Sify Digital Services Ltd.

SASE Product Requirement Document

Contents

[1 Executive Summary 2](#_Toc165273847)

[1.1 Overview 2](#_Toc165273848)

[2 Key Features & Benefits 2](#_Toc165273849)

[2.1 Key Features 2](#_Toc165273850)

[2.2 Key Benefits 3](#_Toc165273851)

[3 Purpose, Scope & Stakeholders 3](#_Toc165273852)

[3.1 Business Drivers for the Product: 3](#_Toc165273853)

[3.2 Critical Success Factors: 4](#_Toc165273854)

[4 Features and Functionality 4](#_Toc165273855)

[5 Technical Specifications 5](#_Toc165273856)

[5.1 Network Architecture 5](#_Toc165273857)

[5.2 Security Components 5](#_Toc165273858)

[5.3 Integration 6](#_Toc165273859)

[5.4 Scalability 6](#_Toc165273860)

[5.5 Performance 6](#_Toc165273861)

[6 Sify Deliverables 6](#_Toc165273862)

[7 Ordering & Billing 7](#_Toc165273863)

[8 CPQ Related Information 7](#_Toc165273864)

[8.1 Order Login Data for GUI 7](#_Toc165273865)

[9 Terms and Conditions 8](#_Toc165273866)

[10 SLA 9](#_Toc165273867)

[10.1 Delivery SLA 9](#_Toc165273868)

[10.2 Operation SLA 10](#_Toc165273869)

[11 User Experience 10](#_Toc165273870)

[11.1 User Training and Documentation 10](#_Toc165273871)

[12 Regulatory and Compliance Considerations 10](#_Toc165273872)

[13 Timeline and Milestones 11](#_Toc165273873)

[13.1 Development Timeline 11](#_Toc165273874)

[14 Risks and Mitigation Strategies 11](#_Toc165273875)

[14.1 Potential Risks 11](#_Toc165273876)

[14.2 Mitigation Strategies 12](#_Toc165273877)

[15 Stakeholder Approval 12](#_Toc165273878)

[15.1 Review and Approval 12](#_Toc165273879)

[16 Appendices 12](#_Toc165273880)

[16.1 Glossary 12](#_Toc165273881)

# Executive Summary

## Overview

As enterprises transform their business processes to embrace greater digitization, cloud and mobility are combining to rapidly shift the application and data traffic profile within the enterprise. More enterprise applications are being delivered from the cloud, and more enterprise users are mobile and require anytime/anywhere access to applications. The network delivering application data to users must evolve. In distributed enterprises, such as those with several branches and remote workers, it is the wide area network (WAN) that requires an urgent transformation.

WAN transformation for a distributed Enterprise needs to address a diverse set of connection types, dispersed locations with different bandwidth needs, and the need to access applications both within the network and through the cloud. At the same time WAN transformation needs to look at simplifying networks, enhancing control, improving performance, visibility and driving efficiency.

Secure Access Service Edge (SASE) provides a solution to the WAN transformation. The SASE model converges networking and security services into a unified cloud-based architecture, providing secure access to applications and data from anywhere. Its primary objectives include:

* **Secure Access**: Enable secure access to applications and data for users regardless of their location (office, remote, mobile) or the device they're using.
* **Cloud-Native Architecture**: Leverage cloud-native technologies to deliver scalable, flexible, and resilient networking and security services.
* **Unified Platform**: Integrate multiple networking and security functions, such as SD-WAN, firewall, secure web gateway (SWG), and zero-trust network access (ZTNA), into a single platform.
* **Simplified Management**: Streamline network and security management through centralized policy orchestration and enforcement, reducing complexity and operational overhead.
* **Optimized Performance**: Ensure optimal performance and user experience by leveraging edge computing and intelligent traffic routing capabilities.
* **Enhanced Security**: Provide comprehensive security capabilities, including data encryption, threat detection and prevention, identity-based access control, and continuous monitoring.
* **Scalability and Agility**: Scale services dynamically based on demand and adapt to changing business requirements quickly and efficiently.

Sify’s SASE solution aims to transform traditional network architectures into modern, cloud-centric models that prioritize security, flexibility, and user experience in the increasingly distributed and digitalized business environment.

# Key Features & Benefits

## Key Features

|  |
| --- |
| **Unified Architecture:** Integration of multiple networking and security functions into a single cloud-native platform, eliminating the need for disparate point solutions. |
| **Secure Access**: Provides secure access to applications and data for users regardless of their location or device, ensuring data confidentiality and integrity. |
| **SD-WAN Capabilities**: Software-defined wide area networking (SD-WAN) functionality for efficient and optimized traffic routing across the network, improving performance and reliability. |
| **Firewall as a Service (FWaaS)**: Cloud-delivered firewall capabilities for perimeter security, protecting against unauthorized access and malicious threats. |
| **Secure Web Gateway (SWG)**: Web security features, such as URL filtering, malware detection, and data loss prevention (DLP), to safeguard against web-based threats and enforce acceptable use policies. |
| **Zero Trust Network Access (ZTNA)**: Identity-centric access controls that enforce the principle of least privilege, ensuring that only authorized users and devices can access specific resources. |
| **Data Encryption**: End-to-end encryption of data in transit and at rest to prevent unauthorized interception and access, ensuring data privacy and compliance with regulatory requirements. |
| **Edge Computing**: Leveraging edge locations for localized processing of data and applications, reducing latency and improving performance for distributed users and devices. |

## Key Benefits

|  |
| --- |
| **Description** |
| **Enhanced Security**: Comprehensive security capabilities protect against a wide range of threats, reducing the risk of data breaches and cyber attacks. |
| **Improved User Experience**: Secure, high-performance access to applications and data from anywhere, leading to increased productivity and user satisfaction. |
| **Simplified Management**: Centralized policy management and orchestration streamline network and security operations, reducing complexity and administrative overhead. |
| **Scalability and Flexibility**: Cloud-native architecture allows for seamless scalability and adaptability to changing business requirements and user demands. |
| **Cost Savings**: Consolidation of networking and security functions onto a single platform reduces hardware and operational costs, as well as simplifies licensing and procurement. |
| **Regulatory Compliance**: Built-in security controls and encryption help organizations comply with industry regulations and data protection laws. |
| **Business Agility**: Faster deployment of new applications and services, as well as the ability to quickly respond to evolving threats and market conditions. |

# Purpose, Scope & Stakeholders

The SASE solution offers organizations a modern approach to networking and security, empowering them to securely connect users, devices, and applications in today's distributed and digitalized business landscape. Managed Service Providers (MSPs) such as Sify play a crucial role in delivering technology solutions and services to businesses. Offering a Secure Access Service Edge (SASE) solution can align with several business drivers for Sify, enhancing its value proposition and addressing the evolving needs of their customers.

Sify’s scope would be to manage customer’s WAN infrastructure end to end. This would be further covered in the Deliverables section. Key stakeholders involved in the creation of this product include the OEM, as well as Sify Product, Engineering, Commercial, Service Delivery, Service Support & Infrastructure Services teams.

## Business Drivers for the Product:

|  |
| --- |
| **Business Drivers** |
| Meeting customer demands for comprehensive network and security solutions that an adapt to their evolving IT environments, support remote workforces, and provide seamless connectivity to cloud-based applications |
| Differentiation and Competitive Advantage by offering innovative and cutting-edge solutions. |
| Revenue Growth: Offering a SASE solution can open up new revenue streams for Sify through subscription-based pricing models, recurring revenue from managed services, and value-added offerings such as consulting, implementation, and ongoing support services. |
| Reduced Operational Costs: SASE solutions typically involve cloud-based architectures that require less hardware, infrastructure, and maintenance compared to traditional networking and security solutions. |

## Critical Success Factors:

|  |
| --- |
| **Critical Success Factors** |
| Comprehensive Security Strategy. |
| User Experience and Adoption. |
| Network Performance and Reliability. |
| Integration and Interoperability. |

# Features and Functionality

These unique technical features are collectively required to address the complex requirements of modern networking environments.

|  |  |
| --- | --- |
| **Technical Feature** | **Description** |
| **Secure Remote Access** | * Support for remote and mobile users to securely access corporate resources from any location. * Authentication mechanisms such as multi-factor authentication (MFA) to verify user identities. * Encryption of data in transit to protect against eavesdropping and unauthorized access. |
| **SD-WAN Capabilities** | * Software-defined wide area networking (SD-WAN) features for optimizing network performance and reliability. * Dynamic traffic routing to ensure efficient use of network resources and minimize latency. * Quality of Service (QoS) mechanisms to prioritize critical applications and ensure consistent performance. |
| **Firewall as a Service (FWaaS)** | * Cloud-delivered firewall capabilities to enforce security policies and protect against unauthorized access. * Application-aware firewall rules to control access based on application type and behavior. * Intrusion detection and prevention (IDS/IPS) capabilities to detect and block malicious traffic. |
| **Secure Web Gateway (SWG)** | * Web filtering and content inspection to enforce acceptable use policies and protect against web-based threats. * Malware detection and prevention to identify and block malicious websites and downloads. * Data loss prevention (DLP) to prevent the unauthorized transmission of sensitive information. |
| **Zero Trust Network Access (ZTNA)** | * Identity-centric access controls based on user identity, device posture, and contextual factors. * Just-in-time access provisioning to grant temporary access privileges based on specific conditions. * Continuous monitoring and adaptive authentication to dynamically adjust access controls based on risk levels. |
| **Data Encryption and Privacy** | * End-to-end encryption of data to protect confidentiality and integrity. * Encryption key management to securely generate, store, and distribute encryption keys. * Data masking and anonymization to protect sensitive data from unauthorized access. |
| **Edge Computing Support** | * Edge computing capabilities to process data and run applications closer to the source of data generation. * Support for containerized applications and microservices architectures at the network edge. * Integration with edge computing platforms to enable distributed computing and analytics. |
| **Centralized Policy Management** | * Centralized policy orchestration and enforcement across networking and security functions. * Role-based access controls to delegate administrative responsibilities and ensure compliance. * Real-time visibility and reporting to monitor policy adherence and identify security incidents. |
| **Scalability and High Availability** | * Scalable architecture to support growing numbers of users, devices, and applications. * Redundancy and failover mechanisms to ensure high availability and minimize downtime. * Load balancing and auto-scaling capabilities to distribute traffic and resources efficiently. |
| **Integration and Interoperability** | * APIs and integration points to integrate with existing IT systems, applications, and security tools. * Compatibility with industry-standard protocols and frameworks to ensure interoperability. * Support for multi-cloud and hybrid cloud environments to accommodate diverse deployment scenarios. |

# Technical Specifications

## Network Architecture

|  |
| --- |
| **SASE Vendor Platforms Network Architecture** |
| Description of the overall network architecture, including edge locations, data centers, and cloud services. |
| Identification of networking components such as routers, switches, and access points. |
| Design considerations for network segmentation, routing protocols, and VLAN configurations. |
| Capabilities to integrate with on-premises data center solutions. |
|  |

## Security Components

|  |
| --- |
| Specification of security components such as firewalls, secure web gateways, and intrusion detection/prevention systems. |
| Configuration requirements for access control lists (ACLs), security policies, and encryption algorithms. |
| Integration with identity and access management (IAM) systems for authentication and authorization. |
|  |

## Integration

|  |
| --- |
| **Integration** |
| Integration with various cloud platforms and services. |
| Compatibility with third-party security solutions for enhanced threat protection. |
| Integration with network monitoring and analytics tools for real-time visibility. |
| Compatibility with on-premises data center solutions for seamless integration. |
| Integration with WAN optimization tools for enhanced performance. |
| Support for integration with network management and orchestration platforms. |

## 

## Scalability

|  |
| --- |
| **Scaling Considerations** |
| Scalability in terms of supporting a growing number of branch offices, remote sites, or locations. |
| The ability to scale the SASE solution to accommodate an increasing number of users and connected devices. |
| Scalability in handling higher volumes of network traffic as the organization grows. |
| The capability to efficiently manage a diverse set of applications and services over the network. |
| Scalability in connecting to and supporting a growing number of cloud services and applications. |
| The ability to easily expand available bandwidth to meet the increasing demands of the organization. |
| Scalability in integrating with existing network infrastructure, including legacy systems and technologies. |

## Performance

The managed SASE product must deliver reliable, efficient, and secure connectivity for users across various scenarios and locations.

|  |
| --- |
| **Performance Metric** |
| Specification of performance metrics such as throughput, latency, and packet loss. |
| Performance benchmarks and testing procedures to validate the performance of the SASE solution under various conditions. |
| Service level agreements (SLAs) for performance guarantees and uptime commitments. |

# Sify Deliverables

|  |  |
| --- | --- |
| **Requirement** | **Description** |
| Service portal | Portal to customer, able to view, configure, monitor WAN network performance of Sify and other providers |
| Capacity management | Measure WAN link utilization trends, create baselines and recommend customer on the actions taken – upgrade, downgrade |
| Transition and implementation services | Site survey, CRD, HLD and LLD. Deploy initial CPE devices across all sites. Perform MACD as and when changes required [bandwidth upgrade/downgrade, new features] |
| Proactive network monitoring | 24x7 Monitoring of network related faults and performance management. Able to view these alerts on self-service portal |
| Application visibility | Identify applications and sub-applications, report the performance of applications |
| Incident reporting and management | Trouble ticketing for all network related issues including other SP links. Detection of alerts from fault and performance management systems |
| Problem management | Diagnose, identify and isolate issues. Work on fix and workarounds with providers and SASE vendors |
| Configuration management | Configuration of managed CPE devices, auditing, backup of configuration, template-based config |
| Inventory management | Manages inventory of CPE devices, resources – IP address, VLAN etc. |
| Vendor management | Co-ordinate with vendors for issue reporting and resolution, faulty hardware management, recommended best practices |
| Change management | Scheduled network changes – changing software based on EOL, proactive identification of network issues and resolution, MACD of WAN links and bandwidth |
| Service desk | 24x7 technical support team to co-ordinate with customer for issue reporting and resolution |
| Hardware replacement time | Replacement of faulty hardware and components |
| Support systems | IAM, NTP, OOB management systems |
| Root cause analysis | Analysis of issues and identify root causes – including CPE and provider links |

# Ordering & Billing

|  |
| --- |
| Billing T&C |
| OT: One Time, 100% within 30 days of invoicing to the customer. |
| RC1 Option: Quarterly in Advance, within 30 days of invoicing to the customer. |
| RC2 Option: Yearly in Advance, within 30 days of invoicing to the customer. |

# CPQ Related Information

## Order Login Data for GUI

Key configuration information will be:

1. Managed SASE Service and SASE Build offerings from XXX as per OEM Platforms
2. Payment Terms agreed with the customer.
   1. OTC – One-time and upfront within 30 days of invoicing
   2. Recurring Charges – Quarterly/Annually in Advance within 30 days of invoicing
3. Characteristics (attributes) of the product that may alter the price can be defined as per below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **MANAGED SSE STRUCTURE ON CPQ** | | | | |
| **Platform** | Cisco | - | - | - |
| Netskope |
| Zscaler |
| Versa |
| **Contract Term** | 1 | - | - | - |
| 3 |
| 5 |
| **License Type** | User based | - | - | - |
| Bandwidth based |
| **Access Category** | Private Access | - | - | - |
| Public Access |
| **Tier** | <Cisco Tiers> | <Netskope Tiers> | <Zscaler Tiers> | <Versa Tiers> |
| Essentials |
| Advantage |
| Premier |
| **Quantity** | <Textbox> | - | - | - |
| **Change Management Options** | User Quantity increase/ decrease | BW upgrade/ downgrade | License Tier upgrade/ downgrade | Platform Change |
|  |

1. Product information (attributes) that is agreed with customer which will be delivered by Sify
2. Identify attributes that need to be printed in proposal
3. Validations on attributes or price

# Terms and Conditions

1. All pricing provided are exclusive of applicable taxes.
2. PO should be in name of SDSL, Chennai.
3. The contract period will be for 3 years or 5 years (applicable as per the PO).
4. The project delivery timelines will be 12 - 14 weeks from the date of Sify’s acceptance of a customer PO. Any delays caused due to Customer premises or infrastructure not being ready will result in extension of delivery timelines.
5. Additional Charges are applicable for any additional cabling requirements.
6. Any physical hardware damage caused by customer will incur hardware charges for replacement of faulty hardware (OTC). Customer must provide UPS Power and earthing for the any hardware required to offer SASE solution.
7. Early Termination charges are applicable for any services terminated within the contract period.
   1. In the event of performance degradation in Sify’s scope of work, which is brought to the notice of Sify in writing, Sify shall use all means available to rectify the same immediately and communicate to the customer on the action taken.
   2. If the performance degradation is not rectified within one month (1 month) from the time Sify acknowledges the customer complaint in writing/mail and if this performance degradation is repeated for the same site / network element for 3 consecutive times within a calendar quarter after Sify has taken necessary corrective measures, Customer has the option of terminating the contract with 1 month notice period for the affected site / network element.
   3. If the Customer chooses to terminate the entire contract for convenience or any other reason other than performance degradation of the service, the customer is liable to pay the annual recurring charges for the remaining period of the contract on a pro-rata basis. These charges will pertain to any Hardware and/or Software Licenses that have been specifically deployed for the use of the customer.
8. Any requirement of changing the SASE feature tier will result in associated change of commercials.
9. Any changes to the Solution design and configuration will result in the design change along with the revised commercials.
10. Cancellation or reschedule of site visits (for international locations) within 48 hours’ notice will incur additional charges.
11. The provisioning/commissioning of any unmanaged or managed network security services (apart from anything included within SASE Solution) is considered out of scope.
12. All Payment will be as per Sify's payment terms and conditions.
13. 24\*7 proactive monitoring and management of the network as defined in the solution document is included.
14. The customer will sign a scope of work document along with the PO and that will be considered as the reference for sign off on delivery of the project. Any scope not explicitly mentioned in the SOW will be considered out of scope of the project.
15. Only one site visit is factored for all on-site deployments and implementation for international locations, any additional site visits required will incur additional charges.
16. Installation SOW - basic rack & stack, uploading IOS/config file.
17. For International locations, Field Engineering services are factored for during business hours (9 AM - 5.00 PM Local Time Business Days). Out of business hours and Weekends and holidays will incur additional charges.
18. All Internal Cabling needs to be completed within 5 business days from the date of Service Readiness communicated by Sify. Failure to comply with the timeline will lead to the initiation of the billing for the SASE service automatically from the Sixth day.”

# SLA

Sify’s service offerings are SLA-driven and offer a good value proposition to corporations seeking to improve the return on their IT investments.

Network SLA

Uptime: > 99.50%

## Delivery SLA

The project delivery timelines will be 12 - 14 weeks from the date of Sify’s acceptance of a customer PO. Any delays caused due to Customer premises or infrastructure not being ready will result in extension of delivery timelines.

## Operation SLA

**Incident Management**

|  |  |
| --- | --- |
| **SLA Attributes** | **SLA Indicators** |
| Incident Notification | Severity 1 - 15 mins  Severity 2 - 30 mins  Severity 3 – Online |
| Incident Response | Severity 1 - 15 mins  Severity 2 - 30 mins  Severity 3 – 120 mins |
| Incident / Problem Resolution | Severity 1 – 4 Hours  Severity 2 – 8 hours  Severity 3 – 24 hours |
| Sify GNOC Availability | >99.90% |
| Sify Service Portal Availability | >99.50% |

**Note:** \* From the time of call / trouble ticket logged on to Sify’s portal

**Change Management**

|  |  |
| --- | --- |
| **SLA Attributes** | **SLA Indicators** |
| Any changes to the network / SASE setup | Customer will be informed 24 hours in advance or Customer must make a request 24 hours in advance of the changes to be executed (does not include hardware replacements) |
| Change Resolution | Severity 1 – 4 hours  Severity 2 – 8 hours  Severity 3 – 48 hours |

# User Experience

## User Training and Documentation

|  |  |
| --- | --- |
| **Component** | **Description** |
| Certification Programs | - Enrolling Engineering, Solutions, BD & Sales for certification programs. |
| Documentation | - Tiered & focused training decks to be created for different roles of stakeholders. |
| Regular Updates | - Keep training materials and documentation up to date with product releases. |
| Training Schedule | - Plan training sessions for different roles of stakeholders.  - Provide recordings for on-demand access. |
| Integration with LMS | - Integrate training modules with existing Learning Management System. |

# 

# Regulatory and Compliance Considerations

|  |  |
| --- | --- |
| **Regulatory & Compliance Considerations** | **Description** |
| Data Protection Laws | Adhere to India's data protection laws, including the Personal Data Protection Bill, ensuring the secure processing and storage of personal and sensitive information within the office-in-a-box product. |
| Cybersecurity Regulations | Comply with cybersecurity regulations and standards issued by the government or regulatory bodies. Implement robust cybersecurity measures to protect the office-in-a-box product from cyber threats and attacks. |
| IT Act, 2000 and Amendments | Align with the Information Technology Act, 2000, and its subsequent amendments. Ensure legal compliance with provisions related to electronic signatures, data protection, and electronic records. |
| Telecom Regulatory Authority of India (TRAI) Guidelines | Comply with TRAI guidelines, especially if the office-in-a-box product involves telecommunications services. Ensure adherence to regulations related to telecommunication and consumer protection. |
| Goods and Services Tax (GST) Compliance | Ensure compliance with GST regulations for invoicing and taxation if the office-in-a-box product involves the sale of goods or services. Adhere to GST guidelines and maintain accurate records for tax purposes. |
| Intellectual Property Rights (IPR) | Respect intellectual property rights, including patents, copyrights, and trademarks. Avoid unauthorized use of third-party intellectual property within the office-in-a-box product to prevent legal complications. |
| Local and State Regulations | Stay informed about local and state-specific regulations that may impact the operation of the office-in-a-box product. Comply with licensing requirements and other regional regulations applicable to the business. |
| Health and Safety Regulations | If applicable, adhere to health and safety regulations, especially if the office-in-a-box product involves physical components or equipment. Ensure a safe working environment for users. |
| Environmental Compliance | Consider environmental regulations and implement eco-friendly practices if the office-in-a-box product involves hardware components. Adhere to waste disposal guidelines and minimize environmental impact. |

# Timeline and Milestones

## Development Timeline

|  |  |
| --- | --- |
| **Milestones** | **Timeline** |
| Product Requirement Document | TBD |
| Internal Deck | TBD |
| Customer Facing Deck | TBD |
| Proposal Format | TBD |
| Price Book | TBD |
| Onboarding on CPQ | TBD |

# Risks and Mitigation Strategies

## Potential Risks

|  |  |  |
| --- | --- | --- |
| **Risk Category** | **Potential Risks** | **Impact** |
| Regulatory Risks | - Non-compliance with data protection regulations. | - Legal penalties and reputational damage. |
| - Data localization requirements. | - Impact on cross-border data transfers. |
| Project Management | - Scope creep and changing requirements. | - Delays, increased costs, and resource strain. |
| - Untrained or poorly trained implementation/ support resources | - Deadline overruns, service outages and penalties |
| Vendor/Partner Risks | - Dependence on a single OEM for product delivery. | - Delays and potential disruptions. |
| Adoption Risks | - Resistance to adoption of the product among end-users. | - Poor adoption rates and underutilization. |

## Mitigation Strategies

|  |  |  |
| --- | --- | --- |
| **Risk Category** | **Potential Risks** | **Mitigation Strategies** |
| Regulatory Risks | - Non-compliance with data protection regulations. | - Stay informed about relevant regulations and ensure compliance. |
| - Data localization requirements. | - Implement data localization strategies and legal compliance. |
| Project Management | - Scope creep and changing requirements. | - Establish a robust change control process and communicate changes. |
| - Untrained or poorly trained implementation/ support resources | - Ensure availability of trained resources for each project. |
| Vendor/Partner Risks | - Dependence on a single OEM for product delivery. | - Maintain constant communication with OEM on product lifecycle. |
| Adoption Risks | - Resistance to adoption of the product among end-users. | - Conduct user training programs and create awareness campaigns. |

# Stakeholder Approval

## Review and Approval

|  |  |
| --- | --- |
| Document Owners | Suresh Gummaraju |
| Saurabh Kumar Acharya |
| Approved By | Pranesh Babu Khyatasandra |
| Ramakrishna Kotha |
| Anuj Malhotra |
| Joseph Abraham |
| Mohan Raj S |
| Hari Hara Moorthy |
| Suresh Gummaraju |

# Appendices

## Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Quality of Service (QoS) | A set of techniques used to manage network resources, prioritize certain types of traffic, and ensure a consistent level of service for critical applications. |
| Regulatory Compliance | Adherence to laws, regulations, and industry standards related to data protection, privacy, and other relevant requirements. |
| Cyber Threats | Malicious activities and attacks aimed at exploiting vulnerabilities in computer systems, networks, and data. |
| Centralized Management | The ability to monitor, configure, and control network devices from a central location, providing efficiency and ease of administration. |
| Scalability | The capability of a system or network to handle increased demand by adding resources or adapting to accommodate a growing user base. |
| Reliability | The ability of a system or network to consistently perform its intended functions without failures or interruptions. |
| Analytics and Reporting | Tools and capabilities for collecting and analyzing data, generating reports, and gaining insights into network performance and user behavior. |
| Compliance Adherence | Conforming to established rules, regulations, and standards relevant to a specific industry or jurisdiction. |
| Digital Transformation | The integration of digital technologies into various aspects of business operations, often leading to fundamental changes in how businesses operate and deliver value. |
| IoT (Internet of Things) | The network of interconnected devices and objects that can communicate and exchange data, contributing to automation and smart functionality. |
| Remote Work | Work conducted away from a traditional office environment, often facilitated by digital technologies and connectivity. |
| Mesh Networking | A network topology where each node (device) is connected to multiple other nodes, forming a flexible and resilient communication infrastructure. |
| Managed Service Provider (MSP) | An organization or company that provides managed services, such as managed SASE, to clients, often on a subscription or contractual basis. |
| 5G Technology | The fifth generation of cellular technology, offering increased data transfer speeds, lower latency, and improved connectivity for mobile devices. |

Top of Form