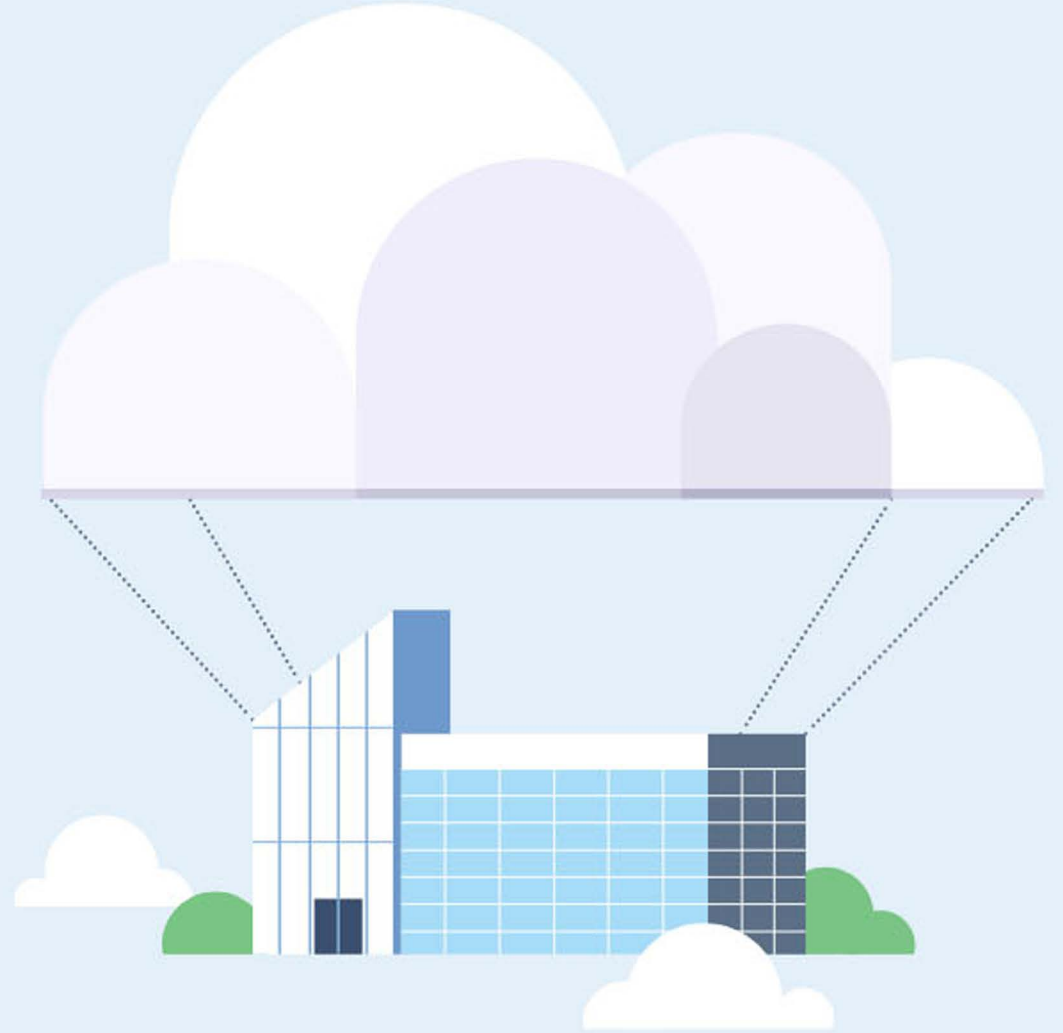


ManageEngine 

**Give your IT the
cloud advantage**



ManageEngine 

Aligning IT with business

Comprehensive IT management software for all your business needs



Disclaimer

This presentation is confidential and is intended, among other things, to present a general overview of Zoho's ("Zoho") products and services. This presentation is provided for informational purposes only. The contents are not to be reproduced or distributed to the public or press. While the information in this presentation is believed to be accurate and reliable, Zoho makes no representation regarding, and assumes no responsibility or liability for, the accuracy or completeness of, or any errors or omissions in, any information contained herein.

ManageEngine is the enterprise IT Management software division of ZOHU Corporation

Privately held and profitable since inception



(Est. 1996)



(1996-2021)

Enterprise Internet of Things & Unified Network Management Solutions



(Est. 2002)

Enterprise IT Management Solutions



(Est. 2005)

Application for Business, Collaboration, and Productivity



(Est. 2021)

Workflow orchestration software



ManageEngine:

A bootstrapped, private, and profitable company

19+

years in the
industry

180,000+

Organizations across the
globe use our products

90+

products and free tools for
IT management

3,500+

ManageEngine
employees

190+

countries

ZOHOO Corp. Offices Worldwide



BRINGING IT TOGETHER



Available for
Enterprise IT | Managed service providers (MSPs)
as
Self-hosted on-premises
Self-hosted in public cloud (AWS, Azure)
Zoho Cloud-native

Enterprise service management

- Full-stack ITSM suite
- IT asset management with CMDB
- Knowledge base with user self-service
- Built-in and custom workflows
- Orchestration of all IT management functions
- Service management for all departments
- Reporting and analytics

Identity & access management

- Identity governance and administration
- Privileged identity and access management
- AD and Azure AD management and auditing
- SSO for on-premises and cloud apps with MFA
- Password self-service and sync
- Microsoft 365 & Exchange management and auditing
- AD & Exchange - backup and recovery
- SSH and SSL certificate management

Security information & event management

- Unified SIEM for cloud and on-premises
- AI driven user and entity behavior analytics
- Firewall log analytics
- Data leakage prevention and risk assessment
- Regulatory and privacy compliance

Unified endpoint management & security

- Desktop and mobile device management
- Patch management
- Endpoint device security
- OS and software deployment
- Remote monitoring and management
- Web browser security
- Monitoring and control of peripheral devices

IT operations management

- Network, server and application performance monitoring
- Bandwidth monitoring with traffic analysis
- Network change & configuration management
- Application discovery & dependency mapping
- Cloud cost and infrastructure monitoring
- End user experience monitoring
- AIOps

Advanced IT analytics

- Self-service IT analytics
- Data visualization and business intelligence for IT
- Hundreds of built-in reports and dashboards
- Instant, flexible report creation
- Out of the box support for multiple data sources

ManageEngine cloud solutions

can be classified into:



SaaS-based applications that are hosted on Zoho's cloud infrastructure



Applications that can be self-hosted on a public cloud ([AWS](#) and [Azure](#))



Cloud monitoring and reporting solutions installed on-premises

The cloud advantage



SaaS applications are hosted in Zoho's own data centers



Our [security, privacy, and compliance practices](#) are built on the foundation of trust

The emphasis on data centers

- ManageEngine's SaaS based IT management solutions are hosted on Zoho's cloud platform, a complete suite of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) tools and services
- These SaaS based solutions offer multiple benefits which includes:
 - Multi-tenancy
 - High availability
 - Ground up applications
 - Effortless Scalability
 - Seamless upgrades
- Zoho Corporation has ten data centers located in the US (Seattle and Dallas), Europe (Dublin and Amsterdam), China (Beijing and Shanghai), India (Chennai and Mumbai), and Australia (Sydney and Melbourne)
- Customers can choose their preferred data center when they sign up for ManageEngine's cloud services

ZOHO Corp. Datacenters Worldwide





Data center security guaranteed

To mitigate security and data protection risks, the data centers are:

- Hosted in some of the most secure facilities available today; each location is undisclosed and protected from physical and logical attacks, as well as natural disasters
- Equipped with around-the-clock security, video monitoring, controlled entrances, biometric and two-factor authentication systems, and bullet-resistant walls
- Accessed on a need-only basis that's limited to select employees with the highest clearance
- Guarded by industry-standard fire prevention and control systems; the servers are backed by N+2 redundant HVAC systems and temperature control systems

Availability: The vital function

- User data is backed-up periodically across multiple servers and mirrored in a separate geographic location for disaster recovery and business continuity purposes, ensuring high availability
- Customer data is spread over geographically diverse data centers such that data in one DC is replicated in another. This ensures that if one DC fails, operations carry on smoothly with minimal or no loss of time

Cloud security and privacy

- Dedicated team assigned to run privacy programs, internal audits, and awareness training for employees
- All cloud services comply with industry standards to ensure data security and privacy
- Privacy and security certifications that ManageEngine's cloud offerings comply with:

Our compliance certifications



ISO/IEC 27018:

We follow guidelines for implementing measures to safeguard the PII that is processed in a public cloud



ISO/IEC 27001

ManageEngine has earned, the most widely recognized independent international security standards, the ISO/IEC 27001:2013, for Applications, Systems, People, Technology, and Processes



ISO/IEC 27017

ManageEngine is certified with ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services



ISO/IEC 27701

ManageEngine and its solutions are fully compliant with the requirements of ISO/IEC 27701. This certification enhances the existing Information Security Management System (ISMS) and helps continually improve the Privacy Information Management System (PIMS), thereby enables us to demonstrate compliance with various privacy regulations



SOC 2

SOC 2 Type II

The design and operating effectiveness of our controls meet the AICPA's Trust Services Principles criteria



GDPR

GDPR

Our cloud offerings have privacy features that comply with the GDPR, and our processing of customer data adheres to the GDPR's data protection principles

PRIVACY FEEDBACK

Powered by TRUSTe

TRUSTe

TRUSTe Review

Our processes and policies have been reviewed by TRUSTe for compliance with their program requirements for all the controls including that of privacy

Data center compliance certifications

US

Central Washington

SOC 1 TYPE II | SOC 2 TYPE II | HIPAA | PCI DSS

Dallas

SOC 1 TYPE II | SOC 2 TYPE II | SOC 3

India

Chennai

ISO 27001

Mumbai

ISO 27001 | ANSI/TIA ISO 20000-1:2011 | SOC 1 TYPE II | SOC 2 TYPE II

Australia

Sydney

SOC 1 TYPE II | SOC 2 TYPE II | ISO 27001

Melbourne

SOC 1 TYPE II | SOC 2 TYPE II | ISO 27001

Europe

Amsterdam

ISO 27001 | ISO 22301

Dublin

ISO 9001 | ISO 27001

China

Shanghai

ISO 27001 | ISO 22301 | CNAS

Beijing

ISO 9001 | ISO 22301 | ISO 27001



**SaaS-based IT management solutions that are
hosted on Zoho's cloud infrastructure**

1. **ServiceDesk Plus:** Full-stack service management for enterprises
2. **Identity Manager Plus:** Secure single sign-on for enterprise applications
3. **Desktop Central:** Unified endpoint management and security
4. **Mobile Device Manager Plus:** Comprehensive mobile device management
5. **Mobile Device Manager Plus MSP:** Comprehensive mobile device management for MSPs
6. **Remote Access Plus:** Enterprise remote access
7. **Patch Manager Plus:** Automated multi-OS patch management
8. **Log360 Cloud:** Secure log management from the cloud
9. **Site24x7:** Full-stack monitoring for IT admins, DevOps, and SREs
10. **Site24x7 (MSP):** Infrastructure, performance and end user experience monitoring for MSPs
11. **Site24x7 StatusIQ:** Status pages for real-time status and incident communication
12. **Site24x7 CloudSpend:** Cloud cost management for modern software teams
13. **AlarmsOne:** Centralized IT alert management

ServiceDesk Plus

Full-stack service management
for enterprises





Why ServiceDesk Plus?

- Recommended process workflows and features available out-of-the-box
- Highly customizable and scalable for different process maturities
- Tight, contextual integrations with other IT management and business apps
- Flexible, easy-to-use interface with a short learning curve
- Leverages the latest in technology, including virtual assistants and AI capabilities
- Extends proven IT best practices to non-IT departments in an organization

Implement ITSM best practices for support operations

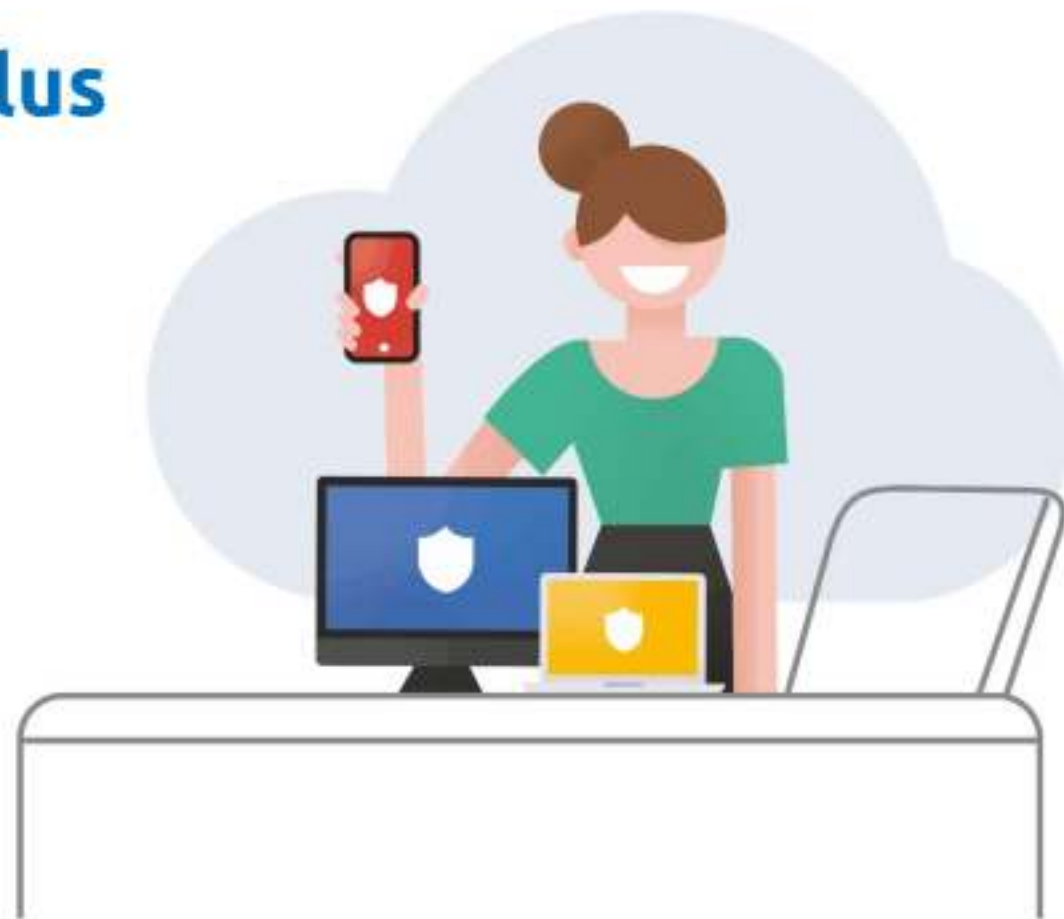
- Incident management
- Service request management
- Knowledge management
- Problem management
- Change management
- Project management
- Release management
- Asset management
- Reporting
- Integrations

Integrations

- Active Directory
- SAML authentication
- Microsoft Azure
- Zoho Analytics
- Jira
- Microsoft 365 Calendar
- Microsoft Teams
- Slack
- Zapier

Mobile Device Manager Plus

Comprehensive mobile device
management



Why Mobile Device Manager Plus?

- Manage multiple mobile platforms and device types from a single interface
- Segregate corporate and personal data on BYOD deployments to ensure user privacy
- Silently install, uninstall, or update apps, and test enterprise apps before deployment
- Secure data at rest, in transit, and in use with enhanced data loss prevention (DLP) capabilities
- Configure corporate email accounts, and securely distribute, save, and view sensitive business content on managed mobile devices
- Remotely troubleshoot devices, and create a geofence to automatically locate, lock, or wipe non-compliant devices remotely
- Blacklist or whitelist apps, and test, approve, automate, and schedule OS updates



Empower your enterprise workforce with the power of mobility

- Mobile device management
- Mobile app management
- Mobile security management
- Mobile email management
- Mobile content management
- Mobile asset management
- Remote troubleshooting
- Containerization
- Location tracking
- OS update management
- Kiosk mode

Integrations

- ManageEngine ServiceDesk Plus
- ManageEngine AssetExplorer
- Zoho CRM
- Zoho Creator
- Jira Service Desk
- Spiceworks
- ServiceNow
- Zendesk Support

Mobile Device Manager Plus MSP*

Comprehensive mobile device management
for MSPs



* - same feature set as [Mobile Device Manager Plus](#), mentioned in the previous 3 slides

Log360 Cloud

Secure log management from the cloud



Why Log360 Cloud?

- Helps meet high bandwidth and storage requirements related to SIEM deployments
- Enables better agility, and in turn, better enterprise security
- Installs quickly and offers analytical inferences within minutes of installation

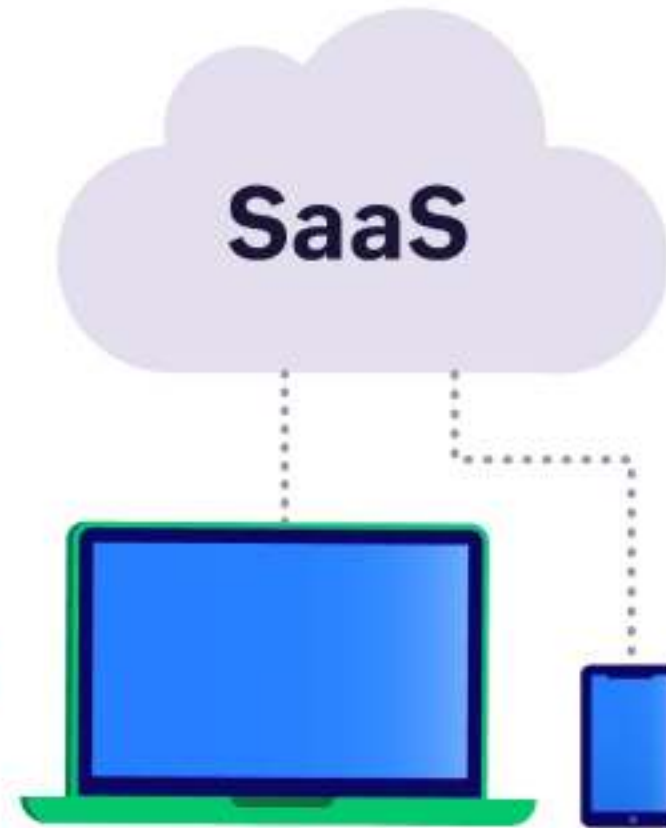


Discover threats quickly with comprehensive log collection and monitoring

- Secure log data management
- Forensic analysis and post-breach analyses with a super fast log search engine
- Comprehensive security auditing reports that give information on "who did what from where and when"
- Integrated IT compliance management module that makes security auditing a lot easier

Desktop Central

Unified endpoint management
and security



Why Desktop Central?

- Automate patch deployment related to OS and third-party applications
- Simplify software distribution to install and uninstall software using built-in templates
- Instantly troubleshoot remote devices via remote desktop sharing
- Monitor and manage all of your IT assets
- Simplify device and application management
- Deploy security and management configurations to all network users and devices
- Define roles with specific privileges, and delegate users to these roles
- Monitor and detect anomalies by looking at the numerous reports offered
- Improve employee productivity by blacklisting unwanted applications



Enable 360-degree endpoint management with cloud-based UEM

- Patch management
- Software deployment
- Asset management
- Remote control
- Configurations management
- Mobile device management
- Modern management
- USB device management
- Reporting and analysis
- Power management
- User administration
- Service packs deployment

Patch Manager Plus

Automated multi-OS patch management



Why Patch Manager Plus?

- Scan endpoints to detect missing patches
- Pre-test and approve patches before deployment to mitigate security risks
- Automate patch management to get endpoints on various OSs patched in minimal time
- Secure your network by applying timely patches to OSs, related applications, and over 350 third-party apps
- Customize deployment policies to meet your enterprise's patching needs
- Use powerful audits and reporting to better analyze and fix vulnerabilities faster



Gain complete visibility and control over your patching

- Automated patch management
- Option to test and approve patches
- Customized deployment policies
- Dynamic monitoring and reporting
- Cross-platform support
- Patch compliance



Integrations

- Spiceworks
- Microsoft 365
- Microsoft Outlook

Remote Access Plus

Enterprise remote access



Why Remote Access Plus?

- Access computers connected to multiple monitors, and track sessions by recording them
- Establish clear communication channels with voice, video, and text chat support
- Wake computers on LAN, fetch idle computers, and remotely shut down machines
- Monitor users by shadowing remote sessions
- HIPAA, PCI, and trade practice compliant remote control
- Tailor roles and prevent users from accessing information beyond their privileges
- Track and measure everything with audit-ready logs and real-time reporting



Simplify remote troubleshooting

- Advanced remote control
- Granular control over computers
- Voice and video chat for collaboration
- Wake on LAN to instantly turn remote computers on
- Over 12 handy diagnostic tools
- Secure and comprehensive assistance



Integrations

- Spiceworks

Identity Manager Plus

Secure single sign-on for enterprise applications



Why Identity Manager Plus?

- Provide users secure, one-click access to all their applications via SAML-based SSO
- Automate user provisioning and deprovisioning for cloud applications using SCIM
- Centrally manage identities from multiple sources with the built-in directory
- Track who accessed which applications, from where, and when
- Gain insights into the most used applications, top users, inactive users, and more
- Reduce costly password-related help desk calls, and improve the user experience

Secure single sign-on for enterprise applications

- Centralized access management
- Standardized SAML-based SSO
- Auditing of application usage and access
- Leverages existing identities
- Enables SSO to custom or in-house SAML applications

Integrations

- SSO support to hundreds of enterprise applications
- SCIM-based automated user provisioning support for multiple cloud applications

Supported directories

- Microsoft 365
- Salesforce
- G Suite
- Dropbox
- Slack
- Zoho

AlarmsOne

Centralized IT alert management



Why AlarmsOne?

- Centralize your IT alarms
- Resolve issues fast with real-time alerts and multi-channel notifications
- Get in-depth visibility with intelligent classification and easy filtering
- Manage your workforce effectively with on-call schedules
- Notify the right person at the right time using escalations
- Manage alerts from anywhere



Manage alerts from all your IT management tools in one place

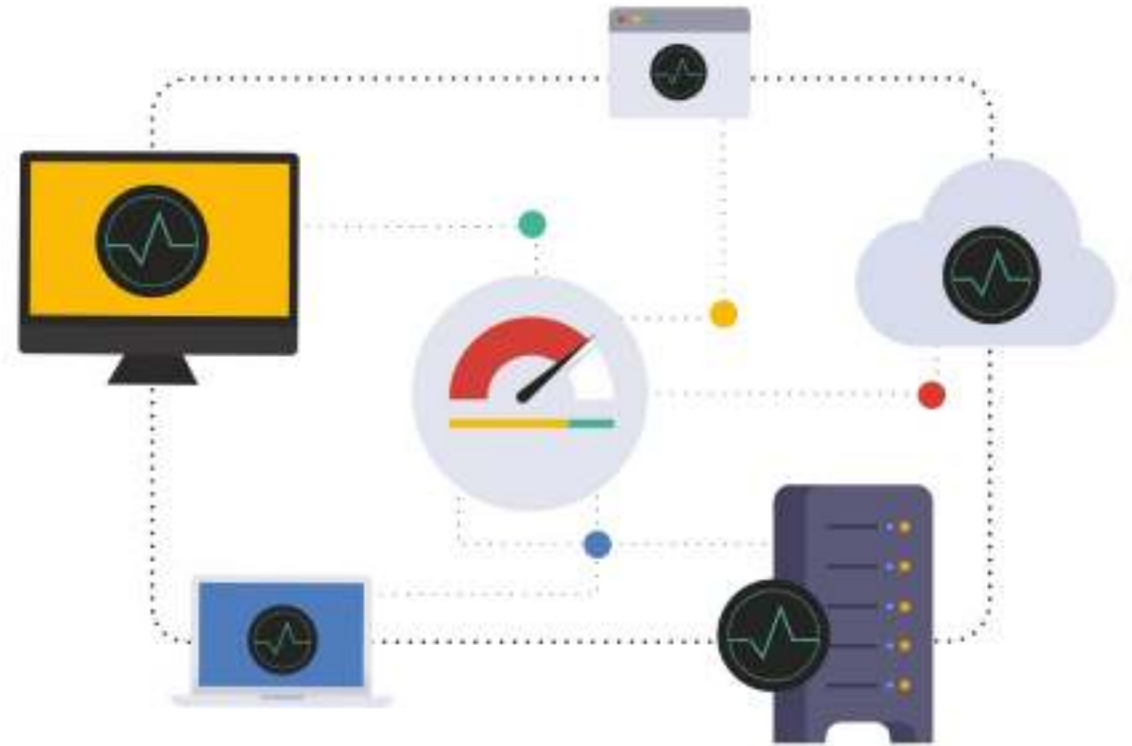
- Role-based access
- Noise reduction
- Alarm escalations
- Auto-remediation
- Alarm modifier
- Criteria-based alerting
- Real-time collaboration and alarm scheduling

Integrations

- **Over 60 integrations with multiple tools across various categories of solutions**
- **Integrations with:**
 - On-premises monitoring tools
 - SaaS monitoring tools
 - Log analysis and management tools
 - Team collaboration tools
 - Help desk tools
 - Project management tools

Site24x7

Full-stack monitoring for IT admins, DevOps, and SREs



Why Site24x7?

- Full stack monitoring from the cloud
- Conveniently manage users' digital experience
- Perform comprehensive monitoring for digital assets like websites, REST APIs, mobile apps, and user transactions
- Improve application performance by troubleshooting issues with ease
- Leverage complete infrastructure monitoring for on-prem, cloud, and virtual infrastructure
- Ensure security against SSL Error, domain blacklist and defacement for your end user transacting in the website



All-in-one monitoring solution for DevOps and IT operations

- Website performance monitoring
- Server monitoring
- Synthetic web transaction monitoring
- Application performance monitoring
- Public and private cloud monitoring
- Network monitoring
- Real user monitoring
- Remote infrastructure monitoring for MSPs and CSPs
- Log management from the cloud

Integrations

- ManageEngine AlarmsOne
- ManageEngine ServiceDesk Plus MSP
- ManageEngine ServiceDesk Plus Cloud
- Webhooks
- ServiceNow
- HipChat
- Stride
- Opsgenie
- Jira
- ConnectWise Manage
- PagerDuty
- Slack
- Zapier
- Microsoft Teams

Site24x7 (MSP)

Site24x7 with capabilities for MSPs



Site24x7 CloudSpend

Cloud cost management for modern software teams



Why Site24x7 CloudSpend?

- Bridge the gap between capacity planning and cost optimization for resources running in the Amazon Web Services (AWS) environment
- Gain a high-density snapshot of your spending
- Optimize operational expenditures
- Analyze cloud cost data easily
- Enable cost control by implementing budgets
- Drive organizational accountability by tracking costs related to different business units



Cloud cost management to optimize your AWS cloud spending

- Automate bill processing
- Analyze spending
- Leverage cost control budgets
- Track spending based on business units
- Analyze subsets of cloud costs with the resource explorer

Site24x7 StatusIQ

Status pages for real-time status and incident communication




Why Site24x7 StatusIQ?

- Establish a reliable, dedicated channel that can publish updates, deflect support tickets, and keep internal stakeholders informed
- Quickly acknowledge and update customers about specific problems by posting the incident on your status page
- Inform customers about upcoming maintenance events to help them prepare for any potential impact
- Send out notifications to your customers via email or SMS, or enable them to access updates via RSS
- Provide an accurate account of incidents to customers. Give them information on what happened, the root cause, and how it was resolved
- Showcase and preserve your branding throughout the entire incident life cycle



Status and incident communication platform for modern software teams

- Email and SMS notifications
- Incident notification for end users
- Maintenance notification for end users
- Domain, logo, and page customization
- Analysis and postmortem of incidents



Applications that can be self-hosted on public cloud platforms (AWS or Azure)

Our on-premises solutions can be deployed in any public cloud platform.

Microsoft Azure

Service management

- ServiceDesk Plus
- ServiceDesk Plus MSP

Identity and access management

- ADManager Plus
- ADAudit Plus
- ADSelfService Plus
- Exchange Reporter Plus
- M365 Manager Plus
- SharePoint Manager Plus
- Recovery Manager Plus
- Password Manager Pro
- Password Manager Pro MSP
- Access Manager Plus

Unified endpoint management

- Desktop Central
- Desktop Central MSP
- Mobile Device Manager Plus
- Mobile Device Manager Plus MSP

IT operations management

- Site24x7
- Applications Manager

IT security management

- EventLog Analyzer
- ADAudit Plus

Amazon Web Services (AWS)

IT service management

- ServiceDesk Plus
- ServiceDesk Plus MSP

Identity and access management

- ADManager Plus
- ADSelfService Plus
- ADAudit Plus
- SharePoint Manager Plus
- M365 Manager Plus
- Password Manager Pro

Advanced IT analytics

- Analytics Plus

Unified endpoint management

- Desktop Central
- Desktop Central MSP
- Patch Manager Plus
- Remote Access Plus

IT security management

- Firewall Analyzer

IT operations management

- OpManager
- Network Configuration Manager
- NetflowAnalyzer
- OpUtils
- Applications Manager

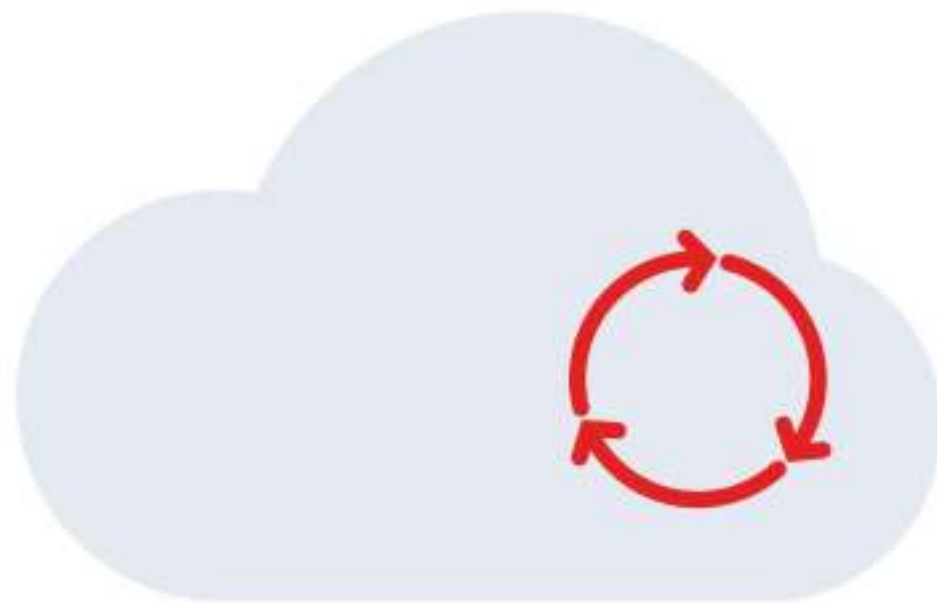


**Cloud monitoring and management solutions that
are installed on-premises**

- 
1. **M365 Manager Plus:** Microsoft 365 management, reporting, and auditing
 2. **SharePoint Manager Plus:** SharePoint reporting and auditing
 3. **Exchange Reporter Plus:** Reporting, auditing, and monitoring for hybrid Exchange and Skype
 4. **ADAudit Plus:** Real-time Active Directory, file, and Windows server change auditing
 5. **Recovery Manager Plus:** Active Directory, Microsoft 365, and Exchange backup and recovery
 6. **M365 Security Plus:** Microsoft 365 security
 7. **Cloud Security Plus:** Cloud security monitoring and analytics
 8. **PAM suite:** Control and secure privileged access to critical enterprise systems
 9. **Applications Manager:** Server and application performance monitoring

M365 Manager Plus

Microsoft 365 management,
reporting, and auditing



Why M365 Manager Plus?

- Get out-of-the box reports on Exchange Online, Azure Active Directory, OneDrive for Business, Skype for Business, and more
- Audit even the most granular user activities, and get notified of critical activities and changes
- Provision and manage users, mailboxes, groups, contacts, and licenses in bulk
- Monitor Microsoft 365 service health around the clock, and receive instant email notifications on service degradations
- Create event-driven automation policies to carry out user and mailbox management tasks
- Preconfigure templates to speed up Microsoft 365 user, group, and contact creation processes
- Search for emails with personally identifiable information (PII), insider information, and malicious content to ensure email security and compliance

One solution for all your Microsoft 365 needs

- Microsoft 365 reporting
- Microsoft 365 management
- Microsoft 365 auditing
- Microsoft 365 automation
- Microsoft 365 security
- Microsoft 365 alerting
- Microsoft 365 monitoring
- Password expiration notification
- Help desk delegation



Integrations

- ManageEngine AD360
- ManageEngine Log360
- Syslog
- Splunk

SharePoint Manager Plus

SharePoint reporting and auditing



Why SharePoint Manager Plus?

- Audit log reports and analyze all activities in your SharePoint environment to ensure security
- Carry out critical management tasks (grant and revoke permissions, create or delete groups, and more) from a central console
- Get insights on user behavior with details on traffic and search with the help of usage analytics
- Ensures seamless collaboration with out-of-the-box Office 365 reports to manage your online SharePoint
- Categorize reports by statistics, security, activity, usage, analytics, and Office 365 for simplified analysis
- Meet compliance requirements that outline audit log data archival for forensic analysis



Manage, audit, and secure your on-premises and Microsoft 365 SharePoint servers

- SharePoint reporting and management
- SharePoint security and auditing
- SharePoint permission and group management
- Microsoft 365 management
- Audit log archival
- Usage analytics

Exchange Reporter Plus

Reporting, auditing, and monitoring for hybrid Exchange and Skype



Why Exchange Reporter Plus?

- Track incoming and outgoing Exchange emails, and monitor Exchange mailbox sizes
- Perform Exchange traffic analysis, and keep spam away from Active Directory mailboxes
- Access real-time monitoring reports on Exchange databases and servers
- Ensure Exchange health and smooth functioning of server roles
- Keep up with ActiveSync traffic in your organization
- Keep tabs on the number of messages sent and received by each Exchange Server
- Monitor the vital statistics of Exchange Server public folders
- View reports on Skype for Business audio/video calls, instant messages, file transfers, and more.



Keep an eye on all key aspects of your hybrid Exchange environment

- Comprehensive monitoring of your Exchange environment
- Exchange Server auditing and reporting
- Exchange Online auditing and reporting
- Skype for Business Server reporting
- Real-time change auditing
- Granular reporting
- Compliance reports for SOX, HIPPA, PCI DSS, and GLBA audits

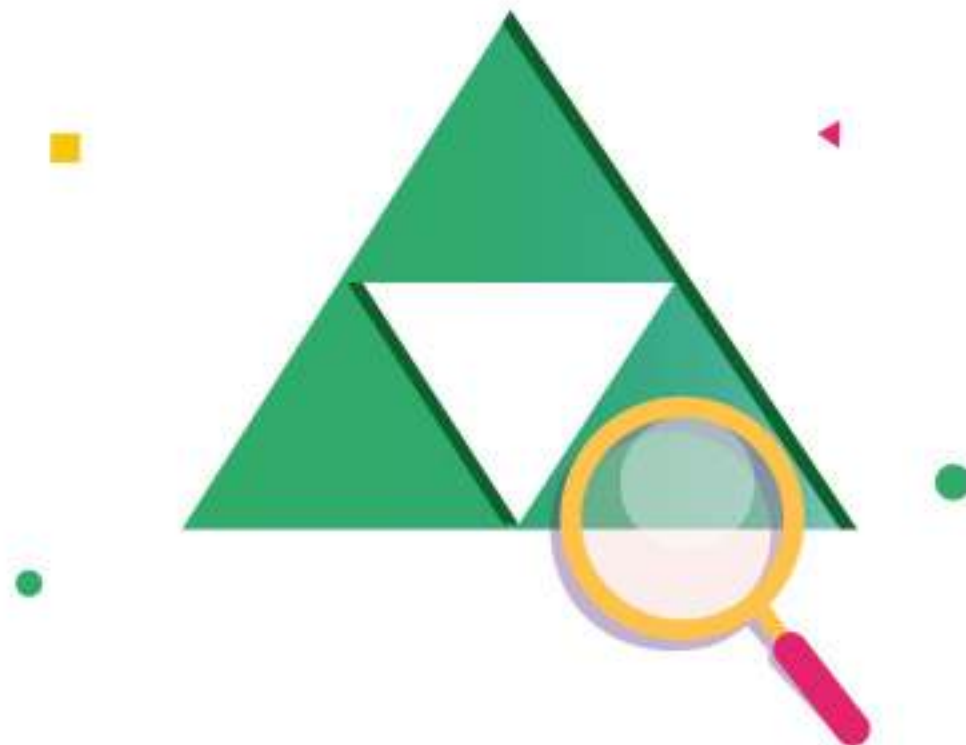


Integrations

- ManageEngine AD360
- ManageEngine Log360

ADAudit Plus

Real-time Active Directory, file,
and Windows server change auditing



Why ADAudit Plus?

- Monitor successful and failed sign-ins
- Instantly detect account lockouts, multi-factor authentication (MFA)-enabled sign-in failures, sign-ins from restricted locations, brute-force attempts, and more
- Audit user and device management actions. Know when a guest user is added or removed
- Track membership changes to groups. Get instantly alerted when a user is assigned the Global Administrator role
- Keep tabs on application management actions. Also, track application usage and conditional access policy changes
- Maintain a complete audit trail of all activity to meet compliance requirements
- Know the origin of any activity, whether on-premises or Azure. Get a correlated view with additional information like a user's on-premises SID



Get full visibility into all changes and sign-ins occurring in your Azure AD

- Successful and failed sign-in auditing
- User and device change auditing
- Group membership and role change auditing
- Application change auditing
- Instant security alerts with granular filters
- Audit-ready compliance reports
- Correlated view of activity
- Long-term audit data retention

Recovery Manager Plus

Active Directory, Microsoft 365, and Exchange backup and recovery



Why Recovery Manager Plus?

- Configure multiple AD domains, Microsoft 365 tenants, and Exchange organizations for backup, and manage them from a single dashboard
- Schedule AD, Microsoft 365, and Exchange backups to happen at fixed intervals
- Secure yourself against ransomware threats on Exchange Online and OneDrive for Business environments
- Restore AD objects from any backup without having to restart your domain controllers
- Stay compliant by defining a retention period and discard older backups



Overcome any disaster caused by unwanted changes in your IT environments

- Incremental backups
- Object-level and attribute-level restoration of AD objects
- Mailbox-level and item-level restoration of Exchange mailboxes
- Easily export Exchange mailboxes to PST format
- Site-level restorations in SharePoint Online and OneDrive for Business
- Enterprise-grade AES-256 encryption for backups
- Stay compliant with flexible retention policies

M365 Security Plus

Microsoft 365 security



Why M365 Security Plus?

- Prevent security breaches with predefined granular audit reports on user and admin activities, failed logon attempts, file access, and role changes. Or create custom audit profiles to suit your security requirements
- Provide quick remediation for critical events with real-time alerts
- Stay on top of service outages with around-the-clock monitoring of the health and performance of Microsoft 365 features and endpoints
- Scrutinize emails with automated content search to detect personal information such as Social Security numbers and login credentials
- Create custom help desk roles and delegate routine tasks to non-admin users without elevating their permissions in Microsoft 365. Leverage advanced delegation features to ease the admin workload



An exclusive solution to fortify Microsoft 365 environments

- Granular auditing of user activities
- Around-the-clock monitoring
- Real-time alerting of critical activities and changes
- Automated content search
- Help desk delegation



Integration

- Splunk

Cloud Security Plus

Cloud security monitoring and analytics



Why Cloud Security Plus?

- Centrally manage public clouds
- Easily search through log data
- Track every activity that happens in Microsoft Azure
- Get granular insights on Google Cloud Platform events
- View detailed reports for your AWS cloud environment
- Proactively monitor your Salesforce environment
- Instantly know about critical changes and other security threats with real-time alerts

Log management and monitoring for your public cloud platforms

- **Securing AWS Cloud platform**

- Amazon S3 log management
- Amazon S3 bucket logging
- AWS IAM activity reporting
- Auto-configuration of AWS
- AWS ELB traffic analysis
- AWS security group change auditing
- Amazon RDS activity reporting
- Forensic analysis using CloudTrail logs

- **Securing Azure cloud platform**

- Microsoft Azure virtual machine (VM) activity reporting
- Microsoft Azure DNS auditing

- **Salesforce log management**

- **Google Cloud platform log management**



Integrations

- ManageEngine Log360
- Syslog
- Splunk

PAM suite:

Control and secure privileged access to critical enterprise systems

- **PAM360:** Complete privileged access security for enterprises
- **Password Manager Pro:** Privileged password management
- **Access Manager Plus:** Secure remote access and privileged session management
- **Key Manager Plus:** SSH key and SSL/TLS certificate management

How the PAM suite helps with cloud management

- Secure storage of IaaS infrastructure access keys and credentials in a central vault protected with AES-256 encryption
- Enforce role-based access controls for credentials. Mandate technicians to go through approval workflows prior to retrieving credentials from the vault
- Periodic password resets for cloud services (AWS IAM, MS Azure, Google Apps, Rackspace, Salesforce, Citrix Netscaler, Magento, and Netapp)
- Quick, one-click login to SaaS applications (Google Apps, Salesforce, Microsoft 365, Rackspace, etc.)
- Secure single sign-on capabilities to streamline remote access to VMs hosted on AWS and MS Azure servers. Establish password-less RDP, SSH, and SQL connections in a single click
- Record remote sessions, and archive them as video files to support forensic audits on privileged access activity

PAM360

Complete privileged access security
for enterprises



Why PAM360?

- Scan and discover privileged accounts across the network
- Onboard privileged credentials into a secure, unified vault
- Centralize the enforcement of privileged access policies for all categories of users. Regulate, monitor, and audit access to all critical assets
- Allow users to launch one-click connections to remote hosts. Record privileged sessions with session shadowing capabilities to achieve dual control over privileged access
- Delegate just-in-time controls for domain accounts through on-demand, time-frame-based privilege elevation
- Create baseline behaviors, and detect anomalies in privileged account activity by correlating privileged access data with endpoint event logs
- Accelerate remediation with prompt access to advanced analytics on privileged access

Holistic privileged access security for enterprise IT

- Complete privileged access governance
- Enterprise credential vault
- Just-in-time privilege elevation
- Privileged session monitoring
- Privileged user behavior analytics and context-aware event correlation
- Secure remote access
- Application credential security
- Ticketing system integrations
- SSH key management and SSL certificate management
- Comprehensive reporting, auditing, and compliance

Key offerings in PAM360 through integrations with other ManageEngine solutions

- Privileged user behavior analytics: **Analytics Plus**
- Privileged access auditing for service requests: **ServiceDesk Plus**
- Just-in-time privilege elevation capabilities: **ADManager Plus**
- Endpoint log correlation for privileged session audits: **Log360**
- Self-service password management and single sign-on capabilities: **ADSelfService Plus**

Other integrations

User authentication

AD
Azure AD
LDAP
RADIUS
Smart Card

Single sign-on

Azure AD
Microsoft ADFS
Okta
Any SAML-based authenticators

Two-factor authentication

PhoneFactor
RSA SecurID
Google Authenticator
Microsoft Authenticator
Okta Verify
RADIUS-based authenticators
Duo Security
YubiKey
Any TOTP-based authenticators

CI/CD platforms

Jenkins
Ansible
Chef
Puppet

ITSM

ServiceDesk Plus On-Demand
ServiceDesk Plus MSP
ServiceDesk Plus
ServiceNow
JIRA Service Desk

Certificate authorities

Let's Encrypt
Microsoft CA
GoDaddy
Sectigo
Symantec
Thawte
GeoTrust
RapidSSL
DigiCert

Cloud storage

Dropbox
Amazon S3
Box

Vulnerability scanners

InsightVM

SIEM

Log360
Splunk
ArcSight
EventLog Analyzer
Sumo Logic
Any RFC 3164-compliant tool

Password Manager Pro

Privileged password management



Why Password Manager Pro?

- Privileged credential vaulting and randomization
- Role-based access controls for insider threat mitigation
- Secure remote access provisions with encrypted access gateways and direct login capabilities
- Session recording and shadowing of privileged users
- Compliance auditing and reporting

Secure your enterprise credentials and protect access to your critical devices

- Privileged account discovery and vaulting
- Granular access control mechanism
- Approval workflows for privileged access requests
- Automated password resets
- Application password management
- DevOps credential security
- SSH key management
- Life cycle management for SSL certificates
- Compliance auditing and reporting
- Secure mobile access

Integrations

User authentication

AD

Azure AD

LDAP

RADIUS

Smart Card

SAML SSO

Azure AD

Microsoft ADFS

Okta

OneLogin

CI/CD platforms

Jenkins

Ansible

Chef

Puppet

Cloud storage

Dropbox,

Amazon S3

Box

Two-factor authentication

PhoneFactor

RSA SecurID

Google Authenticator

Microsoft Authenticator

Okta Verify

RADIUS-based authenticators

Duo Security

YubiKey

ITSM

ServiceDesk Plus On-Demand

ServiceDesk Plus MSP

ServiceDesk Plus

ServiceNow

JIRA Service Desk

SIEM

RFC 3164-compliant tools
such as Splunk, Arcsight, and
EventLog Analyzer

Password Manager Pro MSP: Manage the passwords of multiple customers in a single instance

- Securely store client passwords
- Launch direct connection to remote IT resources
- Selectively share among MSP admins and clients
- Automatically reset passwords
- Control privileged access to client networks
- Gain visibility on password access
- Entrust concurrent control of the password vault to the MSP administrator, the end user, or both

Key Manager Plus

SSH key and SSL/TLS
certificate management



Why Key Manager Plus?

- Gain complete visibility over your SSH and SSL environments
- Discover all SSH keys and SSL certificates across your network, and consolidate them in a secure repository
- Avoid proliferation of keys and certificates by centralizing their creation and deployment
- Tighten security by periodically rotating keys, and prevent their misuse
- Launch remote SSH sessions to target specific endpoints from Key Manager Plus
- Integrate out-of-box with leading certificate authorities to automate SSL certificate life cycle management
- Detect vulnerabilities in SSL configurations and expedite remediation
- Receive timely SSL expiration alerts, stay on top of certificate renewals, and avoid service downtime

Take control over your SSH and SSL certificates

- Automated discovery and vaulting of SSH keys and SSL certificates
- Central key creation, deployment, and periodic rotation
- One-click remote SSH connections to target endpoints
- Policy-based CSR generation and signing
- Out-of-the-box integration with Let's Encrypt, DigiCert, Microsoft CA, and more
- SSL vulnerability scanning and certificate expiration alerts



Integrations

Certificate authority integration

Digicert

Let's Encrypt

Go Daddy

GlobalSign

Sectigo

GeoTrust

Microsoft CA

RapidSSL

Ticketing system integration

ServiceDesk Plus

ServiceNow

Privileged access management

Password Manager Pro

PAM360

Access Manager Plus

Secure remote access and
privileged session management



Why Access Manager Plus?

- Secure remote access management and session governance
- Establish privileged sessions to underlying systems (Windows and Linux) via a central console
- Define roles and access rights for users, and provide them with granular access to critical systems
- Monitor privileged sessions in real time, and record every privileged user session for post-session review
- Leverage extensive audit trails for forensic investigations
- Enhanced regulatory compliance

Secure remote access for privileged sessions

- One-click RDP, SSH, SQL, and VNC sessions
- RemoteApp support for Windows
- Bi-directional remote file transfer
- Jump box support for Windows and Linux
- Privileged session management and recording
- Live monitoring and collaboration
- In-depth audit trails

Integrations

User authentication

AD
Azure AD
LDAP
RADIUS
Smart Card

Single sign-on

Azure AD
Microsoft ADFS
Okta
Any SAML-based authenticators

Two-factor authentication

PhoneFactor
RSA SecurID
Google Authenticator
Microsoft Authenticator
Okta Verify
RADIUS-based authenticators
Duo Security
YubiKey
Any TOTP-based authenticators

SIEM

Log360
Splunk
ArcSight
EventLog Analyzer
Sumo Logic
Any RFC 3164-compliant tool

ITSM

ServiceDesk Plus On-Demand
ServiceDesk Plus MSP
ServiceDesk Plus
ServiceNow
JIRA Service Desk

Applications Manager

Server and application performance
monitoring



Why Applications Manager?

- Single console to monitor your hybrid IT Infrastructure, including servers and applications hosted in physical, virtual, or cloud setups.
- Automated application discovery and dependency mapping between applications
- Application performance monitoring: drill down to elements delaying response times
- Synthetic transaction monitoring to measure the digital experience across geographies
- Robust fault management with dynamic baselining and automated remedial actions

Supported cloud services

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- Oracle Cloud Infrastructure
- OpenStack
- Microsoft 365

Integrations

- OpManager
- ServiceDesk Plus/ServiceDesk MSP
- ServiceNow
- Analytics Plus
- Site24x7
- Alarms One
- PagerDuty
- Slack

ManageEngine cloud customers

ServiceDesk Plus Cloud:



Patch Manager Plus Cloud:



Recovery Manager Plus:



Mobile Device Manager Plus:



AlarmsOne:



SharePoint Manager Plus:



Site24x7:



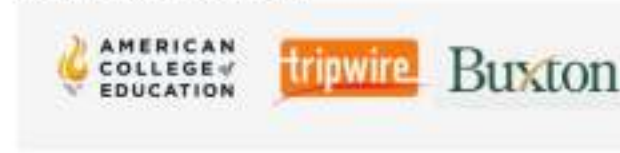
Log360 Cloud:



Exchange Reporter Plus:



Cloud Security Plus:



O365 Manager Plus:



PAM suite:



Applications Manager.



Remote Access Plus:



ManageEngine

www.manageengine.com

