ensure compliance with all regulatory bodies in any case. The vendor further must agree to sign and execute our Business Associate Agreement and follow the provisions therein.

Hosted/SaaS solutions will be required to submit documentation of third-party security audits (Independent HIPAA Security Risk Assessments or industry best-practice certification/audit such as ISO27001), written copies of their security plan (including verification of yearly security risk assessments), and written certification of HIPAA compliance.

Finalists will be required to submit the attached Security Risk Assessment Questionnaire for consideration. The questionnaire is included with the RFP for review, and it is assumed by submitting a proposal that interested vendors will comply with all security requirements and will submit when requested.

4.6 Training Requirements

- Proposals must encompass a thorough training program for a total of 12 staff members, divided equally among three key departments: Information Security (4 staff), Network Operations (4 staff), and Systems Operations (4 staff). The training should be designed to ensure all participants achieve a high level of proficiency in using the system.
- To accommodate different learning preferences and schedules, the training can be delivered through a combination of full-day live sessions, flexible online web-based modules, or an appropriate number of training credits to deliver adequate training for the number of staff as mentioned. This blended approach will provide comprehensive coverage of the system's functionalities and allow for interactive, hands-on learning experiences as well as self-paced study options.
- At the end of the training, all team members should be well-equipped with the necessary skills and knowledge to effectively utilize the system in their respective roles.

4.7 Security Risk Assessment (SRA) Requirements

- The chosen vendor will be required to undergo a comprehensive Security Risk Assessment (SRA) conducted by YVFWC. This assessment is designed to ensure that robust security measures are in place to protect YVFWC's Patient Health Information (PHI). The SRA will be conducted in accordance with HIPAA requirements and will also ensure compliance with industry's best practices and standards, including HIPAA, HITRUST, ISO/IEC, and NIST.
- As part of this process, the vendor will need to complete YVFWC's detailed vendor SRA Questionnaire and submit relevant industry compliance standards and attestations. This thorough evaluation aims to verify that the vendor's security practices meet the highest standards for safeguarding sensitive health information.
- By adhering to these rigorous assessment protocols, YVFWC seeks to ensure that all vendors maintain the necessary security controls to protect PHI, thereby upholding the integrity and confidentiality of patient data. This process not only aligns with regulatory requirements but also reinforces YVFWC's commitment to maintaining the highest levels of data security and privacy.

4.8 Legal Requirements

- The vendor should ensure that the proposed solution complies with all Federal (e.g., HIPAA, HITECH), State, and The Joint Commission (or other accrediting body) health information security standards for data integrity, confidentiality, auditing, and availability.
- As part of the contract and Request for Proposal (RFP) process, the selected vendor will be required to sign and execute a Business Associate Agreement (BAA) to ensure compliance with HIPAA requirements. This agreement is essential for safeguarding protected health information (PHI) and ensuring that the vendor adheres to all necessary privacy and security standards mandated by HIPAA. The BAA will outline the responsibilities and obligations of the vendor in handling PHI, including

measures for data protection, breach notification procedures, and compliance with HIPAA regulations. By signing this agreement, the vendor commits to maintaining the confidentiality, integrity, and availability of PHI, thereby aligning with the organization's commitment to protecting sensitive health information.

4.9 Professional Services or Vendor Integration Requirements

- Vendors responding to this RFP must include full professional services to facilitate the entire setup, configuration, and migration of current configurations. This includes site-by-site cutovers, migration of firewall policies and rules, migration of Forcepoint policies and rules, migration of NAT policies and rules, and the phased cutover of 50 locations. Vendors should either include this pricing directly or collaborate with a Managed Services Provider to deliver a comprehensive response that encompasses both the complete SASE elements and the professional services required for a full migration

5 Implementation Timeline & Constraints

5.1 Proposed Project & Implementation Plan

Respondents are required to submit a detailed implementation plan for the project. This plan should comprehensively cover the following aspects and professional services to facilitate the complete migration of all locations, services, current networks, firewall and web-proxy policies, and associated services. The goal is to ensure a seamless transition with minimal disruptions to organizational operations throughout the project lifecycle.

- Implementation Process: Describe the step-by-step process you will follow to execute the project, from initial consultation to final deployment and post-implementation support.
  - Clinic Firewall Replacements – 50x Locations – YVFWC staff may be physical hands for installation.
    - Migration of all current clinic networks to the SASE implementation.
  - Migration of Existing Security Policies – Palo Alto Firewalls: Migration of 300+ Palo Alto firewall rules to the SASE platform.
  - Migration of Existing Security Policies – Forcepoint Web Proxy: Migration of 50+ Forcepoint policies to the SASE platform.
  - Migration of Existing NAT Policies from Palo Alto Firewalls: Migration of 100+ NAT policies moving traffic to the SASE platform.

- Project Structure: Outline the organizational structure of your project team, including key roles and responsibilities.

- Methodology: Explain the methodology you will use to manage and execute the project, highlighting any specific frameworks or approaches (e.g., Agile, Waterfall).

- Cost: Provide a detailed cost breakdown, including all phases of the project such as planning, design, development, testing, deployment, training, and ongoing support.

- Timeline: Present a comprehensive timeline that includes key milestones and deliverables, specifying the duration of each project phase.

- By addressing these elements, respondents will demonstrate their capability to effectively manage and deliver the project within the specified requirements.

5.1.1 Phased Implementation Requirements

Respondents are required to submit a comprehensive plan detailing the implementation strategy for the project. This plan must consider the following critical factors:

1. Organizational Scope: Yakima Valley Farm Workers Clinic (YVFWC) operates in nearly 50 locations in two states and employs approximately 3,000 staff members. The organization also maintains three datacenters. Full organizational metrics may be found in this document's appendices.
2. Healthcare Context: As a non-profit healthcare provider, YVFWC places a high priority on the reliability and security of its information systems and services, which are essential for delivering patient care.
3. Phased Implementation: The proposal should outline a phased implementation plan. This includes:
    - SASE Modules: A step-by-step deployment of different Secure Access Service Edge (SASE) modules.
    - Site-by-Site Cutover: A detailed schedule for transitioning each YVFWC facility and service into the new system.

The intent is to ensure that the implementation is seamless, minimizes disruption to operations, and maintains the integrity and security of patient information throughout the process. Respondents should provide a clear timeline, resource allocation, risk management strategies, and contingency plans to address potential challenges during the implementation.

5.2 Implementation: Meetings & Deadlines

YVFWC has the goal to start the implementation of the system by November 1st, 2025. Based on final vendor selection by September 30th 2025. Please fill out the following section with major events and deadlines including but not limited to – Earliest Possible Start Date, Begin Build, Build Completion, Begin Training, Earliest Implementation Completion and Latest Implementation Completion. In addition, please provide a sample project plan.

Implementation Event/Deadline	Date
Click here to enter text.	_____
Click here to enter text.	_____
Click here to enter text.	_____
Click here to enter text.	_____
Click here to enter text.	_____
Click here to enter text.	
How long will implementation take? Please breakdown and explain this estimate.	Click here to enter text.

5.3 Pricing Response

Please clarify your licensing model and specify the number of licenses included in your proposal. Organizational metrics can be found in the document's appendices. The SASE system requires a total of 12 Administrator access accounts.

Respondents must provide detailed and guaranteed pricing for the SASE system and any necessary third-party products to ensure optimal functionality. All price quotations and related conditions must be firm and irrevocable for six (6) months from the Proposal Submission or the conclusion of good faith negotiations, whichever is later. Quotes should include annualized pricing over a three-year term.

Pricing must be all-inclusive, covering labor, overhead, travel, equipment, materials, taxes, and any other expenses required to deliver the SASE system as specified in this RFP. Proposers assume all liability for any omissions.

Pricing should reflect a phased migration strategy spanning three to nine months, facilitating the phased rollout of individual SASE components. The full price of the SASE system should account for the time required for features and sites to become fully operational. YVFWC desires to purchase licensing and components only upon full realization and activation of those features.

Please include all applicable payment terms and special conditions. Any additional costs not covered in the sections below should be clearly itemized at the end of this section.

Pricing must include multiple options, including:

- Total cost up-front
- Annualized cost, broken down in a cost grid over the three-year term

Additionally, provide the Total Cost of Ownership (TCO), encompassing both implementation and ongoing annual operational costs. This should include, but is not limited to, the following components:

Implementation	Click here to enter text.
Ongoing Licensure	Click here to enter text.
Ongoing Support/Help Desk	Click here to enter text.
Software Maintenance Fees	Click here to enter text.
Interfaces	Click here to enter text.
Hosting/Storage Fees	Click here to enter text.
Performance guarantees.	Click here to enter text.
Total year one costs – Annualized Billing	Click here to enter text.
Total year two costs – Annualized Billing	Click here to enter text.
Total year three costs – Annualized Billing	Click here to enter text.
Initial Training Fees: include cost as well as how many hours per staff member training requires as	Click here to enter text.

well as how many staff members are included in this price.	
The RFP response should include training for up to 12 staff members. Please itemize cost per additional staff member if needed.	Click here to enter text.
Continued training costs: Training associated with upgrades and changes to system	Click here to enter text.
Other	
How is the product licensed?	Click here to enter text.
Are licenses purchased per named user of concurrent users?	Click here to enter text.
Define 'user' if it relates to the licensing model (i.e., super user, normal user etc. .).	Click here to enter text.
Can user licenses be reassigned when a workforce member leaves?	Click here to enter text.
If licensing is determined per workstation, do handheld devices count towards this licensing and how are off-site licenses and VPN handled and charged?	Click here to enter text.
What does each license actually provide?	Click here to enter text.
For modular systems, does each module require a unique license?	Click here to enter text.
In concurrent licensing systems, when are licenses released by the system (i.e., when the workstation is idle, locked, or only when user logs off)?	Click here to enter text.
Costs for any 3rd party vendors.	Click here to enter text.
Escrow costs.	Click here to enter text.
Costs to provide customizations	Click here to enter text.
Cost of transitioning and/or data conversion	Click here to enter text.

6 Vendor Information Requested

6.1 General

General	
Name	Click here to enter text.
Address (Headquarters)	
Address Continued	Click here to enter text.
Main Telephone Number	Click here to enter text.
Website	Click here to enter text.
Publicly Traded or Privately Held	Click here to enter text.
Parent Company (if applicable)	
Name	Click here to enter text.
Address	Click here to enter text.
Address Continued	Click here to enter text.
Telephone Number	Click here to enter text.
Main Contact	

Name	Click here to enter text.
Title	Click here to enter text.
Address	Click here to enter text.
Address Continued	Click here to enter text.
Telephone Number	Click here to enter text.
Fax Number	Click here to enter text.
Email Address	Click here to enter text.
Market Data	
Number of years as SASE vendor.	Click here to enter text.
Number of live sites.	Click here to enter text.
What is the percentage of vendor-provided installs vs. outsourced to 3rd party companies? Please list all applicable 3rd party vendors.	
Number of new SASE integrations over the last 3 years.	Click here to enter text.
Size of existing user base.	Click here to enter text.
Does the product have a Washington and/or Oregon State presence? If so, # of install sites by specialty and size; list of reference sites.	Click here to enter text.
What is the current implementation timeframe when using only vendor-supplied resources?	Click here to enter text.
How many organizations have de-installed any vendor systems over the past four (4) years? Please specify which systems and why.	Click here to enter text.
What is your customer retention for the years last three years?	Click here to enter text.
Total FTEs Last Year	Click here to enter text.
Total FTEs This Year	Click here to enter text.
Explain how your company is planning to meet the increase in demand for your product (including implementation, training, and support) over the next five (5) years.	Click here to enter text.
Product Information	
Please specify the product(s) you are proposing to use for this implementation.	Click here to enter text.
What version of the product is this?	Click here to enter text.
If this is not already generally available, please indicate an expected release date.	Click here to enter text.

6.2 Vendor References

Please provide client references similar in size to that of YVFWC that have been live with the recommended solution for at least 2 years. We require at least two but would prefer more.

Please list first reference name and contact information	Click here to enter text.
Please list second reference name and contact information	Click here to enter text.
Please list third reference name and contact information	Click here to enter text.
Please list fourth reference name and contact information	Click here to enter text.

6.3 Vendor Financial Stability

Has your company received venture capital as a source of funding in the last 10 years?	Click here to enter text.
Demonstrate history of profitability and market support. Provide 3 years of independently audited financial statements.	Click here to enter text.
Is your company in the process of or, has in the last three (3) years, been considered for any publicly announced acquisition attempts that may change senior management or ownership?	Click here to enter text.
Has your company ever been in litigation regarding fulfillment of contractual obligations or performance?	Click here to enter text.
Has any client terminated their contract with your company in the last three years? If so, please provide reason(s).	Click here to enter text.
How many customers acquired and implemented the proposed system within the last 12 months?	Click here to enter text.

6.4 General Technical Questions

What is the contractual SLA?	Click here to enter text.
Is all data stored in North American Data Centers?* *This is required*	Click here to enter text.
Please confirm which of the following compliance standards your product adheres: HITRUST, HIPAA, SOC 2 Type 1&2, FEDRAMP, PCI-DSS, FIPS 140, ISO/IEC 27001 - ***NOTE: Verification of compliance attestations are required upon final vendor selection.	Click here to enter text.
Does the system record and report all authorization actions?	Click here to enter text.
Do you have specific WAN response time requirements for use across a WAN? If so, please include them. If not, what are the optimal WAN conditions for use of your system across a WAN?	Click here to enter text.

List the security provisions of the system and how it complies with appropriate regulations.	Click here to enter text.
Can the system be set up with two separate work environments: Production, Test	Click here to enter text.
Does the system support multi-tenant functionality (i.e., different departments using the system such as IS, Quality, Training etc.)	
What end-user response time (in milliseconds) is generally considered to be within the normally functioning range?	Click here to enter text.
What other metrics do you monitor to ensure an acceptable user experience	Click here to enter text.
List an inventory of standard/canned reports your system provides. • How are they provided? • Is third party software required? • What kind of documentation do you provide? • What database is the user accessing the data from? Can report execution and delivery be automated?	Click here to enter text.
Describe the system's capabilities for ad hoc and custom reports. • Are data dictionaries or catalogs provided and maintained by your company? • How can we access a certain field if it is not available in the data dictionary? Is the reporting infrastructure maintained separately to ensure reporting load does not affect production?	Click here to enter text.
Is there any data in your system that cannot be reported on?	Click here to enter text.
Does the system have a way to monitor and troubleshoot end-to-end performance issues?	Click here to enter text.
Describe your technical support team, technical support initiation process, SLAs, and availability/escalation methods of getting to an engineer-level resource. Also, outline your expectations of YVFWC prior to initiating a support ticket with you.	Click here to enter text.

7 Product & Implementation Questionnaire

The following section applies to the SASE section unless specifically called out as applying to other modules or systems.

When responding to the specification section below, note that each functional statement's priority is indicated in the "Level of Desirability" column, which contains one of the following values:

Mandatory = Required at Go Live

Mandatory Requirements:

- These are non-negotiable and must be met for a proposal to be considered. Failure to meet any mandatory requirement may result in disqualification.
- Example: "Vendor must have at least five years of experience in providing similar services."

Desirable:

Desirable Requirements:

- These are preferred but not essential. Meeting these requirements can enhance the proposal's score but is not a strict necessity.
- Example: "Experience with similar projects in the healthcare sector is desirable."

Where the function is (or is not) provided by the system, place an "X" under one of the following columns:

"Yes, Included" = the function is available in the system and it is part of the basic system

"Yes, Additional Cost" = the function is available, but it requires system customization at an additional cost

"No" = the function is not available

In addition, enter your response in the RESP (Response) column in accordance to one of the following:

5 = Completely meets requirements today. The function will be available on day one of 'go live.'

4 = Partially meets requirements today

3 = Will completely meet requirements in future (specify date and version)

2 = Will partially meet requirements in future (specify required change and date/version)

1 = Can meet requirement through customization (specify price)

0 = Not planning to offer

Note: The "Comments / Clarifications" column is required where appropriate. This column can also be used to indicate if a function is not currently available but will be available in a future release by indicating the version number and approximate month/year when the function will be available (e.g., V6.1/May 2020).

7.1 Overall Technology Features

Feature	Requirements Criteria	Level of Desirability	RESP	Yes, Included	Yes, Additional Cost	No	Comments / Clarification
GENERAL FEATURES							
Identify general feature being evaluated for the technology	**Clarify the performance and functional requirement associated with the feature.**						
Single-Vendor SASE	Solution where a single provider delivers multiple converged network and security services. These services typically include software-defined wide-area network (SD-WAN), secure web gateway (SWG), cloud access security broker (CASB), network firewalling, and zero trust network access (ZTNA).	Mandatory					
Cloud-Centric Architecture	Simplifies management of all SASE solutions to enhances security, and simplification of management, through integrating these services into a unified, cloud-based platform	Mandatory					
USER INTERFACE & EXPERIENCE							

Customizable Dashboards, Reports and Visualizations	Customizations based on any data attribute without requiring any development / deployment effort	Desirable					
Granular Security Controls	RBAC, data encryption and data masking	Desirable					
Intuitive Navigation	Users should be able to find what they are looking for easily without extensive instructions.	Desirable					
Mobile Application	A Smartphone application should be included to allow administration, monitoring, and management from a mobile device	Desirable					
Simplicity	A streamlined and clutter-free design enables users to concentrate on their tasks without distractions. SASE cloud administration dashboards should be intuitive, straightforward, and accessible to users of all skill levels for effective component management.	Mandatory					
Help and Documentation	Provide easily accessible help and guidance to assist users when they encounter difficulties.	Mandatory					
Mobile Device Support & Alerting	Mobile device support/applications, SASE Mobile, etc.	Desirable					
COMPLIANCE REPORTING							
HIPAA Compliance Reporting	Facilitate the necessary reporting and auditing processes to comply with HIPAA standards, making it a comprehensive solution for healthcare data protection and compliance.	Desirable					
HITRUST Framework Alignment	Essential the SASE solutions are capable of handling sensitive data through supporting HITRUST adherence and reporting.	Desirable					
NIST Framework Alignment	Ensures the organization can manage and report on their security posture effectively through adherence of the NIST framework.	Desirable					

LOG & DATA COLLECTION							
Ability to Integration with Splunk Cloud via API for Log & Data Collection	The SASE solution outlined in this RFP will demonstrate seamless integration with Splunk Cloud, facilitating efficient log and data collection. This integration is essential for streamlining and centralizing security and network management, providing the visibility and analytics needed for organizations to quickly identify and respond to security threats across their network.	Desirable					
Ability to SysLog Integrate with Network Monitoring Systems	The Secure Access Service Edge (SASE) solution proposed in the RFP is designed to offer robust integration capabilities with network monitoring systems. It will support syslog and SNMPv3 protocols, ensuring compatibility with popular platforms like Solarwinds, LiveNX, and AlgoSec Firewall Analyzer. This integration is crucial for maintaining comprehensive visibility and management of network security, providing real-time monitoring, and facilitating proactive threat detection and response.	Desirable					
LOGGING RETENTION & REQUIREMENTS							
90 Days Hot Storage	The SASE solution should provide 90 days of hot storage for all logs, system errors, traffic flows, and related data.	Mandatory					
180 Days Cold Storage	The SASE solution should provide 90 days of hot storage for all logs, system errors, traffic flows, and related data.	Desirable					
Archived Logs - Ease of Restore	Vendor can demonstrate ease of restore and use of historical (archived) logs to aid in incident investigation	Desirable					
Log Exporting	Ability to export raw-logs to on-prem customer owned log server	Desirable					

Automated Logs Searches for Breaches	The SASE automated log search system must provide real-time monitoring, generate alerts for anomalies, integrate with SIEM systems, ensure compliance, and offer machine learning, a user-friendly interface, scalability, customizable dashboards, historical data analysis, and third-party threat intelligence compatibility.	Desirable					
Simplified, User-Friendly Log Searching	The SASE solution must include simplified, user-friendly log searching capabilities, allowing security teams to quickly and easily access and analyze log data to identify potential security threats and breaches.	Desirable					
API and/or THIRD-PARTY DIRECT INTEGRATIONS							
Palo Alto Cortex XDR	The SASE solution should have the capability to integrate directly via API to ingest endpoint security data, alert on key events, and provide cohesive security visibility across the portfolio	Desirable					
Palo Alto NGFW	The SASE solution should be capable of integrating directly via API to ingest firewall security data, alert on key events, and provide cohesive security visibility across the portfolio. This includes firewall events, IDS/IPS information, URL and DNS security events, and other associated metrics.	Desirable					
Forcepoint	The SASE solution should have the capability to integrate directly via API to Forcepoint Cloud to ingest events related to web and URL filtering, and associated security events	Desirable					
Splunk	The SASE solution should have the capability to integrate to the organization Splunk Cloud SIEM integration.	Mandatory					

Critical Start - ZTAP - SOC	The SASE solution should have the capability to integrate directly via API to the organization third-party Security Operations Center (SOC) hosted by Critical Start and using the Zero-Trust Analytics Platform (ZTAP)	Desirable					
DUO - MFA	The SASE solution should have the capability to integrate directly via API to the organizations MFA instance with DUO.	Desirable					

7.2 Architecture Requirements

Feature	Requirements Criteria	Level of Desirability	RESP	Yes, Included	Yes, Additional Cost	No	Comments / Clarification
Cloud-First Strategy	Prioritizes cloud-based services for scalability, flexibility, and cost savings, while ensuring minimal on-premises assets are robust and integrated.	Mandatory					
Infrastructure & Licenses	Comprehensive list of required components, software, and licenses for go-live and anticipated growth.	Mandatory					
Supporting Devices	Details necessary hardware, software, and support services for smooth integration.	Mandatory					
Scalability	Ensures the solution can grow with the enterprise, accommodating new sites, endpoints, and cloud environments.	Mandatory					
Systems Integration	Seamlessly integrates with existing network and security solutions like Cisco Meraki, Palo Alto Networks, Nutanix, Rubrik, Splunk, and more.	Mandatory					
Network Management	Simplifies management by consolidating security functions into a single, cloud-based interface.	Mandatory					

7.3 Network Features & Requirements

Feature	Requirements Criteria	Level of Desirability	RESP	Yes, Included	Yes, Additional Cost	No	Comments / Clarification
SD-WAN Features	**Clarify the performance and functional requirement associated with the feature.**						
Application-Centric Networking	Prioritizes and routes traffic based on application needs.	Mandatory					
Centralized Management	Simplifies network administration through a centralized dashboard.	Mandatory					
Optimized Connectivity	Supports multiple transport services (MPLS, LTE, DIA, broadband).	Mandatory					
Improved Performance	Reduces latency and enhances bandwidth usage.	Mandatory					
Secure Connections	Encrypts data across the network.	Mandatory					
Cloud-Native Architecture	Delivers services from the cloud for rapid deployment and scalability.	Mandatory					
Dynamic Perimeter	Accommodates remote workers and branch offices.	Mandatory					
Simplified Network Management	Reduces complexity of managing security devices.	Mandatory					
Capacity Requirements	Routes/inspects traffic at 1Gbps (clinics) and 10Gbps (data centers).	Mandatory					
Overlay Transport	Provides secure connectivity over insecure mediums.	Mandatory					
Identity-Based Networking	Maps users to IP addresses across the network.	Mandatory					
Application/User Experience Reporting	Reports performance metrics beyond simple ICMP RTT.	Mandatory					
Custom Application Definition	Configures custom applications for routing and policy decisions.	Mandatory					

General Network Features	Clarify the performance and functional requirement associated with the feature.						
Hardware & VLAN Management	Replace Meraki MX, L3 gateway for VLANs, support multiple VLANs, VLAN management across sites.	Mandatory					
Network Security	Access lists, malware protection, IDS/IPS, local/clinic level firewall.	Mandatory					
Routing & Traffic Control	Dynamic routing (BGP, etc.), policy-based routing, automatic route propagation, QoS/traffic shaping.	Mandatory					
DHCP & Captive Portal	DHCP server capabilities, captive portal with splash page.	Mandatory					
Packet Capture & Troubleshooting	Packet capture on L3 device and connected clients, embedded packet capture, basic network troubleshooting tools, detailed flow logging.	Desirable					
Monitoring & Alerts	SNMPv3 polling, device alerts, REST API for stats and configurations.	Desirable					
Content Filtering &	Content filtering (URL, category, IP),	Mandatory					
Teleworker Appliances	Ability to provide and support small, all-in-one/teleworker appliances to allow testing and use of ambulatory equipment in an employee's home	Desirable					
Network Tools	Ping, tracert, nslookup, ARP, speed test, iPerf, tcpdump.	Desirable					
Connectivity & Redundancy	Link aggregation, serial console port, redundant power supplies, support for 100/1000M RJ45 and 10Gb RJ/SFP+ interfaces.	Mandatory					

7.4 Secure Web Gateway (SWG) Features & Requirements

Feature	Requirements Criteria	Level of Desirability	RESP	Yes, Included	Yes, Additional Cost	No	Comments / Clarification
Web Security	URL filtering (malicious, content-based), application control, advanced threat protection, malicious code detection, remote user protection.	Mandatory					
Traffic Inspection	SSL/TLS inspection and decryption, data loss prevention (DLP).	Mandatory					
Policy & Access Management	Dynamic policy enforcement, role-based access policies, multi-factor authentication (MFA).	Mandatory					
Monitoring & Reporting	Logging and analysis, user access reporting.	Mandatory					
Performance & Control	Bandwidth control.	Mandatory					

7.5 Zero Trust Network Access (ZTNA) – Requirements & Features

Feature	Requirements Criteria	Level of Desirability	RESP	Yes, Included	Yes, Additional Cost	No	Comments / Clarification
Identity & Access Control	Identity verification, least-privilege access, role-based access policies, identity, and context-based boundaries.	Mandatory					

Network Security	Micro-segmentation, application layer security, reduced attack surface, dynamic policy enforcement.	Mandatory					
Integration & Support	Integration with SASE solutions, third-party vendor and IoT device support, wide asset coverage.	Mandatory					
Monitoring & Reporting	Context-aware policies, user access reporting.	Mandatory					
Application Layer Security	ZTNA functionality at the application layer to provide more granular security controls.	Mandatory					

7.6 Secured Browser - Features & Requirements

Feature	Requirements Criteria	Level of Desirability	RESP	Yes, Included	Yes, Additional Cost	No	Comments / Clarification
Privacy & Security	Blocking third-party trackers, password management, anti-phishing protection, automatic HTTPS encryption, ad and tracker blocking, cookie management, privacy-focused search engines, customizable privacy settings, pop-up blocking, sensitive data masking, key-logging and screen scraping protection, certificate protection.	Desirable					
Browser Control	Browser extensions control, VPN restriction and blocking, visibility and control, granular control over browser components, identity-based access control, multi-factor authentication.	Desirable					

Updates & Reporting	Regular and automatic updates, reporting capabilities.	Desirable					
Data Loss Prevention (DLP)	Browser DLP alert and blocking, browser DLP alert and accept, control file movements and transfers.	Desirable					
Network Tools	Sandboxing, integrated VPN restriction, packet capture/tcpdump.	Desirable					

7.7 Firewall-as-a-Service (FWaaS) – Features & Requirements

Feature	Requirements Criteria	Level of Desirability	RESP	Yes, Included	Yes, Additional Cost	No	Comments / Clarification
Layer-7 Firewall	Provides L7 firewall with IDS/IPS and other security services.	Mandatory					
Digital Experience Monitoring (DEM)	Monitors service delivery paths and connectivity issues for remote work.	Mandatory					
Web Proxying	Offers secure connections for traffic that cannot be fully inspected.	Mandatory					
Integrated VPN Services	Routes traffic through a VPN to optimize cloud environments.	Mandatory					
Dynamic Performance	Adapts to changing business needs and threat landscapes.	Mandatory					
Threat Protection	Detects and responds to threats in real-time.	Mandatory					
Advanced Threat Protection	Includes next-gen firewall capabilities with advanced inspection and detection.	Mandatory					
Operational Efficiency	Simplifies management and enhances operational speed.	Mandatory					
Simplified Connectivity	Supports remote and hybrid users by connecting to nearby cloud gateways.	Mandatory					

Cloud-Native Architecture	Combines networking and security functions into a single cloud service.	Mandatory					
Web and URL Filtering	Implements advanced URL filtering to protect against web-based threats.	Mandatory					
DNS Security	Monitors DNS traffic to block data exfiltration and enforce security policies.	Mandatory					
Support for EDLs	Integrates External Dynamic Lists for dynamic threat management.	Mandatory					
Consistent Security	Ensures full visibility and inspection of traffic across all ports and protocols.	Mandatory					

7.8 Cloud Access Security Broker (CASB) – Features & Requirements

Feature	Requirements Criteria	Level of Desirability	RESP	Yes, Included	Yes, Additional Cost	No	Comments / Clarification
Secure Access	Provides secure remote access to corporate and cloud applications.	Mandatory					
Risk Visibility	Assesses risk of unsanctioned applications and makes access decisions.	Desirable					
Threat Prevention	Identifies unusual behavior, detects threats, and remediates automatically.	Mandatory					
Cloud Usage Control	Manages cloud usage with advanced analytics, controls access based on status or location.	Mandatory					
Data Encryption	Encrypts sensitive data in motion and at rest.	Mandatory					
Unified Security Policy	Enforces consistent security policies across on-premises and cloud environments.	Mandatory					

Visibility & Control	Provides detailed insights into cloud application usage for monitoring and management.	Mandatory					
Threat Protection	Detects and responds to threats in real-time, protecting against malware and ransomware.	Mandatory					

7.9 Data Loss Prevention (DLP) – Features & Requirements

Feature	Requirements Criteria	Level of Desirability	RESP	Yes, Included	Yes, Additional Cost	No	Comments / Clarification
Cloud Integration	Integrates DLP tools into cloud platforms for seamless security across services and applications.	Mandatory					
Data Protection	Provides inline data inspection, at-rest data protection, and SSL decryption to secure data in transit and at rest.	Mandatory					
Unified Policy Enforcement	Applies consistent DLP policies across all data locations, eliminating the need for separate DLP gateways.	Mandatory					
Shadow IT Protection	Offers visibility into unauthorized applications and services to reduce data loss risks.	Mandatory					
User Error Minimization	Monitors and governs data access to minimize user mistakes.	Mandatory					
Advanced Threat Protection	Identifies and blocks sophisticated threats to enhance data security.	Mandatory					
Agent-Based DLP	Protects sensitive data across networks and devices, both on and off premises.	Mandatory					

7.10 Vendor Support – Features & Requirements

Feature	Requirements Criteria	Level of Desirability	RESP	Yes, Included	Yes, Additional Cost	No	Comments / Clarification
Customer Support	Provides toll-free customer support 24 hours, seven days per week.	Mandatory					
Geographic and Language Support	Provide support in locations needed and in the languages that are spoken by employees.	Mandatory					
User Manuals	Provides a complete set of user manuals for all software applications to document and explain system features and functions.	Mandatory					
Implementation Support	Provides complete turnkey onsite implementation and project management support.	Mandatory					
Training	Provides onsite training to technicians.	Mandatory					
Software Updates	Provides future software releases and updates to all applications as part of regular software maintenance fees.	Mandatory					
Technical Documentation	Provides technical documentation for support staff including system overviews, design, flowcharts, and file layouts.	Mandatory					
Performance Monitoring	(If applicable) Provides remote software monitoring to identify anomalies and provide automatic upgrades.	Mandatory					
Implementation and Configuration	Describe the process by which the collectors, devices, and reporting tools, along with their associated licenses, are deployed and initially configured.	Mandatory					
Ongoing Operations	Describe how, after the initial configuration, the solution is maintained and updated.	Mandatory					

Scalability	Ability to scale all solutions up or down based on the organization's growth and needs	Mandatory					

7.11 Additional Product and Implementation Questions

General Product Questions

How can the proposed solution help improve workflows?	Click here to enter text.
What customer service certifications or awards have you received? What are your service level response times (SLA's)? What are your after-hour's support and support during upgrade weekends?	Click here to enter text
Please provide information on your product's future roadmap. Are there any new directions or key technologies you are looking to adopt?	Click here to enter text
Project Design	
Describe your approach to the project design phase for implementing a Secure Access Service Edge (SASE) solution. • What methodologies and frameworks do you utilize to ensure a comprehensive and effective design? • How do you incorporate client-specific requirements and constraints into the design process? • What steps do you take to validate and refine the design before moving to implementation?	
Describe the roles and responsibilities of both the vendor and the VAR/MSP in the project. • How are tasks and responsibilities divided between the vendor and the VAR/MSP? • Who will be the primary point of contact for the client?	
Project Execution	
Describe your implementation methodology including personnel involved, personnel experience, level of support, method of support, and timeframe from start to finish.	Click here to enter text.
How many YVFWC staff members and what qualifications will be required to implement the system (during the design, testing, and implementation phases?	Click here to enter text.
Explain how coordination and collaboration will be maintained between the vendor, VAR/MSP, and the client during project execution. • What tools and platforms will be used for collaboration and communication? • How will you ensure that all parties are aligned and informed throughout the project?	

How will project timelines, milestones, and deliverables be tracked and communicated?	
YVFWC must grant permission to subcontract any work to be performed under this RFP, and the subcontractor must be identified before approval.	Click here to enter text.
Do you have Implementation plan partners that implement the system? Who would be implementing your proposed solution?	Click here to enter text.
Provide a sample project plan of the implementation.	Click here to enter text.
What kind of documentation do you provide?	Click here to enter text.
Does your implementation process include an efficiency assessment of our current workflows and administrative processes and provide recommendations for optimizing them in the new system?	Click here to enter text.
Is onsite support provided during the rollout? A training offering is required as part of this RFP.	Click here to enter text.
Training	
Describe your training process including personnel involved, personnel experience, timeframe, method of training (Onsite, classroom, internet-based)	Click here to enter text.
Do your training materials include proficiency testing?	Click here to enter text.
Describe your recommended training plan given a comparably sized organization. Include: • Personnel involved, including their level of experience • Level and method of training • Timeframe from start to finish • Central training vs. onsite training vs. train-the-trainer Initial training and subsequent refresher training	Click here to enter text.
Provide a description of all training classes available including technical, application, and end-user classes.	Click here to enter text.
Describe your testing process including testing types, testing environment, personnel involved, personnel experience, and timeframe from start to finish	Click here to enter text.
Provide sample test plan and discuss your approach for automated test coverage	Click here to enter text.

8 Appendix A – YVFWC Site / Facilities Inventory

Equipment Pr...	Name	Address	City	State	Zip Code
BHM	Behavioral Health Services	918 East Mead Avenue	Yakima	Washington	98903
BHT	BHS 12th Avenue	307 South 12th Avenue, Suite 4B	Yakima	Washington	98902
CAD	Coastal Family Administration	3990 Abbey Lane, Building B, Suite 103	Astoria	Oregon	97103
CBD	Columbia Basin Pediatric Dentistry	7501 W. Deschutes Place	Kennewick	Washington	99336
CDC	Community Dental Care	1721 E. Lincoln Ave.	Sunnyside	Washington	98944
CFH	Coastal Family Health Center	2158 Exchange Street, Suite 304	Astoria	Oregon	97103
CHC	Clatskanie Community Health Center	401 SW Bel Air Drive	Clatskanie	Oregon	97016
CHV	Children's Village	3801 Kern Road	Yakima	Washington	98902
DFK	Dentistry For Kids	2611 S. Quinlan Place	Kennewick	Washington	99338
FMC	Family Medical Center	1120 West Rose Street	Walla Walla	Washington	99362
GFM	Granger Family Medicine Clinic	115 Sunnyside Avenue, Suite A	Granger	Washington	98932
GMD	Grandview Medical-Dental	1000 Wallace Way	Grandview	Washington	98930
GNS	Granger Nutrition Services/WIC	121 Sunnyside Avenue	Granger	Washington	98932
LFH	Lancaster FHC Beverly	3896 Beverly Ave. NE, Building J, Ste....	Salem	Oregon	97301
LHC	Lancaster FHC Lancaster	255 Lancaster Drive NE	Salem	Oregon	97301
LMD	Lincoln Avenue Medical-Dental	2205 West Lincoln Ave.	Yakima	Washington	98902
MCM	McMinnville Nutrition Services/WIC	412 NE Ford Street, Suite 101	McMinnville	Oregon	97128
MEM	Memorial WIC	218 S. 29th Avenue	Yakima	Washington	98902
MFH	Mirasol Family Health Center	589 Northwest 11th	Hermiston	Oregon	97838
MHC	Miramar Health Center Pasco	1608 N. Road 44	Pasco	Washington	99301
MHK	Miramar Health Center Kennewick	6351 West Rio Grande Ave.	Kennewick	Washington	99336
MVF	Mid-Valley Family Medicine	620 W 1st Street	Wapato	Washington	98951
MVW	Mt. View Women's Health Center	240 Division Street	Grandview	Washington	98930
NBG	Newberg Nutrition Services/WIC	2251 E. Hancock Street, Suite 107	Newberg	Oregon	97132
NCA	Northwest Community Action Center	706 Rentschler Lane	Toppenish	Washington	98948
NSH	Safe Haven	101 Lincoln Ave.	Toppenish	Washington	98948
PPD	Pacific Pediatrics	1475 Mt. Hood Ave.	Woodburn	Oregon	97071
QDC	Quincy Datacenter	2200 M St NE, Building C	Quincy	Washington	98848
RFH	Rosewood Family Health	3530 SE 88th Ave.	Portland	Oregon	97266
RHG	Rosewood Family Health at Gateway	135 NE 102nd Ave.	Portland	Oregon	97220
RHL	Rosewood Family Health at Lents	9047 SE Foster Road	Portland	Oregon	97266
SIC	Sunnyside Immediate Care	2680 Yakima Valley Hwy. Suite B	Sunnyside	Washington	98944
SMC	Salud Medical Center	1175 Mt. Hood Avenue	Woodburn	Oregon	97071
TAC	Administration Annex	602B W. First Avenue	Toppenish	Washington	98948
TAC	Administration Central	604 W. First Avenue	Toppenish	Washington	98948
TAC	Toppenish Warehouse	303 S. Date St.	Toppenish	Washington	98948
TAN	Administration North	308 Monroe St	Toppenish	Washington	98948
TAS	Administration South	603 W. 4th Avenue	Toppenish	Washington	98948
TCC	Toppenish Conference Center	514 W. First Avenue	Toppenish	Washington	98948
TMD	Toppenish Medical-Dental	510 W. First Avenue	Toppenish	Washington	98948
UMA	Unify Mission Avenue	120 West Mission Avenue	Spokane	Washington	99201
UNE	Unify Northeast	4001 N. Cook Street	Spokane	Washington	99207

VVM	Valley Vista Medical Group	820 Memorial Street, Suite 1	Prosser	Washington	99350
WVF	West Valley Family Health	5109 Summitview Avenue	Yakima	Washington	98908
YAK	Access Central Pharmacy	2601 Commerce Lane	Yakima	Washington	98901
YFM	11th Avenue Family Medicine Clinic	314 South 11th, Suite A	Yakima	Washington	98902
YMD	Yakima Medical-Dental	602 East Nob Hill Blvd.	Yakima	Washington	98901
YPM	Yakima Procurement	1805 S. 24th Avenue, Suite B & D	Yakima	Washington	98902
YPP	Presson Place	1720 Presson Place	Yakima	Washington	98903
YTH	Yakima Administration	601 N. Keys Road	Yakima	Washington	98901
YVT	YV Tech	1120 S. 18th Street	Yakima	Washington	98901

9 Appendix B – Meraki Inventory

CW9164I	233
MG21-NA	3
MR18	1
MR42	2
MR46	8
MS120-24P	3
MS250-24P	3
MS250-48FP	191
MS425-32	6
MX100	1
MX105	7
MX250	2
MX450	2
MX64	5
MX68	3
MX84	39
MX85	1
MX95	8
VMX-M	1
Z4	3

10 Appendix C – Clinic Firewalls – Client Statistics – 30 Day

Client stats

TOTAL UNIQUE CLIENTS	AVERAGE # OF CLIENTS PER DAY	AVERAGE USAGE PER CLIENT
17719	8569	9.96 GB

Clients per day

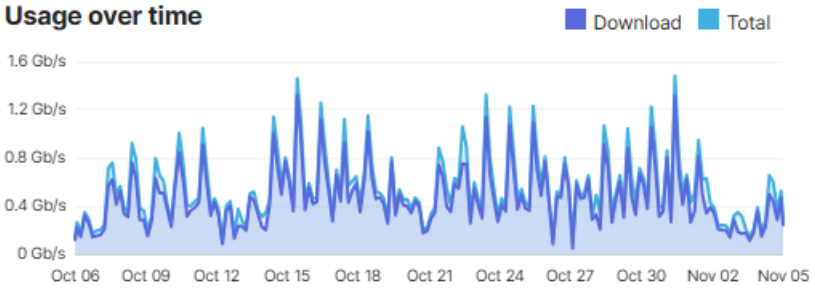
Splash page

NUMBER OF CLIENTS TO REQUEST PAGE	NUMBER OF CLIENTS GRANTED ACCESS
6407	5508

Usage stats

TOTAL DATA TRANSFERRED	TOTAL DATA DOWNLOADED	TOTAL DATA UPLOADED
172.36 TB	147.62 TB	24.74 TB

Usage over time



Top client device manufacturers by usage

Manufacturer	Usage	# Clients	% Clients
Dell	113.19 TB	1815	10.24%
Intel	41.73 TB	1910	10.78%
Other	4.78 TB	8261	46.62%
Apple	4.09 TB	860	4.85%
ShoreTel	3.22 TB	1446	8.16%
SHARP	843.53 GB	179	1.01%
Hewlett-Packard	808.98 GB	331	1.87%
HP	784.58 GB	258	1.46%
Cisco Systems	771.21 GB	653	3.69%
Meraki	428.03 GB	343	1.94%

Top device models by usage

Model	# Devices	Usage	Average Usage per Device
MX95	7	113.78 TB	16.25 TB
MX105	2	16.39 TB	8.19 TB
MX100	1	4.32 TB	4.32 TB
MX84	34	37.76 TB	1.11 TB
MX64	1	97.65 GB	97.65 GB
MX68	1	22.43 GB	22.43 GB

11 Appendix D – Nutanix & Rubrik– Computing Inventory

11.1 Rubrik Inventory

11.1.1 Quincy, WA Datacenter

- 8x Rubrik Model: R6410

11.1.2 Yakima, WA Datacenter

- 4x Rubrik Model: R6404
- 8x Rubrik Model: R6304

11.2 Nutanix Inventory

11.2.1 Quincy, WA Datacenter

- 7x Model: NXS1UNS12G800

12 Appendix E – Server Counts

- 188 Total
  - pc-linux-gnu 4
  - Windows Server 2012 R2 Datacenter 1
  - Windows Server 2016 Datacenter 63
  - Windows Server 2016 Standard 5
  - Windows Server 2019 Datacenter 27
  - Windows Server 2019 Standard 35
  - Windows Server 2022 Datacenter 33
  - Windows Server 2022 Datacenter Azure Edition 3
  - Windows Server 2022 Standard 17

13 Appendix F – General YVFWC Metrics

- Total # of Active Accounts: 3969
- Total # of Employees: 2462
- Total # of VPN Users: 604
- Total # of Managed Endpoints (Workstations + Servers): 3188
- Total # of Endpoints - Workstations: 3021
- Total # of Servers: 166
- Total # of Endpoints in Palo Alto Cortex XDR: 3188