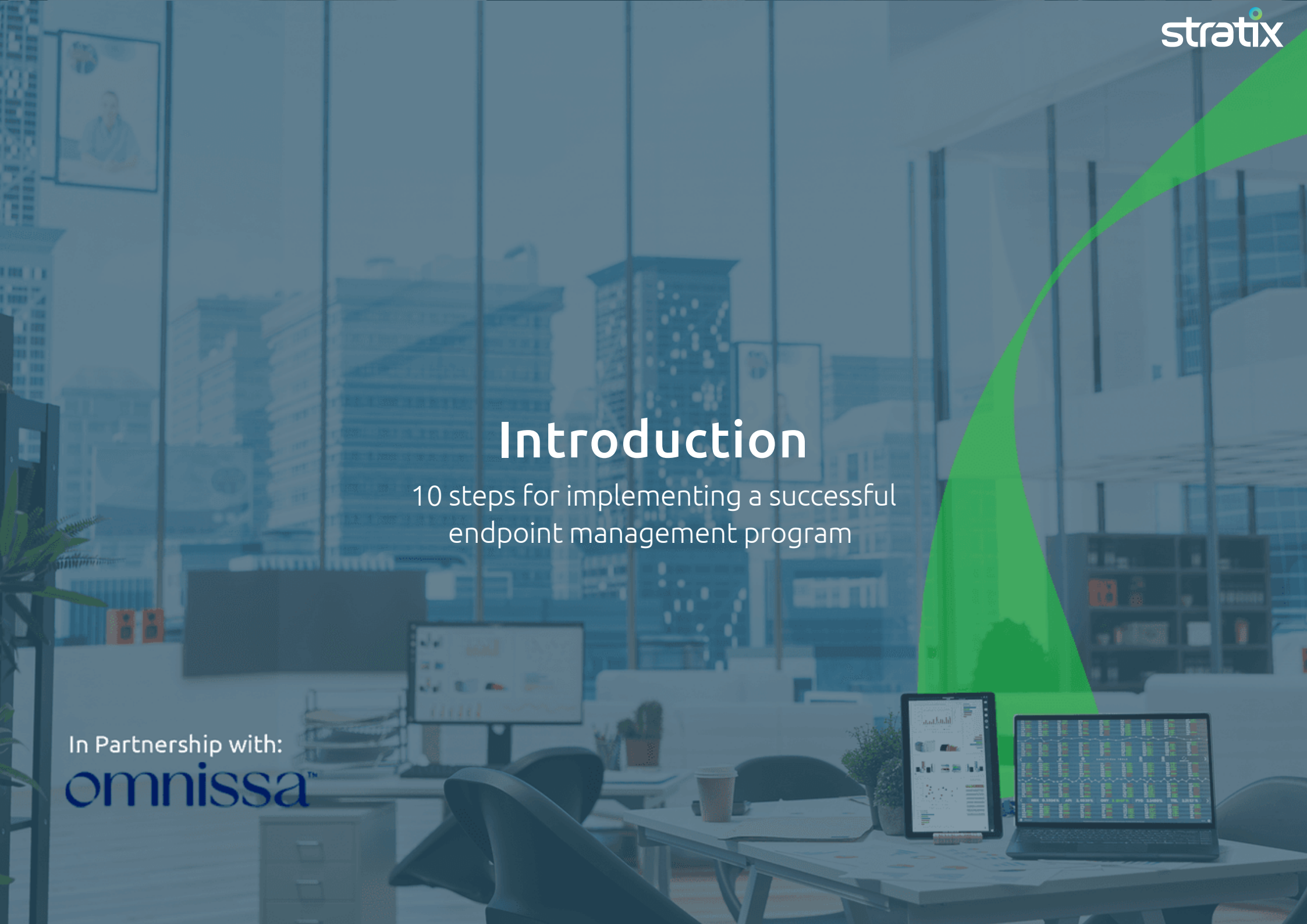
Unified Endpoint Management Masterclass

10 steps for implementing a successful endpoint management program

In Partnership with:

omnissa™



Introduction

10 steps for implementing a successful endpoint management program

In Partnership with:

omnissa™

Get Control

Businesses and organizations rely on an ever-growing number of devices to improve workflows, drive productivity, and streamline operations. From desktops and laptops to mobile devices, printers, and IoT endpoints, managing the highly diverse ecosystem is a significant challenge—and many organizations try to do it with a patchwork of systems that is inefficient and often problematic. Without a robust and strategic unified endpoint management strategy, businesses face security vulnerabilities, operational inefficiencies, and compliance risks.

Endpoint Management

Endpoint management is the process of monitoring, securing, and maintaining an organization's devices, ensuring they remain functional, secure, and compliant with company policies. This includes managing operating systems, applications, security configurations, and network access.

What Do We Mean by Unified Endpoint Management?

The concept of endpoint management began with mobile devices, but as the number and diversity of devices used by organizations has grown, the gold standard is now Unified Endpoint Management (UEM). It's an advanced approach that centralizes the management of all endpoint types—including desktops, laptops, mobile devices, printers, Internet of Things (IoT), and frontline devices—within a single platform.

Why is that better? Once deployed, UEM significantly reduces the management workload through automation while improving security because one system runs and monitors everything—meaning nothing falls through the cracks. It's a tool that solves the twin challenges of managing the sheer scale of current tech stacks within organizations and being able to see everything from one place.

This masterclass explores the importance of endpoint management, the advantages of UEM, and gives you a 10-step approach to implementing a successful endpoint management strategy that will tame your chaos and improve your efficiency and security.

10 Steps for Implementing a Successful Endpoint Management Strategy

Step 1: Define Objectives and Scope

Step 2: Choose the Right Platform

Step 3: Establish Governance and Policies

Step 4: Identify Automation Opportunities

Step 5: Create Your Security Structure

Step 6: Training and Change Management

Step 7: Monitor and Optimize

Step 8: Plan for Incident Response

Step 9: Leverage Analytics and Reporting

Step 10: Integrate with Other Systems

stratix

10 Steps for Implementing a

Successful Endpoint Management Strategy

In Partnership with:

omnissa™

Step 1: Define Objective and Scope

Understand Your Needs

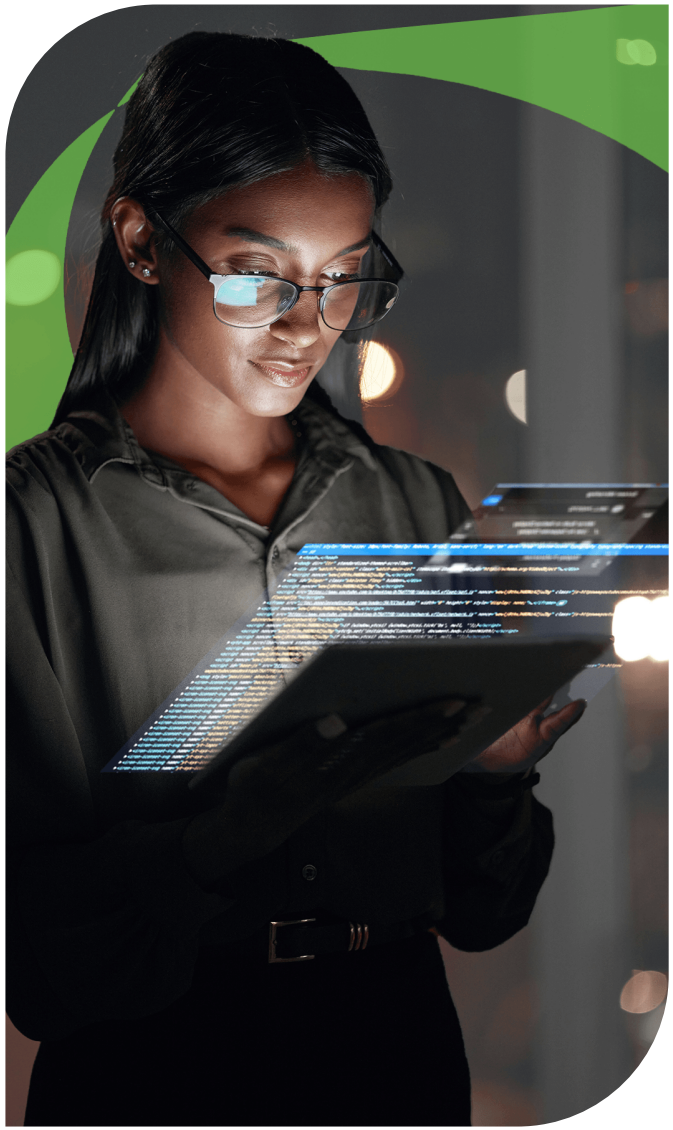
Just like any technology solution, planning should start with where you want to end up. Then, you map the path to get there. Identify your goals for endpoint management. They likely include improving security, simplifying and automating IT workflows like patches and updates, and driving higher productivity within your IT team.

Scope the Implementation

Identity which devices will be managed, including desktops, laptops, mobile devices, and IoT devices, ensuring that all endpoints that interact with company resources are covered. It's crucial to consider all the operating systems in use, such as Windows, macOS, Linux, Android, and iOS, to ensure compatibility and comprehensive management across diverse environments. Additionally, organizations must assess device ownership models (corporate-owned versus bring-your-own-device (BYOD)) to determine different management approaches and levels of control. Clear scoping helps to avoid unmanaged endpoints that may pose security risks and ensures that all relevant devices and platforms are accounted for in the planning process.

Are There Existing Endpoint Management Platforms That Need to Be Migrated?

Most organizations already have one or more endpoint management platforms in use. Recent research by Stratix found the average is between two and four. Existing platforms should be assessed to determine how to migrate them to a new system. Look at which devices and operating systems they manage, their feature sets, and any limitations they may have. Organizations should also look at contractual obligations, licensing costs, and the complexity of migration to avoid business disruptions. Clear documentation of the existing endpoint management environment will facilitate smoother transitions, reduce downtime, and ensure that no devices are left unmanaged during the migration process.



Step 2: Choose The Right Platform

Selecting the right platform is one of the most crucial steps in implementing a successful endpoint management strategy. The platform must align with the organization's business needs, IT infrastructure, and security requirements. Look for features like centralized policy management, real-time monitoring, automated patching, and secure app deployment. Security capabilities such as encryption enforcement, multi-factor authentication (MFA), compliance checks, and integration with threat detection tools are essential for safeguarding sensitive data across devices.

Scalability and flexibility should also be considered. Ensure the platform can support future growth, new device types, and evolving compliance requirements. Additionally, prioritize platforms that provide a seamless user experience, both for IT administrators and end users, to reduce complexity and improve adoption. Compatibility with existing IT and security infrastructure, such as identity and access management (IAM) systems, is key to ensuring smooth integration without significant operational disruption. Cost-effectiveness, vendor support, and ease of migration are important factors as well.

Will it Meet Your Specific Requirements?

For industries with strict regulatory requirements—such as healthcare (HIPAA), finance (PCI-DSS, SOX), or government sectors (FedRAMP, NIST)—the chosen platform must provide built-in compliance tracking and reporting features. This includes automated compliance checks, real-time alerts for non-compliant devices, and customizable reporting dashboards to help IT teams ensure adherence to internal policies and external regulations. The ability to generate audit logs and detailed security reports is especially valuable for organizations that undergo regular security assessments or compliance audits.

Cloud-Based?

A cloud-based endpoint management solution offers significant advantages over traditional on-premises models for organizations with a remote or distributed workforce or those without extensive on-premises infrastructure. Cloud-based solutions provide centralized, always-available management, enabling IT teams to monitor, secure, and support devices from anywhere, without the need for a dedicated data center. This is particularly beneficial for companies with remote employees, field workers, or global offices, as it eliminates the need for VPNs or local network dependencies for endpoint management.

Scalability is another major advantage. Cloud-based platforms allow organizations to scale up or down easily based on workforce changes, new office locations, or seasonal demands without requiring expensive hardware upgrades.

omnissa™

Omnissa Workspace ONE Checks All the Boxes

One of the premier UEM solutions is Omnissa's Workspace ONE. It's a cloud-native platform that delivers the key features organizations need, including:

- Comprehensive device management across all platforms, including mobile devices, desktops, frontline devices, and IoT, enabling centralized management and security enforcement.
- The platform leverages AI and data analytics to automate IT processes, enhance security, and improve user experiences. Features like Omnissa Intelligence service offer actionable insights and automation capabilities to streamline operations.
- With a modern, cloud-native architecture, Workspace ONE supports scalability and flexibility, allowing organizations to adapt to changing needs and manage a diverse range of devices and use cases effectively.

Ultimately, choosing the right platform involves balancing functionality, security, and usability to create a future-proof solution that simplifies endpoint management while minimizing risk.

Step 3: Establish Governance and Policies

A well-defined governance framework is essential for maintaining control over endpoint devices, ensuring compliance, and mitigating security risks. Establishing clear policies for device management, security, and compliance helps standardize IT operations, protect sensitive data, and enforce best practices across the organization. Effective governance ensures that employees, contractors, and third parties adhere to the same security and operational guidelines, reducing vulnerabilities and improving overall endpoint security posture.

Policy Creation

Creating comprehensive policies is the foundation of a strong UEM strategy. They should cover multiple aspects of endpoint security and operational management, including:

- **Device Usage Policies:** Define acceptable use guidelines for company-owned and personal (BYOD) devices. Specify which types of devices are allowed, the applications that can be installed, and restrictions on unauthorized software or modifications (e.g., jailbreaking or rooting mobile devices).
- **Software Installation and Management:** Establish controls over software deployment, ensuring only authorized applications are installed. Use whitelisting and blacklisting strategies to prevent unauthorized software from running on corporate devices.
- **Patch Management:** Implement policies to ensure timely updates and security patches for operating systems and applications. Automated patch deployment should be prioritized to minimize vulnerabilities caused by outdated software.
- **Security Policies:** Define mandatory security measures, such as encryption for data at rest and in transit, endpoint detection and response (EDR) solutions, firewalls, and antivirus software. Require multi-factor authentication (MFA) and role-based access controls (RBAC) to enhance security.
- **Data Protection and Remote Wipe Policies:** Establish data protection policies to secure sensitive business information on endpoints. In case of lost, stolen, or compromised devices, remote wipe functionality should be enforced to prevent unauthorized data access.

By clearly defining and enforcing these policies, organizations can standardize device management while mitigating security risks.

Compliance Standards

To maintain regulatory compliance, endpoint management strategies must align with relevant industry standards and legal frameworks. Organizations operating in regulated industries, such as healthcare, finance, and government, must ensure that endpoint management policies comply with data protection and cybersecurity requirements. Some key compliance frameworks include:

- **General Data Protection Regulation (GDPR):** Ensures the privacy and security of personal data for individuals in the European Union (EU). Endpoint management must include data encryption, secure access controls, and logging mechanisms to meet GDPR requirements.
- **Health Insurance Portability and Accountability Act (HIPAA):** Applies to healthcare organizations, requiring strict protection of patient data. Endpoint policies should enforce encryption, access controls, and audit logs to comply with HIPAA regulations.
- **ISO/IEC 27001:** A global information security management standard that defines best practices for data protection. Endpoint security policies should align with ISO 27001 requirements for risk assessment, security controls, and continuous monitoring.
- **Payment Card Industry Data Security Standard (PCI DSS):** Requires organizations handling credit card transactions to secure endpoints that process, store, or transmit payment data. Encryption, regular security audits, and endpoint monitoring are key PCI DSS compliance measures.
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework:** Provides best practices for cybersecurity risk management, including endpoint protection, continuous monitoring, and incident response.

To ensure compliance, organizations should implement automated compliance checks, generate audit-ready reports, and integrate endpoint security with Security Information and Event Management (SIEM) systems. Regular policy reviews and updates are necessary to stay ahead of evolving compliance requirements and emerging threats.

By establishing strong governance and compliance frameworks, organizations can create a secure, efficient, and well-regulated endpoint management environment that protects sensitive data while ensuring operational continuity.

Step 4: Identify Automation Opportunities

Automation plays a crucial role in streamlining endpoint management, reducing administrative overhead, and improving security by ensuring that devices remain up-to-date and compliant with policies. By automating key processes such as patch management, device provisioning, and alerting, IT teams can minimize human errors, respond to security threats faster, and enhance the overall efficiency of endpoint operations. There are three major areas where automation can drive significant improvements in endpoint management.

Patch Management

Keeping operating systems, applications, and security software up to date is critical for protecting endpoints from vulnerabilities and cyber threats. Manual patching can be time-consuming and inconsistent, leading to security gaps and non-compliance. Automating patch management ensures that updates are applied promptly and consistently across all devices.

- **Automate OS and Application Updates:** Configure endpoint management solutions to automatically deploy OS updates, security patches, and third-party application updates. This reduces the risk of exploitation due to unpatched software.
- **Enforce Patch Compliance:** Set policies to ensure that devices remain compliant with patching requirements. Devices that fail to install updates within a specified timeframe can be flagged for remediation.
- **Staggered Rollouts:** Implement phased patch deployments to test updates on a small group of devices before rolling them out organization-wide, minimizing disruptions caused by faulty updates.
- **Scheduled Maintenance Windows:** Automate update installations during off-peak hours to reduce downtime and ensure minimal disruption to business operations.

Provisioning

Automating device provisioning simplifies the setup process for new employees, device replacements, and system upgrades. IT teams can preconfigure devices with the necessary settings, security policies, and applications, reducing the time and effort required for manual setup.

- **Zero-Touch Deployment:** Use solutions like Omnissa Workspace ONE to enable zero-touch provisioning, allowing new devices to be automatically configured upon first boot without IT intervention.
- **Predefined Configuration Profiles:** Automate the application of security settings, network configurations, and software installations based on user roles and device types. This ensures that every device adheres to corporate standards from the moment it is activated.
- **Cloud-Based Enrollment:** Enable automatic enrollment into your UEM platform, ensuring that all devices are immediately registered for monitoring and compliance enforcement.
- **Automated Deprovisioning:** When an employee leaves the organization, automate the removal of corporate data, revoke access permissions, and remotely wipe company-owned devices to prevent unauthorized access.

Alerts and Automated Responses

Proactive monitoring and automated alerts help IT teams detect and respond to security threats, compliance violations, and performance issues in real-time. By setting up automated alerts, organizations can quickly mitigate risks before they escalate.

- **Non-Compliance Alerts:** Automatically detect when a device is out of compliance due to missing security updates, unauthorized software installations, or disabled security features (e.g., antivirus turned off). Alerts can trigger automated remediation actions, such as enforcing updates or blocking network access until compliance is restored.
- **Security Threat Detection:** Integrate endpoint management with Security Information and Event Management (SIEM) tools to detect suspicious behavior, such as repeated failed login attempts, unauthorized file access, or malware activity. Automated alerts can notify IT teams for immediate investigation.
- **Device Health Monitoring:** Configure alerts for hardware failures, low disk space, or performance degradation. Automated scripts can initiate troubleshooting steps, such as clearing temporary files, reallocating system resources, or rebooting affected devices.
- **Automated Incident Response:** In case of a security breach or policy violation, automated workflows can isolate compromised devices, revoke user credentials, and trigger incident response protocols to minimize damage.

By leveraging automation in these key areas, organizations can enhance security, improve operational efficiency, and free up IT resources to focus on strategic initiatives rather than repetitive tasks.

Step 5: Create Your Security Structure

3 Security Measures to Implement

1. Endpoint Protection
2. Encryption
3. Access Control

Building a robust security structure is a fundamental component of endpoint management, ensuring that all devices are protected against cyber threats, unauthorized access, and data breaches. A well-designed security framework includes endpoint protection, encryption, and strict access controls, all of which help safeguard sensitive information and maintain regulatory compliance. Here are some security measures organizations can implement to minimize risks while maintaining operational efficiency.

Endpoint Protection

Endpoints—such as desktops, laptops, mobile devices, and IoT devices—are prime targets for cyberattacks, making endpoint protection a top priority. Implementing strong security measures across all managed devices helps prevent malware infections, phishing attacks, and unauthorized access.

- **Deploy Antivirus and Anti-Malware Solutions:** Ensure all devices have up-to-date antivirus and anti-malware software to detect and block malicious threats. Solutions like Omnissa Workspace ONE Mobile Threat Defense offer advanced endpoint protection.
- **Enable Host-Based Firewalls:** Configure firewalls on all endpoints to filter incoming and outgoing network traffic, preventing unauthorized access and blocking malicious communications.
- **Enforce Web and Email Security:** Use DNS filtering and email security gateways to protect users from phishing attempts, malicious websites, and spam attacks. Secure Email Gateways (SEGs) can help filter out harmful emails before they reach users.
- **Automate Security Updates:** Ensure that security software is automatically updated to protect against new threats. This includes antivirus definitions, intrusion prevention system (IPS) updates, and security patches for known vulnerabilities.

Encryption

Encryption is a critical security measure that ensures sensitive data remains protected, even if a device is lost, stolen, or compromised. Organizations should enforce encryption at multiple levels to safeguard information.

- **Require Full-Disk Encryption (FDE):** Implement FDE on all devices handling sensitive data. Solutions like BitLocker (Windows), FileVault (macOS), and Linux LUKS ensure that all data stored on endpoints is encrypted and cannot be accessed without proper authentication.

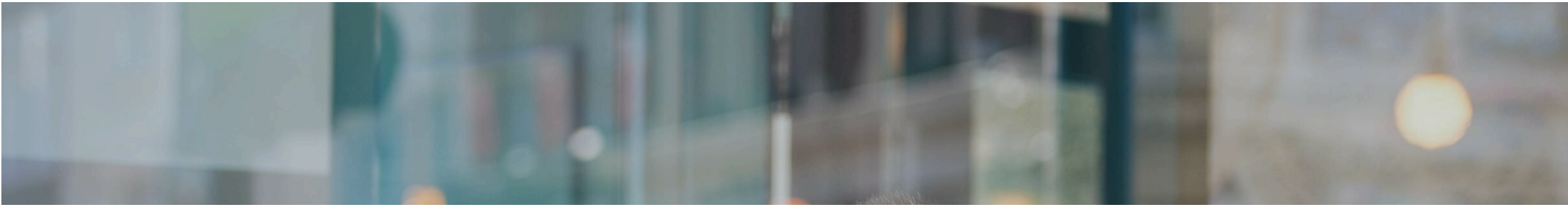
- **Enforce Encrypted Communications:** Use Transport Layer Security (TLS) and Virtual Private Networks (VPNs) to encrypt data in transit, preventing interception of sensitive information during remote work or over public networks.
- **Protect External Storage Devices:** Restrict or require encryption on USB drives and external hard drives to prevent unauthorized data access. Some endpoint management platforms allow organizations to enforce encryption policies on removable storage.
- **Secure Cloud Data:** If endpoints access cloud storage (e.g., OneDrive, Google Drive, Dropbox), ensure data is encrypted at rest and in transit, and use access control measures to limit unauthorized access.

Access Control

Strong access control mechanisms ensure that only authorized users can access corporate data and resources. Implementing authentication and authorization best practices reduces the risk of credential-based attacks and insider threats.

- **Multi-Factor Authentication (MFA):** Enforce MFA for all users accessing corporate systems, cloud services, and sensitive applications. MFA requires users to verify their identity using multiple authentication factors (e.g., password + authentication app or biometric verification).
- **Role-Based Access Control (RBAC):** Assign permissions based on user roles, ensuring that employees have access only to the data and systems necessary for their job functions. Avoid granting unnecessary administrative privileges that could lead to security risks.
- **Conditional Access Policies:** Implement conditional access rules that restrict access based on factors such as device security posture, location, or login behavior. For example, block access to corporate applications from untrusted devices or geographic locations.
- **Zero Trust Architecture:** Follow the Zero Trust principle of "never trust, always verify," requiring continuous verification of users and devices before granting access to corporate resources.
- **Automated Account Lockouts and Monitoring:** Implement security policies that automatically lock out accounts after multiple failed login attempts and monitor access logs for suspicious activity.

By establishing a strong security structure that includes endpoint protection, encryption, and access control, organizations can significantly reduce the risk of cyber threats and ensure a secure, compliant endpoint environment.



Step 6: Training and Change Management

Successfully implementing an endpoint management strategy requires more than just deploying new technology—it also demands effective training and change management to ensure adoption and compliance. Training IT staff and end-users on the platform's features, security best practices, and policy requirements helps maximize efficiency while reducing the risk of misconfigurations or security incidents. Additionally, clear communication and structured change management minimize resistance to new systems and promote a smooth transition.

Training IT Staff and End-Users

Comprehensive training programs should be designed for both IT administrators and end-users to ensure they understand how to use the endpoint management platform effectively and securely.

IT Staff Training:

- Train IT teams on configuring, managing, and troubleshooting endpoint management solutions.
- Provide hands-on sessions for deploying security policies, monitoring compliance, and responding to security incidents.
- Educate administrators on automation capabilities, such as software updates, patch management, and remote troubleshooting.
- Ensure IT teams understand reporting features and compliance tracking to maintain regulatory standards.
- Offer ongoing education on emerging threats and best practices for managing evolving endpoint security risks.

End-User Training:

- Educate employees on how to properly enroll and use their managed devices under the new system.
- Provide security awareness training on phishing attacks, safe browsing, and device hygiene.
- Train users on corporate policies regarding data handling, remote work security, and software installation restrictions.
- Offer simple guides or video tutorials to help employees navigate new security protocols and compliance requirements.
- Encourage adoption of security features like Multi-Factor Authentication (MFA) and encrypted communication tools.

Training should be continuous, with refresher sessions offered regularly to keep up with changes in security policies, compliance requirements, and technology updates.

Change Management and Communication
Effective change management ensures a smooth transition to the new endpoint management system by addressing potential resistance, clarifying expectations, and providing necessary support.

Develop a Clear Communication Plan:

- Announce upcoming changes well in advance, explaining the reasons for the transition and the benefits of the new system.
- Use multiple communication channels (emails, intranet posts, webinars) to inform employees of what to expect.
- Address common concerns, such as privacy issues with device monitoring and changes in user permissions.

Provide Support During the Transition:

- Set up a dedicated helpdesk or support channel to assist users experiencing issues with device enrollment, security settings, or software access.
- Offer a transition period where both old and new systems run in parallel to minimize disruptions.
- Use surveys and feedback mechanisms to collect input from employees and IT staff on their experience with the new system, and make adjustments where necessary.

Engage Leadership and Department Heads:

- Secure buy-in from leadership to reinforce the importance of compliance and security.
- Work with department heads to tailor training and policies to specific teams' workflows and needs.

By prioritizing training and clear communication, organizations can enhance adoption, minimize resistance, and ensure a seamless transition to the new endpoint management strategy.

Step 7: Monitor and Optimize

Once an endpoint management strategy is in place, continuous monitoring and optimization are essential to maintaining security, compliance, and operational efficiency. A proactive approach to monitoring helps detect security threats, performance issues, and policy violations in real time, while regular audits ensure long-term compliance. Additionally, establishing a feedback loop with end-users and IT teams allows organizations to refine processes, enhance user experience, and improve overall endpoint management effectiveness.

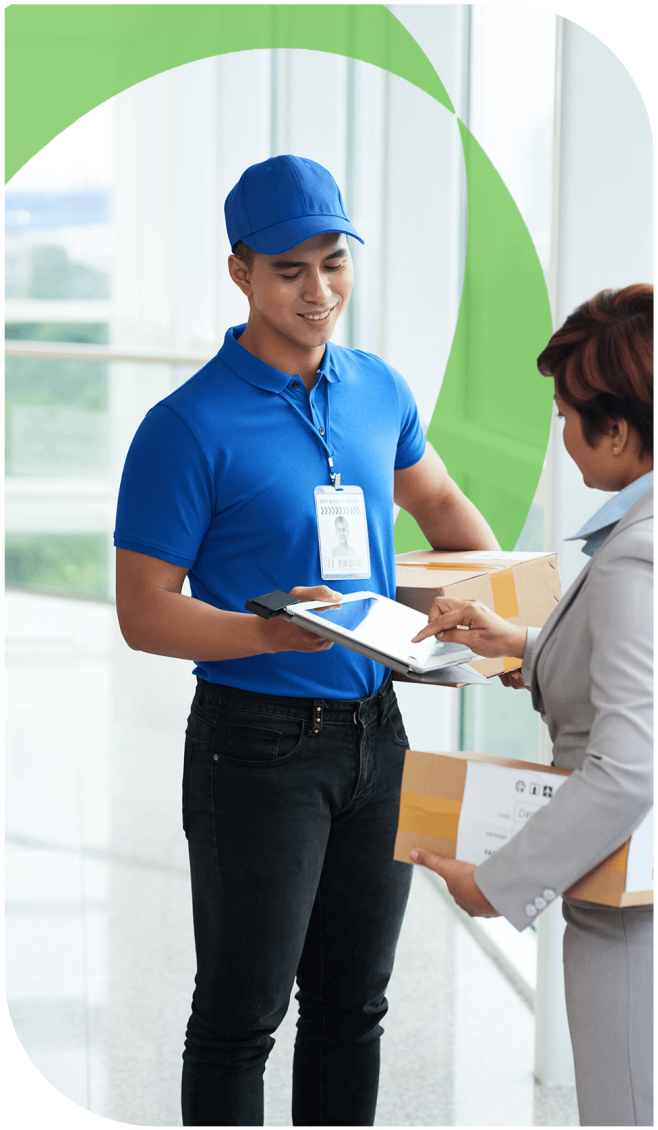
Real-Time Monitoring

Real-time monitoring provides IT teams with visibility into the status of all managed devices, helping them detect issues early and take corrective action before they impact business operations.

- **Centralized Dashboard:** A UEM platform like Omnissa Workspace ONE has an intuitive dashboard to track device health, software compliance, security threats, and usage analytics in real-time.
- **Automated Alerts and Incident Response:** Configure alerts to notify IT teams of critical events, such as unauthorized access attempts, malware detections, or device non-compliance.
- **Device Performance Monitoring:** Track hardware and software performance metrics, such as CPU utilization, memory usage, and disk space, to identify potential performance bottlenecks and proactively address them before they affect user productivity.
- **Remote Diagnostics and Troubleshooting:** Enable IT teams to diagnose and resolve issues remotely through built-in troubleshooting tools, minimizing downtime and reducing the need for on-site support.

Regular Audits

Conducting periodic audits ensures that endpoint management policies remain effective and that all devices comply with security standards and regulatory requirements.



- **Compliance Audits:** Schedule regular compliance checks to ensure endpoints adhere to internal policies and external regulations such as GDPR, HIPAA, or ISO 27001. Automate compliance enforcement by flagging non-compliant devices and enforcing policy updates.
- **Patch Management Audits:** Review patching reports to verify that all devices are running the latest security updates and that no critical vulnerabilities are left unaddressed. Identify devices that repeatedly fail to update and take corrective action.
- **Access Control Audits:** Periodically review user permissions and role-based access controls (RBAC) to ensure users only have access to the data and applications they need. Remove outdated permissions for former employees or role changes to reduce security risks.
- **Asset Inventory Audits:** Maintain an up-to-date inventory of all managed endpoints, ensuring that unauthorized or unmanaged devices are not accessing corporate resources. Conduct periodic asset reconciliation to track lost, stolen, or decommissioned devices.
- **Security Incident Reviews:** Analyze past security incidents to identify patterns, assess the effectiveness of security measures, and implement improvements to prevent future breaches.

Feedback Loop

Gathering feedback from end-users and IT teams helps organizations refine endpoint management processes, improve system usability, and address pain points.

- **User Experience Surveys:** Conduct periodic surveys to understand user challenges related to endpoint management, such as software restrictions, performance issues, or security concerns. Use this feedback to adjust policies and improve device usability.
- **Help Desk Analytics:** Analyze support tickets and IT help desk trends to identify recurring endpoint issues. If certain problems are reported frequently, consider optimizing device policies, training materials, or automation workflows.
- **Stakeholder Meetings:** Hold regular discussions with department heads, IT administrators, and security teams to evaluate the effectiveness of endpoint management strategies and discuss potential improvements.
- **Continuous Improvement:** Use collected data to refine endpoint policies, update configurations, and enhance automation processes. Adopt an agile approach where endpoint management strategies evolve based on new security threats, technology advancements, and business needs.

By implementing real-time monitoring, conducting regular audits, and incorporating user feedback, organizations can ensure that their endpoint management strategy remains secure, efficient, and adaptable to future challenges.

Step 8: Plan for Incident Response

A well-defined incident response plan is essential for quickly detecting, mitigating, and recovering from endpoint-related security incidents. A structured incident response plan should include predefined steps to handle various endpoint security threats, ensuring a swift and coordinated response. The plan should cover:

A) Incident Identification and Detection

- Implement endpoint detection and response (EDR) solutions to identify and alert IT teams about security threats in real-time.
- Use automated monitoring tools to detect unusual behavior, such as unauthorized access attempts, excessive data transfers, or malware activity.
- Establish clear guidelines for reporting security incidents, ensuring employees know how to recognize and report potential threats.

B) Containment and Mitigation

- If a device is compromised, immediately isolate it from the corporate network to prevent malware spread or data exfiltration.
- Temporarily disable user accounts associated with a compromised device to prevent unauthorized access.
- Use application control policies to block malware-infected or unauthorized software.
- Limit endpoint access to sensitive data until the security issue is resolved.

C) Investigation and Threat Analysis

- Conduct forensic analysis to determine the root cause of the incident.
- Identify affected systems, users, and data to assess the potential impact.
- Review endpoint logs and security alerts to track malicious activity and pinpoint vulnerabilities.

D) Eradication and Recovery

- Use antivirus, anti-malware, or endpoint security solutions to remove infections from affected devices.
- Apply security patches to fix exploited vulnerabilities and prevent recurrence.
- If an endpoint is severely compromised, reset it to factory settings and reinstall essential applications.

E) Post-Incident Review and Policy Updates

- Conduct a post-mortem analysis to assess what went wrong and identify areas for improvement.
- Update security policies and incident response procedures based on lessons learned.
- Provide additional security awareness training to employees if human error contributed to the incident.

An effective incident response plan ensures organizations can quickly contain and mitigate endpoint security threats, minimizing disruption and protecting critical business data.

Step 9: Leverage Analytics & Reporting

Analytics and reporting are essential components of a robust endpoint management strategy, providing IT teams with the visibility needed to proactively address security risks, optimize resource usage, and ensure compliance with regulatory requirements. By leveraging built-in analytics and reporting capabilities, organizations can make data-driven decisions to enhance endpoint security, improve operational efficiency, and maintain compliance.

Generate Compliance Reports for Internal and External Audits

Regulatory compliance is a key concern for many organizations, especially those in industries like healthcare, finance, government, and retail, where data security and privacy regulations are strict. Automated compliance reporting simplifies audit preparation and ensures organizations can demonstrate adherence to internal policies and external regulatory standards.

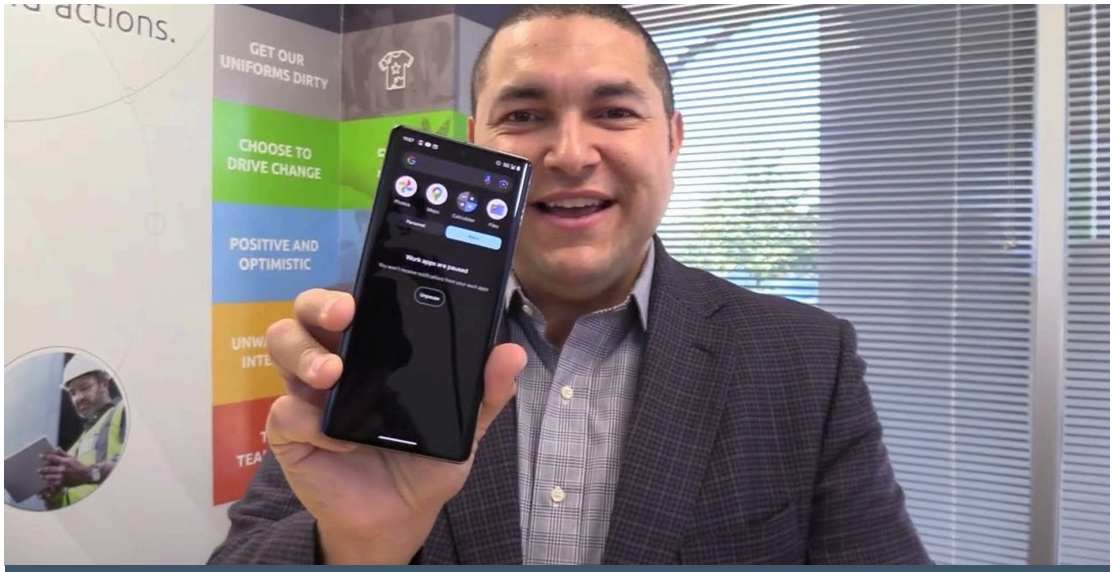
By leveraging analytics and reporting, organizations can proactively manage security risks, optimize endpoint performance, and streamline compliance processes.

Identify Trends, Vulnerabilities, or Underutilized Resources

- Monitor threat detection reports to identify patterns of malware infections, phishing attacks, or unauthorized access attempts.
- Use behavioral analytics to detect anomalies, such as repeated failed login attempts, unexpected file access, or unusual network activity.
- Track the effectiveness of security policies and identify areas where additional enforcement is needed.
- Analyze endpoint security posture by identifying devices with missing patches, outdated antivirus software, or disabled security settings.
- Use risk-scoring mechanisms to prioritize vulnerabilities based on severity and likelihood of exploitation.
- Automate compliance tracking by flagging non-compliant devices and taking corrective actions, such as enforcing policy updates or blocking network access.
- Monitor hardware usage trends to identify underutilized devices, helping organizations optimize hardware investments and decommission unnecessary assets.
- Track software licensing and usage patterns to identify unused applications, reduce licensing costs, and enforce software compliance policies.
- Use performance analytics to detect devices that frequently experience slowdowns, crashes, or hardware failures, enabling proactive maintenance.

Step 10: Integrate with Other Systems

A successful endpoint management strategy doesn't operate in isolation—it must be seamlessly integrated with other IT systems to enhance security, streamline operations, and improve overall efficiency. By integrating endpoint management platforms with identity and access management (IAM), security information and event management (SIEM), helpdesk tools, and other IT solutions, organizations can create a more unified, automated, and secure IT environment.



Stratix and Omnissa Solve BYOD Security Challenge with a Great User Experience for Utility Giant

Omnissa's unified endpoint management approach is not just a great user experience that delivers high security. It reduces the support burden on IT teams because it works across all device types—whether iOS or Android.


stratix
You Don't Have
to Go It Alone
In Partnership with:
omnissa™

A Trusted Advisor Makes All the Difference

Implementing a UEM platform is a complex endeavor that requires expertise in endpoint management, security, and user experience optimization. While many organizations have internal IT teams, they often lack the dedicated resources, specialized knowledge, or bandwidth to successfully deploy and manage a UEM platform at scale.

This is where partnering with a trusted advisor makes a significant difference. A managed services provider like Stratix, with deep expertise in endpoint management, can help organizations navigate the complexities of UEM implementation, ensuring a seamless deployment, enhanced security posture, and optimal device performance across all endpoints. Stratix is Omnissa's largest managed services provider, with certified experts and extensive knowledge about endpoint management. We're here to help.

Solution Design

Stratix's team of certified experts conducts workshops to understand your business requirements, devices, operating systems, and end-user workflows. We then recommend and design an effective endpoint management strategy tailored to your organization.

Implementation and Management

Stratix handles the day-to-day administration, upgrades, updates, and troubleshooting of your UEM environment, allowing your IT staff to focus on innovation and growth activities.

Support Services

Our onshore UEM support team is available 24/7 to resolve issues promptly, ensuring minimal downtime and maintaining productivity.

Stratix and Omnissa – Better Together

By leveraging Stratix's managed services and the Omnissa platform, organizations can implement a robust UEM solution that enhances security, streamlines operations, and improves user experiences across all devices. Reach out today for an audit of your endpoint management environment.

About Stratix

Stratix designs, deploys, manages, and supports end-to-end mobile technology solutions for business, healthcare, and education. With our industry-leading expertise and resources, you get just one hand to shake and everything you need to maximize your technology investments.

www.stratixcorp.com