Secure, Browser-Based and Desktop app based Workspace - Datasheet

Oneable is a secure, browser-based workspace solution designed to optimize remote, hybrid, office in cloud, and in-office work environments. It enhances productivity, protects intellectual property, and simplifies governance through centralized password management and data security controls. Oneable's flexible architecture supports cloud, on-premises, and multi-cloud environments, allowing businesses to scale resources efficiently. Its non-intrusive productivity measurement promotes work-life balance while ensuring compliance with industry regulations like GDPR and HIPAA. With a focus on seamless integration, low-bandwidth performance, and cost-effective operations, Oneable is an ideal solution for modern enterprises embracing digital transformation and secure remote collaboration.

Oneable offers a comprehensive solution for secure remote access and digital workspace management. Its unified platform integrates application virtualization, secure VDI, and centralized identity management, providing seamless access to critical resources without the need for multiple third-party tools. With features like multi-factor authentication (MFA), single sign-on (SSO), and zero trust access, Oneable ensures robust security for remote, and hybrid workers. Its thin-client support and efficient resource allocation minimize hardware investments while maintaining performance across diverse devices. Designed for scalability and flexibility, Oneable simplifies IT management, delivering a single, integrated solution for modern enterprise environments.

Oneable's workspace is highly flexible, providing seamless access to web, SaaS, client-server, legacy applications, and virtual desktops and applications. It integrates easily with existing infrastructure, offering a unified, secure platform for all business-critical tools. Ideal for organizations of any size, Oneable simplifies operations and supports digital transformation.

Oneable is a comprehensive solution offering centralized access to applications and servers, secure VDI access, and centrally managed passwords. It combines remote access, VDI, MFA, identity management, and SSO in one unified platform, simplifying management and ensuring secure, seamless access to critical business resources across devices and locations.

Increase productivity with non-intrusive productivity Monitoring

Promote BYOD, Go-green with thin clients or even Zero clients

Protect Intellectual property, Reduce data leaks

Reduce overcosts and TCO, by elimiating Endpoint protection tools, DLP, MDM on endpoints Optimize Opex

Key Features

Hypersecure Workspace

Oneable's Hyper Secure Workspace provides robust security for enterprises by centralizing access to applications and data. It leverages advanced encryption, multi-factor authentication (MFA), and Zero Trust principles to ensure that only authorized users can access critical resources. Features like session recording, data leak prevention, and content protection further enhance security by disabling risky actions such as screenshots, file downloads, and unauthorized sharing. With centralized control over devices and applications, Oneable provides enterprises with a highly secure, scalable environment that protects intellectual property and sensitive information, making it ideal for industries with stringent security requirements.

Cloud Delivered WS

Oneable's Cloud-Delivered Workspace enables organizations to provide secure access to applications and desktops from anywhere, without the need for on-premises infrastructure. By hosting applications in the cloud, businesses can offer remote workers instant, browser-based access to their workspace, reducing the need for expensive hardware. Oneable's cloud architecture ensures low-latency performance even in low-bandwidth environments, providing a seamless user experience. The cloud-based workspace simplifies IT management by allowing centralized updates, patching, and monitoring, making it an efficient solution for organizations embracing remote work or seeking to reduce their data center footprint.

Data Leak Lockdown

Oneable's Data Leak Lockdown feature ensures that sensitive data remains protected at all times by preventing unauthorized actions that could compromise intellectual property. Features like disabling copy-paste, blocking screen sharing, and preventing file downloads ensure that data is only accessible within the secure workspace environment. Oneable also tracks and records user activity through detailed logs, enabling organizations to monitor potential breaches and comply with regulatory requirements. This robust data protection ensures that confidential information is safeguarded against both internal and external threats, providing peace of mind for businesses handling sensitive data.

100% End Point Compliance

Oneable ensures 100% Endpoint Compliance by enforcing strict security policies on all devices accessing the workspace. Only compliant devices that meet organizational security requirements, such as encryption, antivirus protection, and firewall settings, are granted access. Oneable continuously monitors and validates device compliance, blocking unauthorized or non-compliant devices from accessing corporate resources. This ensures that all endpoints, whether personal or company-owned, adhere to security protocols, mitigating the risk of breaches. This feature is especially crucial for organizations with distributed or remote workforces, ensuring consistent security across all devices.

Secure BYOD Enabler

Oneable's Secure BYOD (Bring Your Own Device) Enabler allows employees to securely access corporate resources from their personal devices without compromising data security. The platform applies strict security controls such as encrypted connections, MFA, and device compliance checks before granting access. Sensitive data is never stored on personal devices, and actions like copy-paste and file downloads are restricted to prevent data leaks. With Oneable, organizations can confidently implement BYOD policies, enabling employees to work flexibly while ensuring that company data remains secure and compliant with organizational policies.

Secure Access Gateway

Oneable's Secure Access Gateway acts as a central entry point for accessing all corporate applications and resources, whether hosted on-premises or in the cloud. It employs strong encryption and zero-trust authentication to verify users and devices before granting access. By consolidating access into a single gateway, Oneable simplifies IT management while providing a secure, seamless user experience. The gateway also integrates with VDI, SaaS applications, and legacy systems, ensuring that users have secure, consistent access to all their work tools. This centralized access point strengthens security and reduces the complexity of managing multiple access points.

Productivity Enabler

Oneable enhances productivity by providing employees with centralized, streamlined access to all necessary applications and resources, eliminating the need for multiple logins and reducing context switching. With features like seamless VDI access, secure SaaS integration, and the ability to work from any device or location, employees can maintain productivity without sacrificing security. Oneable's non-intrusive productivity tracking ensures that businesses can monitor performance without disrupting employee workflows, promoting a healthy work-life balance. By optimizing resource access and removing inefficiencies, Oneable empowers organizations to enhance overall productivity while maintaining robust security controls.

Secure Collaboration

Oneable facilitates secure collaboration across distributed teams by providing a unified workspace where employees can work together in real time, while ensuring data security and compliance. Features like encrypted audio/video conferencing, secure document sharing, and session recording make it easy for teams to collaborate on projects, regardless of their location. With granular access controls, organizations can restrict data sharing and limit access to sensitive information, ensuring that intellectual property is protected. Oneable's collaboration tools integrate seamlessly with popular applications like Microsoft Teams, Zoom, and Google Workspace, creating a secure, efficient environment for teamwork.

Launch Local for SaaS Applications with Data Protection

Oneable's Launch Local feature allows users to access SaaS applications like Google Workspace and Office 365 directly on their local machines without requiring additional infrastructure. This functionality ensures that businesses can avoid costly investments in hardware or virtualization systems while maintaining a secure environment. Data protection is enforced through features like copy-paste restrictions, download blocking, and watermarking to prevent data leaks. The watermarking feature adds a visible identifier to documents and screens during sessions, making it easier to track and deter unauthorized sharing or screenshots, further safeguarding sensitive information.

Enterprise SSO

Oneable's Enterprise Single Sign-On (SSO) simplifies access to all business applications by allowing users to log in once and gain access to multiple platforms without needing to re-enter credentials. By integrating with existing identity providers, Oneable provides a seamless authentication experience across cloud, on-premises, and SaaS applications. SSO reduces password fatigue and the risk of credential-related breaches, while also streamlining user management for IT teams. With centralized authentication, organizations can enforce stronger security policies, such as MFA and session monitoring, while improving the user experience and reducing administrative overhead.

Built-In Data Privacy

Oneable incorporates Built-In Data Privacy features to ensure that sensitive information is always protected. The platform is designed to comply with stringent data privacy regulations like GDPR, HIPAA, and PCI-DSS, offering tools such as data masking, encryption, and anonymization to prevent unauthorized access to personal data. All user activities are logged and monitored for compliance, ensuring transparency and accountability. By integrating privacy into the core architecture, Oneable helps businesses avoid costly data breaches and regulatory fines while maintaining trust with customers and employees.

Infrastructure Optimization

Oneable optimizes infrastructure usage by enabling efficient resource allocation and reducing the need for expensive hardware investments. Its containerized architecture allows organizations to scale both horizontally and vertically, ensuring that resources are used effectively. Oneable's support for thin clients, cloud environments, and virtual desktops reduces the burden on physical infrastructure, streamlining IT operations. This optimization not only improves performance but also enables businesses to scale their operations as needed, without overprovisioning or wasting resources, making it an ideal solution for growing enterprises looking to optimize their IT investments.

Cost optimization

Oneable helps organizations reduce costs by consolidating multiple IT functions into a single platform. By integrating remote access, VDI, MFA, SSO, and secure password management, Oneable eliminates the need for multiple vendor solutions, reducing licensing and support costs. Its efficient resource management and support for thin clients further lower hardware and maintenance expenses. Additionally, Oneable's cloud-delivered workspace reduces the need for costly on-premises infrastructure, optimizing operational expenses while maintaining performance. Overall, Oneable provides a cost-effective solution that maximizes ROI while streamlining IT operations and reducing overhead.

Centralized Password Management

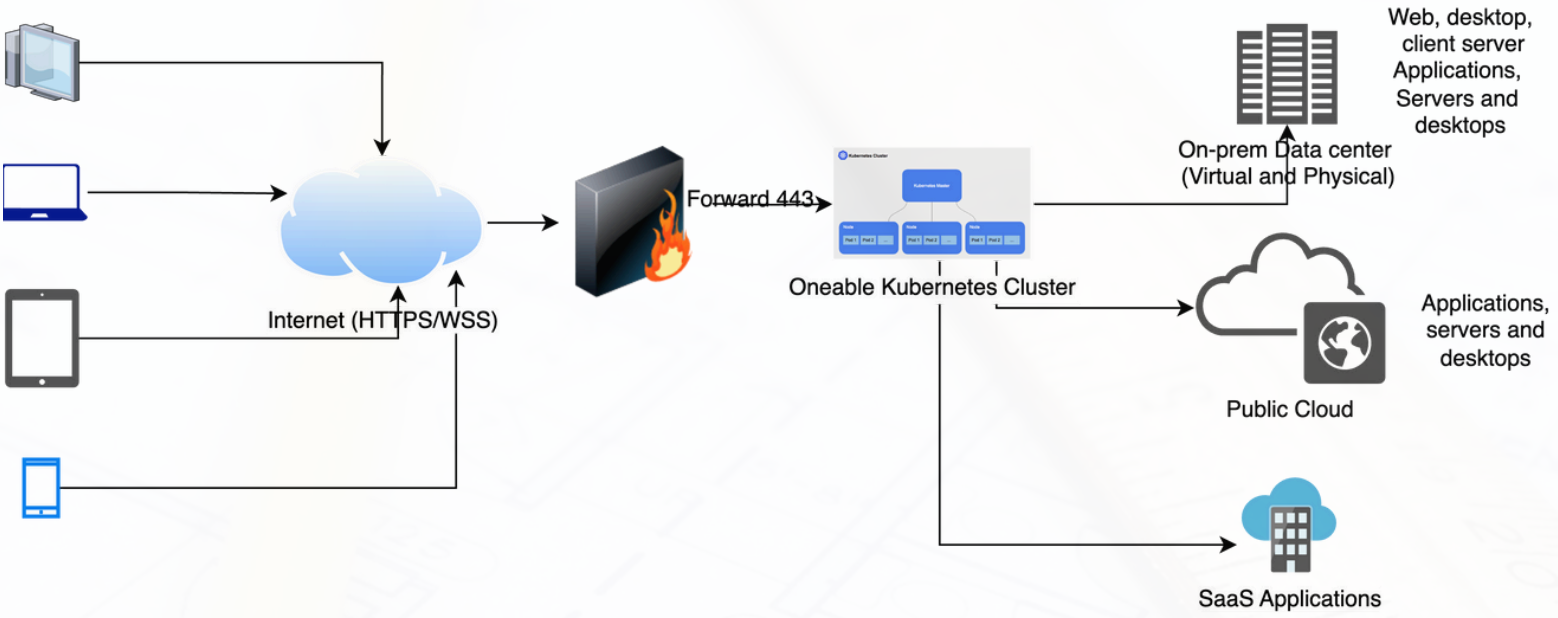
Oneable's centralized password management eliminates the need for Privileged User Password Management (PUPM) and Privileged Access Management (PAM) tools by providing a secure, integrated solution for handling credentials. It stores and manages passwords in a secure vault, automatically logging users into applications without exposing credentials. This reduces the risk of password-related security breaches and simplifies access for users. Centralized management allows IT teams to enforce password policies, rotate credentials, and monitor access in real time, improving security while reducing the complexity and cost associated with traditional PAM/PUPM solutions.

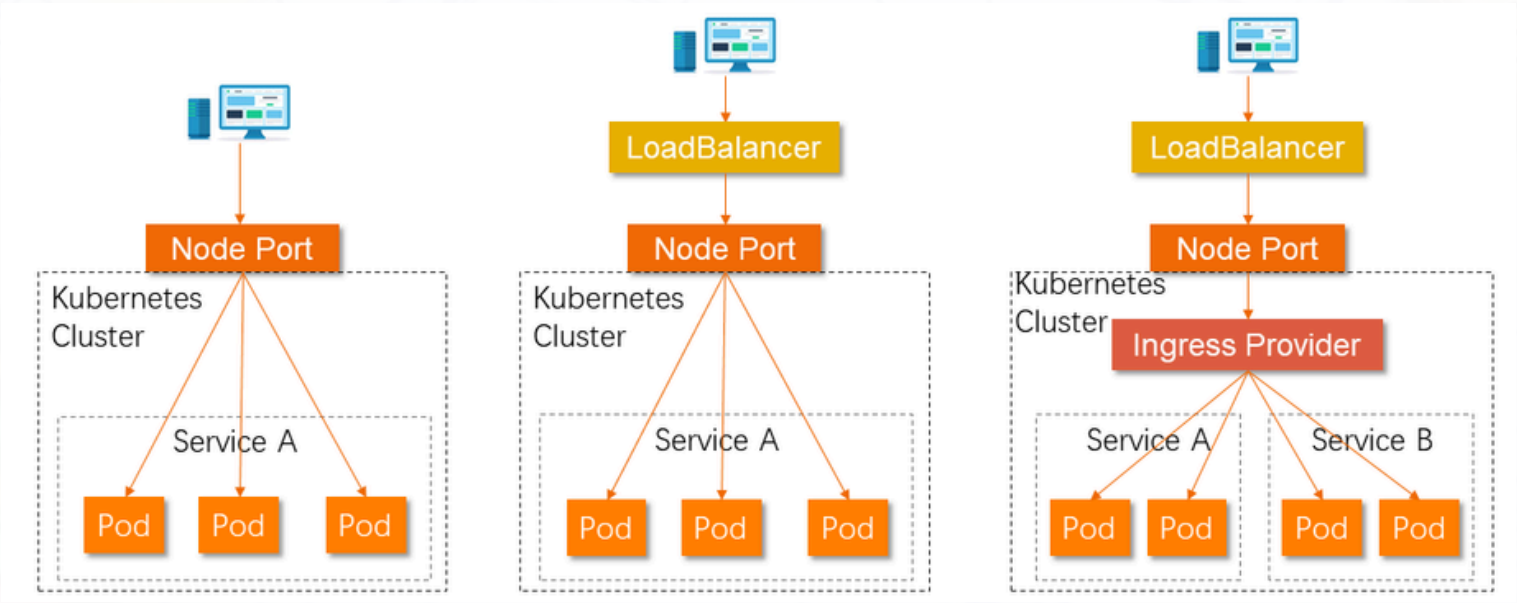
Centralized Operations

Oneable provides a single platform for managing all IT operations, including application access, device management, security policies, and user authentication. This centralization simplifies the management of remote and hybrid work environments by providing IT teams with complete visibility and control over the organization's infrastructure. By consolidating multiple tools into one interface, Oneable reduces operational complexity, improves security, and enhances the efficiency of day-to-day management tasks. This centralized approach ensures consistent enforcement of policies across all devices and users, helping organizations maintain compliance while minimizing the administrative burden.

OneAble

Architecture And Deployment





OneAble

Data Sheet

Application and server/Desktop Publishing	**Access Security**
Session-based Access	TLS 1.0, 1.1, 1.2 and Above
Windows RDS 2008, 2012, 2016, 2019. 2022	Encryption: AES, and PKI with RSA
Ubuntu. CentOS, RHEL- SSH	Authentication: SHA,RSA
Ubuntu, CentOS, RHEL- XRDP	4096 RSA Key for PKI
Windows Workstation 7/8/10/11, Multi-session windows desktop	Users do not know their own passwords for servers or applications
Linux: Ubuntu, CentOS	**Entitlements**
Physical and Virtual Machines Support	Users to machine and application mapping
Any VM (Xen, Parallels, VMWare, KVM, Nutanix, Hyper-V etc)	User store users and Machine users are mapped unless it is Active directory Authentication
Any Cloud, Azure, GCP, Oracle, AWS, Alibaba, IBM, etc.	Google workspace and O365 Users' passwords managed and securely transferred to the client
Physical machines Arm, X64, X86	Users imported from thirdparty like Okta and AzureAD (Entra ID) and Google workspace or 0365 based on OUs
Applications	**Access Methods**
All web based, TCP, UDP, Client server applications	Desktop applications for PC, Mac and Ubuntu based OS
Windows file shares and drive mapping on the server side	Browser based access on any browser
Dynamic port-based applications	No VPN required Or VPN is Optional. Complete Https/WSS based access
Application server's load balancing	**Time metrics and productivity Monitoring**
Session caching for load-balanced applications	Non-intrusive productivity and time metrics monitoring
VoIP both remote and local	configurable for who can access the productivity data
FTP remote	Detailed reports based on application access, server access, total time on a daily, monthly and yearly access
File share - remote	Session recording of the user serssions based on group of users, user, and application
VDIs and Hosted Applications	**Deployment**
O365, Gsuite, Sales force both access from remote and local	Scalable horizontally and vertically
	Kubernetes cluster based deployment for Self healing and auto scaling

OneAble

Data Sheet

Device Management	Deployment
Device management on Access devices is optional	Runs on Ubuntu 22.04
No installation required for browser based access	Can run on Virtual infrastructure as well.
Desktop applications supported on Mac and Windows	Can deploy multi-master multi-worker based on Load, and high availability
MFA for users to Login	**Authorization**
Integrated with Okta, Azure AD (Entra ID), and active directory for authentication	Domain And network policies enforced as is
web based administration console for operations and system administration	User authentication and Role Based
System Management	Display only provisioned applications on a need to know basis
Logging and reporting user logs	Time based and shift based restriction policies
Hot Warm and cold databases built in	Support for OKTA and other SAML based authentication and authorization
Automated and Manual backup	Automatic fetching of group information from AD and LDAP
Application Publishing Features	**Authentication**
Remote browser application	2FA based
Launch in single session or multiple sessions	Supports OKTA, AD Azure AD (Entra ID) and other SAML based authentication
Launch Local for SaaS applications	Password reset and password rotation support
Custom UI for customers	Protected access to SaaS based applications
Water marking	Passwords automatically managed on server
Watermarking configuration on server	Passwords injected securely if accessing SaaS applications from local machine
Applied to launch local and remote applications or server accesss	Integrates with Google Workspace or O365
Collaboration	Context based access based on IP address is not required
Private and public channel creation	Additional Hardware is not required for SaaS application access
Multiple workspace creation for collaboration	**Project Management and Task Management**
Completely On-premise solution	Create and manage the tasks
Video and audio calls	Push the tasks from Oneable to Jira
Group and individual chat	Customizable to integrate with other project management applications
Screen sharing with full desktop or particular application	Time spent on task automatically captured and pushed to Jira
Automated Timesheet filling	Better project base lining
Time spent on tasks is automatically captured	Better grip on product backlog
Manual entry to add additional tasks	
Approval workflow	
Can be integrated with other timesheet applications	

Empower, Secure & Save: Elevate Your Business with OneAble, Where Security Meets Efficiency and Productivity Soars.

OneAble

sashankp@oneable.ai

+919849273680