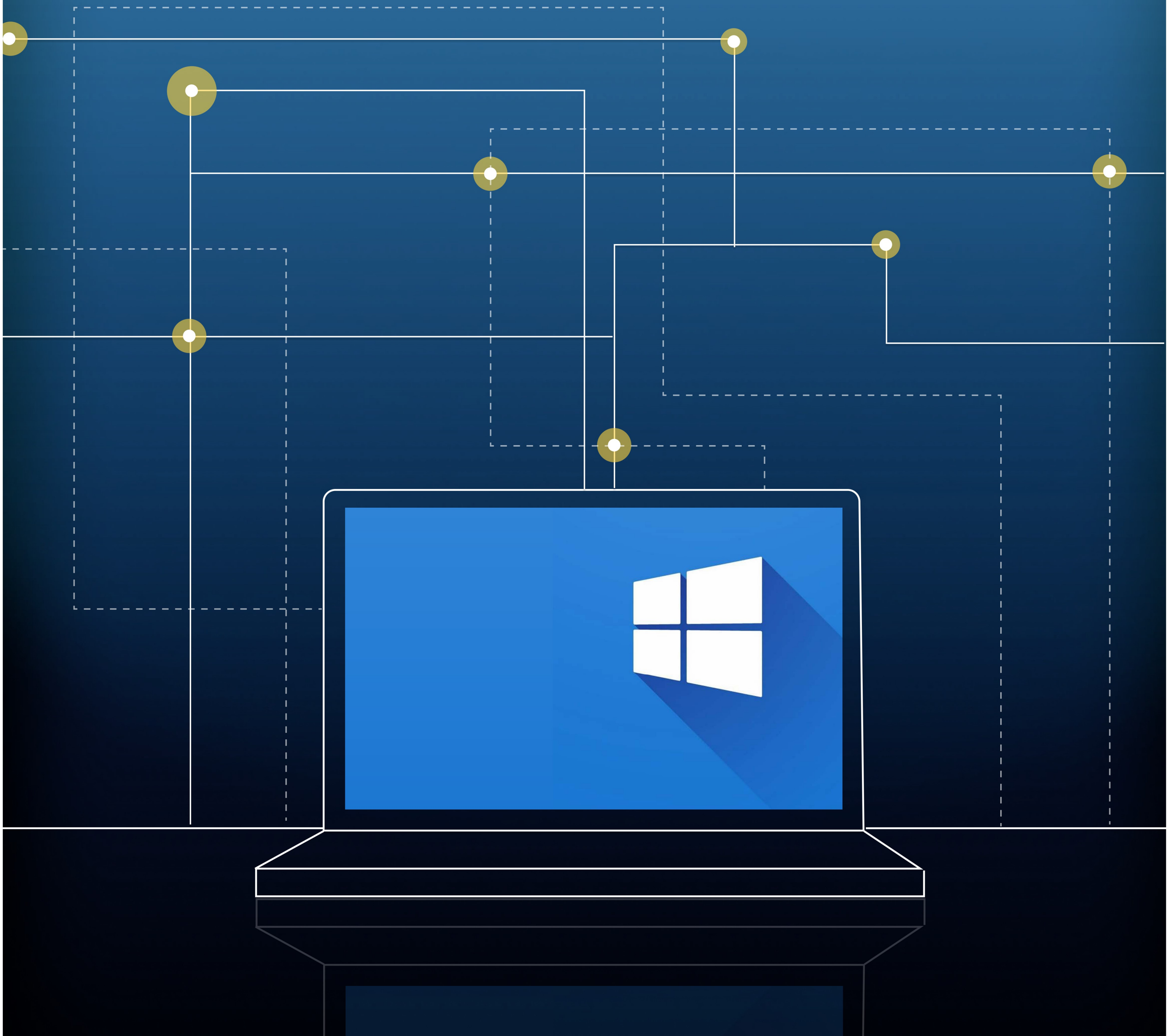
Scalefusion

Best Practices to Implement Endpoint Management for Windows

An IT admin's playbook to manage and secure all Windows endpoints



What’s Inside?

Why should you read this ebook?

Imagine you're a surgeon about to perform a delicate operation on a patient. You've spent years studying, training, and preparing for this moment. However, it’s known to you that one small mistake could have catastrophic consequences. If there's a 90% chance that the operation will be successful, would you take the risk and leave the remaining 10% to chance? One wrong move, missed a detail, or unforeseen complication could cause a lot of difference. Similarly, in the case of Windows Device Management, it takes one small error to destroy years of data and reputation.

Windows Device Management is an essential component of any organization's IT strategy. Whether running a 20 or 20,000-people team, having a secure and reliable policy to manage your Windows devices is necessary.

In this e-book, you'll learn how to effectively manage Windows devices, including desktops, laptops, and tablets. You'll discover the best practices to optimize device performance, configure security settings, and troubleshoot common issues.

The e-book covers various topics relevant to Windows Device Management, including device enrollment, application management, and device updates. It equips you with the knowledge and tools needed to easily manage Windows devices, whether corporate-owned, personal-owned, or hybrid.

As a seasoned IT professional or someone just entering the field, this book is an invaluable resource that will give you the confidence to manage all Windows devices successfully. Take control of your Windows Device Management with this powerful guide and elevate your IT game to the next level!

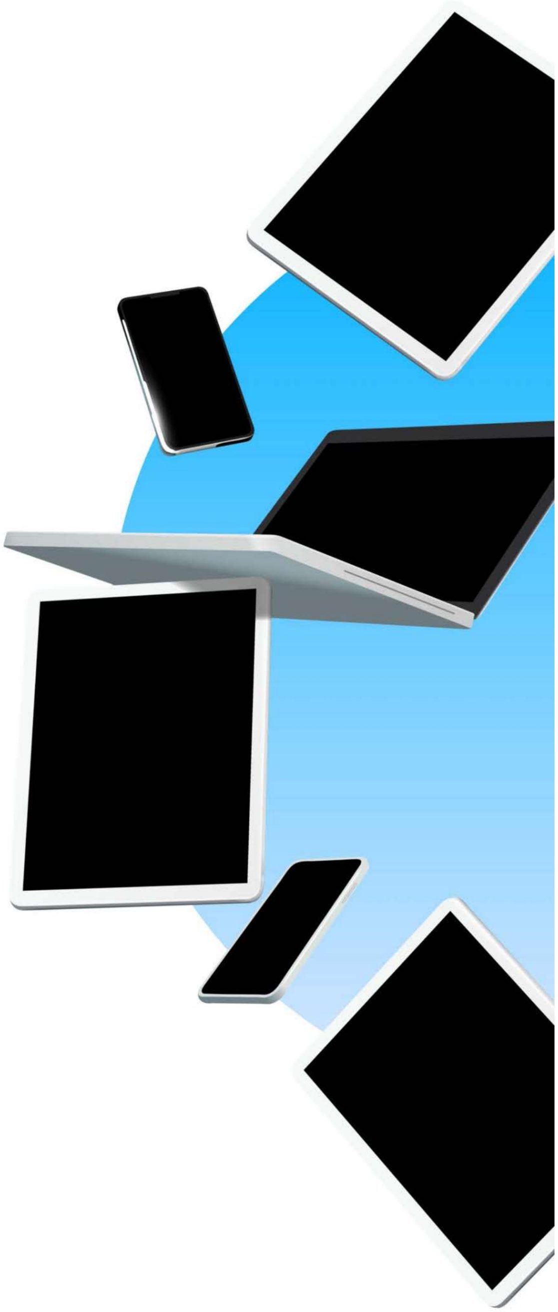
Introduction to Endpoint Management

Motorola DynaTAC 8000X was the first mobile device made available from 1983. Then came the era of 2G handsets that introduced a package of technological advancements that kept on evolving. The UI/UX of mobile phones has witnessed a complete transformation over the last couple of decades.

Similarly, endpoint management has also undergone a significant transformation over the years. Initially, IT admins only managed PCs, but now they manage various endpoints, including laptops, desktops, POS systems, IoT devices, tablets, and many more. This change has been driven by the increasing demand for more sophisticated technologies in the workplace and the rise of remote work, leading to the need for more robust endpoint management solutions.

Several tools have been implemented to streamline device management, including CMT (Client Management Tool), MDM (Mobile Device Management), EMM (Enterprise Mobility Management), and ultimately the tool that we all know—UEM (Unified Endpoint Management). With its ability to centralize management and security across all endpoints, UEM has become the go-to solution for organizations seeking comprehensive endpoint protection and risk mitigation.

An endpoint management solution offers capabilities like bulk enrollment, security updates, software and OS deployment, and remote troubleshooting.



Insights into Endpoint Management in Today's World

The COVID-19 pandemic in 2020 brought about unprecedented changes to the corporate world, resulting in a remote or a hybrid working environment. According to a Forrester study,[1] 51% of enterprise leaders hint that their organizations will deploy a hybrid working model, while 15% of them intend to go fully remote. As a result, organizations need a solution that allows them to manage, secure, and remotely monitor their endpoints. The convergence of technology and the pandemic has made it critical for businesses to take proactive steps toward endpoint management to safeguard their assets and protect against potential breaches.

According to another report[2] by McKinsey, there will be around 51 billion connected devices by 2025. Therefore, it's essential for businesses to implement smart measures that ensure the security of enterprise data across endpoints.

In addition to implementing smart security measures, it's also important for enterprises to have a clear understanding of their endpoint ecosystem. This includes identifying all endpoints connected to the network and assessing their security posture and risk levels. The world of endpoint management is undergoing a significant transformation, marked by a shift toward cloud-based solutions. Experts predict that the global cloud services market would reach USD 166.6 billion by 2024. In the past, companies would install endpoint management software on their servers or devices, but the emergence of cloud computing has enabled businesses to manage and secure their devices from anywhere without the need for on-site infrastructure.

51% of enterprise leaders hint that their organizations will deploy a hybrid working model

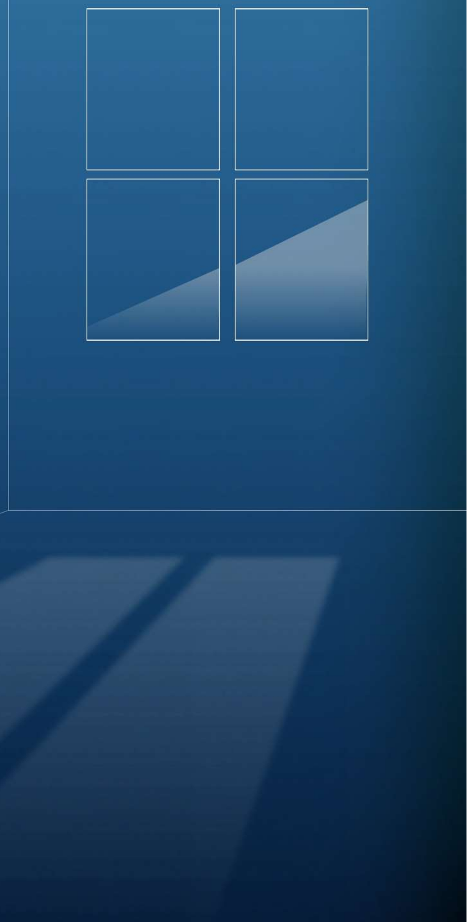
51 billion connected devices by 2025.

Experts predict that the global cloud services market would reach USD 166.6 billion by 2024.

Need for Securing Windows Endpoints

Bill Gates and Paul Allen, with the dream of getting PCs to every desk in houses and offices, launched Windows, and the rest is history. With more than four decades under its belt, Windows has conquered the market as the most popular operating system for laptops and desktops. This makes Windows endpoints susceptible to a range of cyberattacks that can compromise the integrity, confidentiality, and availability of sensitive corporate information.

Hence, your organization’s success hinges on the strength of its endpoint management structure. Even if you have the most technologically advanced systems and networks, a lack of effective endpoint management strategy can cause your operations to crumble. Think of it as your Achilles' heel. Without a cohesive plan to manage your Windows endpoints, your organization could be vulnerable to fatal data security intrusions.



Importance of UEM for Windows

Windows endpoints vary a lot in device configurations and specifications, including processor, storage space, and connectivity. By embracing a flexible and adaptable endpoint management approach, you can ensure your organization is always prepared to accommodate new technologies and user preferences. Organizations must adopt UEM for Windows if they want to be future-ready on how models like work-from-anywhere will continue to gain wider acceptance. The SaaS and cloud penetration makes Windows endpoint management furthermore imperative.

Scalefusion UEM simplifies Windows endpoint management and ensures unmatched endpoint security and compliance. It is designed to help businesses take control of their entire Windows device fleet. Let’s explore some of the best approaches that organizations should take for the most streamlined Windows UEM experience using Scalefusion.

Best Practices To Manage Your Windows Endpoints

1. Simplify Enrollment with OOB

2. Secure Business Data with a Powerful Suite of Features

3. Manage OS and App Patches

4. Quickly Remediate Device Errors with Remote Troubleshooting

5. Push and Manage Work Apps

6. Enhance Engagement with Kiosk Mode

7. Enforce Secure Browsing

8. Execute Remote Actions & Troubleshooting

Best Practices To Manage Your Windows Endpoints

Simplify Enrollment with OOB

Managing Windows devices has always been daunting for businesses, especially in the age of BYOD (Bring Your Own Device). The constant need to upgrade devices based on technology disruptions has made the task even more challenging. Moreover, every new device requires a fresh round of authentication, adding to the complexity of the process.

With Scalefusion, IT teams can incorporate bulk enrollment and provisioning of Windows devices with management policies or automate it with the help of Windows Autopilot for an OOB (out-of-box) experience. Scalefusion streamlines authentication of managed devices for faster and more reliable security.

Scalefusion supports Azure Active Directory (AD) integration to facilitate importing users into device profiles. This saves IT time spent on the manual configuration of individual devices while ensuring employees can begin using the devices by connecting to the nearest network and entering their Azure AD credentials.

Secure Business Data with a Powerful Suite of Features

Scalefusion UEM equips IT admins with robust features to secure Windows endpoints that are constantly exposed to cyber threats. To begin with, IT teams can whitelist apps, websites, and browsers to ensure that Windows devices only access what is safe and don’t fall prey to threat actors via phishing links. Once this is in place, they can enforce stringent passcode policies to take endpoint security a step further. Passcode policies include defining the ideal password type, complexity, and the period after which it must be changed.

But that's not all, IT teams can also configure Cortana and device peripherals such as cameras, USBs, and Bluetooth with Scalefusion UEM. Hence, they can customize Windows devices to meet the specific security requirements of their organization.

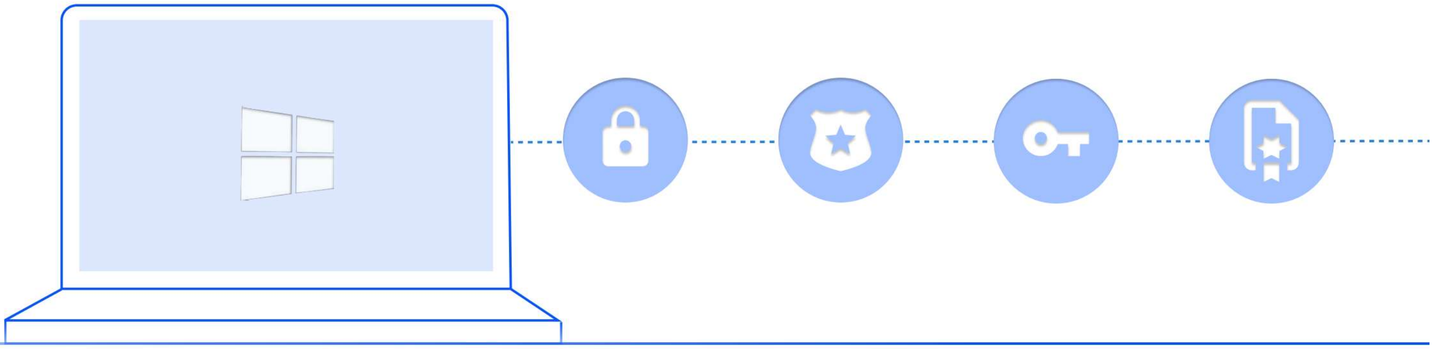
Here are some more security-oriented features of Scalefusion UEM which IT teams can leverage:

BITLOCKER ENCRYPTION -
Scalefusion helps IT admins encrypt device hard disks to protect data from theft or exposure on lost, stolen or retired computers. It also enables IT admins to configure BitLocker settings to help protect corporate data and ensure that a device has not been tampered with while offline.

VPN CONFIGURATION -
The rise of remote work has brought with it a unique set of challenges for businesses, one of the most pressing being the need to protect corporate data on devices outside the company's network perimeter. That's where Scalefusion comes in. With its easy-to-use VPN configuration options for managed Windows devices, IT admins can rest assured that all traffic will be securely routed to corporate apps and data. Plus, with the ability to selectively enforce per-app VPNs, businesses can customize their security approach to match their needs.

DEFENDER POLICIES -
You can protect your Windows devices against malware attacks with the powerful Microsoft Defender Antivirus (previously known as Windows Defender). Scalefusion allows you to customize policies such as scanning, real-time monitoring, signature updates, and cloud protection from the dashboard, making it easy to implement and manage advanced security features.

CERTIFICATE MANAGEMENT -
With Scalefusion UEM, you can revolutionize the deployment of digital certificates on your organization's devices and unlock a host of additional benefits that enhance device security. The Certificate Management feature is a game-changer for IT admins, enabling them to effortlessly provision digital identities onto devices without requiring end-user involvement. This means you can easily authenticate devices accessing your organization's Wi-Fi network by pushing digital identity certificates via a certificate payload to managed Windows devices.



Manage OS and App Patches

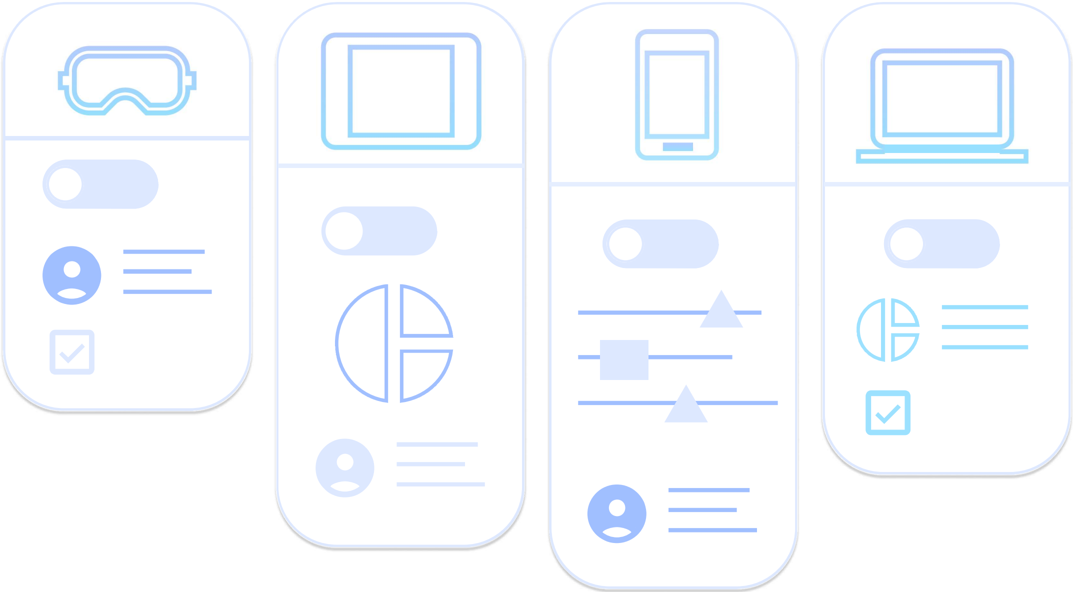
Delays in detecting and fixing third-party applications and OS patch vulnerabilities can leave Windows endpoints open to online exploitation. Ignoring these threats is not an option.

Patch management is a critical process that involves applying updates or patches to OS and apps to fix vulnerabilities, bugs, and security threats. Scalefusion's patch management for Windows offers a comprehensive solution that optimizes IT efforts and reduces costs associated with patching software, OS updates and driver patches. With Scalefusion's patch management, businesses can streamline patching to secure IT environments for end users

Quickly Remediate Device Errors with Remote Troubleshooting

Remote access enables IT teams to take control of a device, regardless of the geographical distance. The most important aspect of this IT tool is remote troubleshooting. Remote troubleshooting is a convenient feature of Scalefusion UEM, where IT admins can troubleshoot device issues without their physical presence or end user involvement. This feature is quite handy and flexible for organizations with a globally distributed workforce as time zone barriers won't disrupt the troubleshooting process. An employee can simply leave his/her Windows device on and the IT admin, irrespective of the local time, can step in for the needful.

Thus, remote troubleshooting using Scalefusion UEM reduces device downtime by enabling IT admins to mirror device screens, troubleshoot issues, and create support tickets with screenshots or recordings. This, in turn, improves employee productivity.



Execute Remote Actions & Troubleshooting

- **Remote Commands -** Scalefusion delivers a robust and versatile suite of remote commands that empower enterprises to take charge of their device management effortlessly. These commands offer an array of powerful options, including the ability to lock/unlock, remote wipe and remote shutdown Windows endpoints.

- **Remote Cast & Control** - This exclusive Scalefusion feature lets IT admins access devices from anywhere, even restarting them remotely if needed. With the added bonus of a remote view, they can see exactly what's happening on the device screen, making managing a breeze.

- **Unattended Access -** Even if the end user is unavailable and the device is unattended, IT admins can still leverage Scalefusion to resolve device issues. Also, Scalefusion's integration with Intel® AMT allows IT admins to troubleshoot Windows devices even when the OS is down, or PC's power is off. The benefit of this is that device downtime is minimized, which, in turn, enhances employee productivity.

- **Workflows** - Scalefusion helps IT admins remotely execute workflows on managed Windows devices. Workflows can be categorized into two types—scheduled and compliance. Compliance workflows are used to send alerts on specific device metrics and vitals and link it to certain actions when the compliance is breached. For example, IT admins can set a specific threshold battery level for devices. When the battery level goes below the threshold, an alert is sent. Scheduled workflows help in scheduling certain tasks and the required action on devices from a selected device group. For example, clearing the cache or app data.

Push and Manage Work Apps

Scalefusion UEM offers a comprehensive approach to application management, which goes beyond simply restricting usage or configuring apps with policies. It includes managing the source from which end users install apps.

One of the primary reasons IT teams manage Windows devices in enterprise environments is to enable employees to accomplish their work as quickly as possible. With Scalefusion UEM, application delivery to managed devices is streamlined. IT admins can push UWP (Universal Windows Platform) app and Win32 apps via the Windows Business Store on managed devices at the time of enrollment. This can be done at any time during the device lifecycle. IT admins can also install a private line of business apps on managed devices, including UWP and MSI apps.

Administrators can also create app groups to increase efficiency and reduce the time it takes to push apps to multiple devices.

Enhance Engagement with Kiosk Mode

So far, we've discussed the settings available within Scalefusion UEM when Windows devices are used by employees. But one of the other popular use cases of Windows devices is kiosks. Kiosks are devices restricted to a single or limited set of functions. Examples of kiosks include self-check-in screens at airports, self-ordering kiosks at quick-service restaurants, and the large, colorful screens displaying movie posters and advertisements in shopping arcades or areas with large footfalls. With the popularity of self-service, kiosks have become an integral part of our daily lives. Apart from branding experiences, kiosk mode devices serve as excellent customer experience enablers, especially in retail and hospitality. Customers can interact with kiosks and submit polls or feedback which are invaluable to business to improve product or service value.

Scalefusion Windows Kiosk Mode can cater to two different use cases by allowing devices to be locked to a single app or multiple apps based on whether they are meant for public use or dedicated use within an organization.

For Windows devices available for public access where a high degree of control is needed, Scalefusion Single App Kiosk Mode enables you to lock devices into a single app mode, and the users can't tab out of the application running on devices.

For Windows devices used by organizations where operations require the use of multiple applications, Scalefusion Multi-App Kiosk Mode helps enable only essential apps and features for employees and limits all extraneous functionalities.

Single and multi-app kiosk mode for Windows can improve employee productivity and heighten device and data security. Kiosk mode devices ascertain that employees aren't spending working hours on apps or websites which are not conducive to productivity. In addition, as kiosks are effectively restricted to specific purposes, accessing malicious websites or applications is out of question. Hence, device and corporate data remains secure.

Windows devices strengthened with Scalefusion UEM can provide a valuable experience for businesses looking to improve efficiency and customer satisfaction.

Enforce Secure Browsing

We spend a lot of time on the internet, predominantly using a web browser to access various online resources. While much of this time may be related to work, prolonged use of the internet and a lack of browser security measures can lead to potential security risks.

It's important to recognize that running an everyday browser can pose several threats to Windows endpoints. Consider all the websites you visit and the transactions you make on your browser. Unsecure websites are the hunting grounds of bad actors and cybercriminals alike. Just a click can lead to irreparable damages in terms of money and data.

Scalefusion UEM enables you to provide your employees with a safe and secure browsing experience, thereby restricting unauthorized access.

Browser Configuration

IT admins can access various configuration settings for Google Chrome and Microsoft Edge web browsers with Scalefusion UEM. These settings include customizing startup preferences, bookmark management, and cookie policies and fine-tuning privacy settings such as browsing history and geolocation. In addition, Scalefusion UEM offers advanced security features to safeguard browsing activity, such as configuring incognito mode settings and managing extensions.

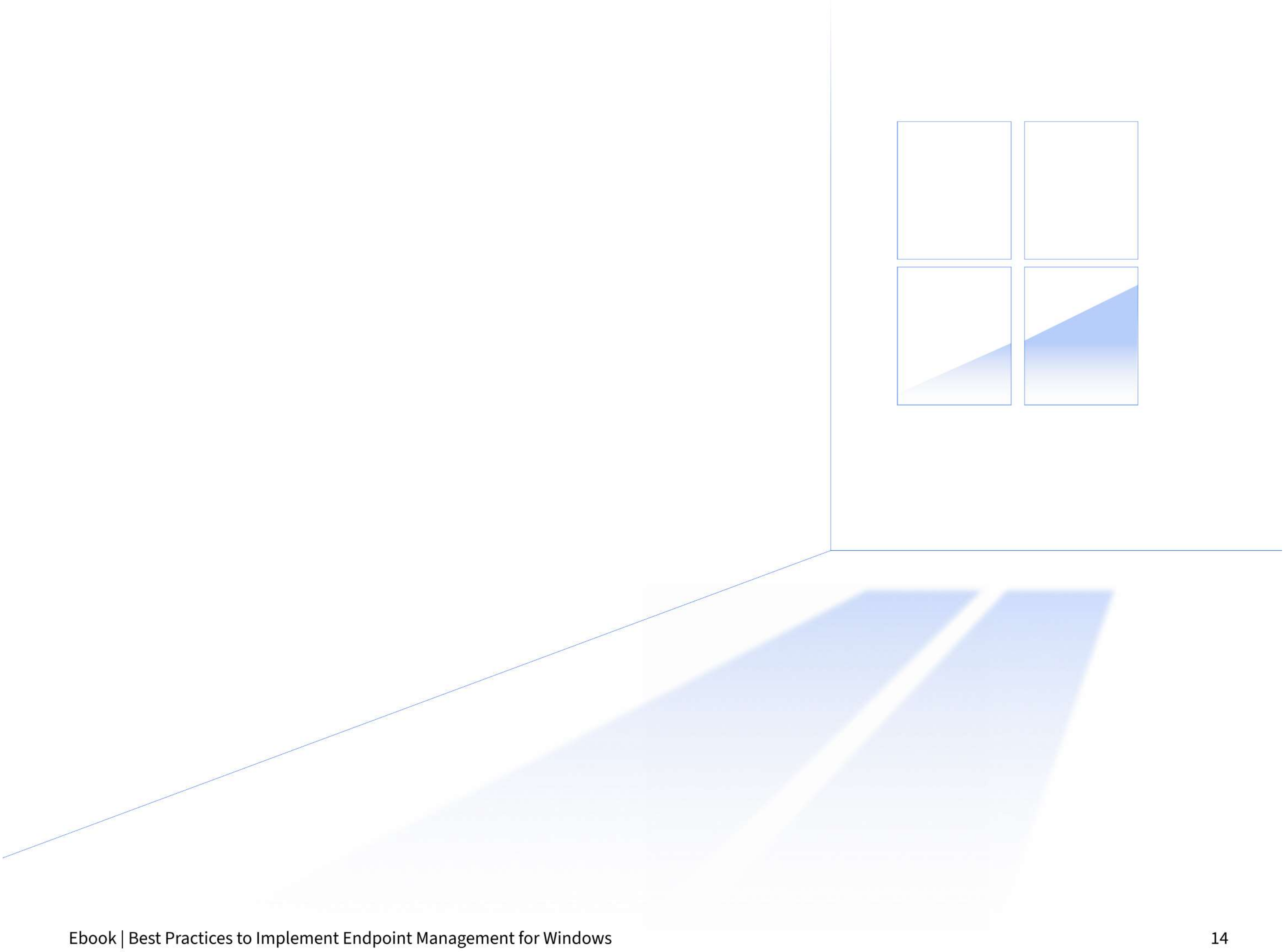
Allowing or Blocking Websites

With Scalefusion, IT teams can ensure secure browsing on the entire Windows device inventory, whether deployed as a kiosk or as a device for employees. IT teams can populate a list of allowed websites within the Google Chrome or Microsoft Edge browser. This helps reduce distractions at work and enables safe browsing, mitigating the threat of malware attacks from untrusted websites.

Scalefusion UEM enables IT admins to configure browser security settings, depending on the purpose that the Windows endpoint serves. These settings include allowing/blocking incognito mode, browser sign-ins and history, and attempts at suspicious websites. All of these ensure that the probability of bad actors gaining access to Windows endpoints is absolute minimum.

Configuring kiosk browsers is also an effective way to deliver exclusive customer experiences. A prime use case of this is in hospitality and healthcare where the same Windows kiosk endpoint is shared between different customers. IT admins can enforce the best privacy levels in such kiosk browsers, maintaining the security and exclusivity of customer data.

There are different types of best practices based on the type of organization or industry you are in. It all boils down to choosing a secure and reliable UEM that helps you extend these capabilities in both offline and online working models. Scalefusion is one such UEM solution that helps you streamline endpoint management and make it as effortless as possible for IT admins.

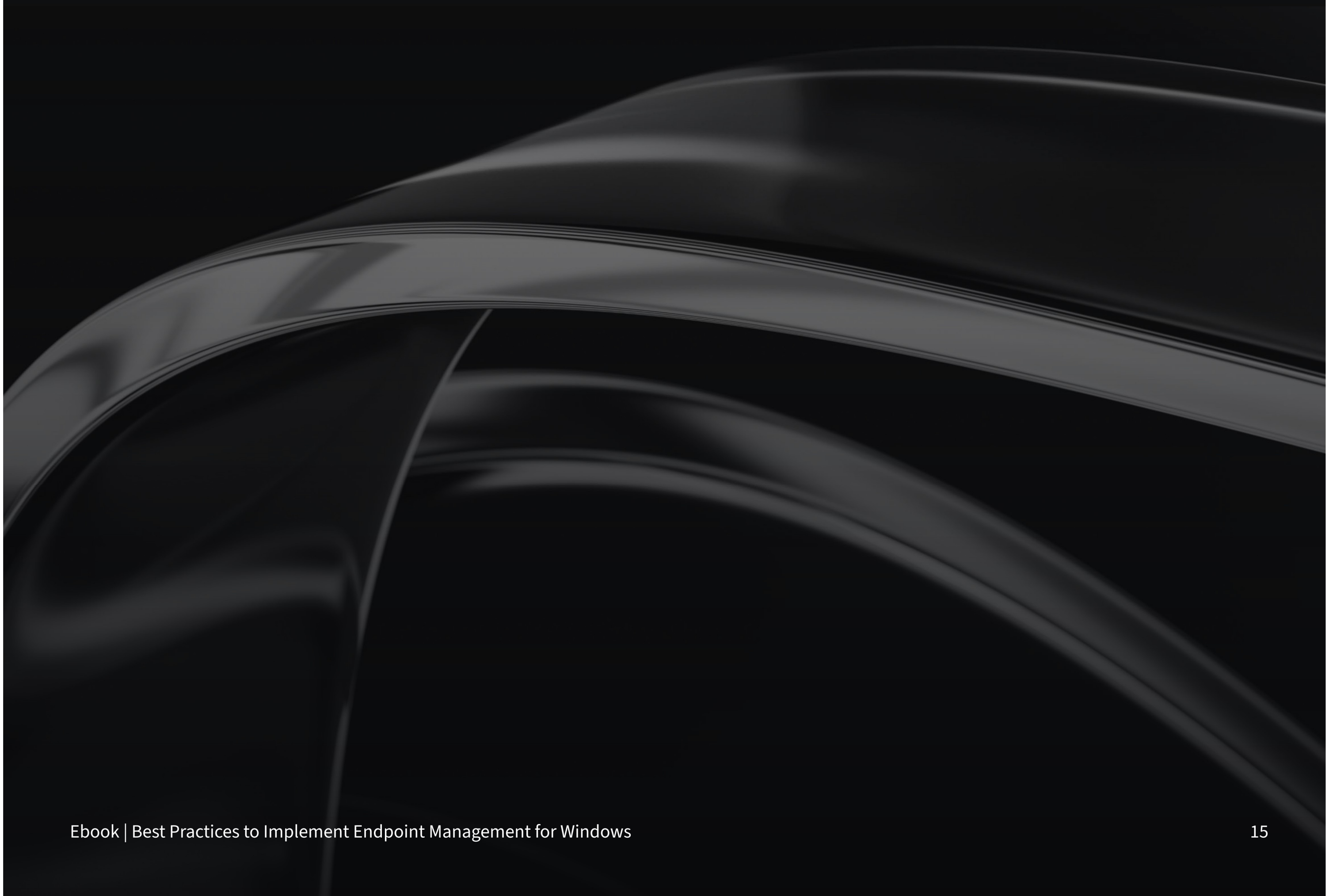


Scalefusion AirThink AI : A Context-Aware Revolution of a Kind

AirThink AI is the revolutionary, chatGPT-powered AI offering from Scalefusion. AirThink AI maximizes OpenAI’s GPT algorithm and is equipped with context-aware intelligence. It combines the best of natural language processing and machine learning for IT teams to take endpoint management a notch above.

AirThink AI allows IT admins to generate Python, Bash, Shell and PowerShell scripts straight up from the Scalefusion dashboard. This empowers IT teams with a more evolved understanding of their in-house scripts through the ‘Validate with AirThink AI’ feature. Now, that’s context-aware intelligence! AirThink AI is therefore a revolution in the world of endpoint management which is set to evolve more in times ahead.

With digital transformation being accelerated across industries and new technologies making headlines everyday, why is Scalefusion just the right fit for your endpoint management needs? Well, let’s answer this by highlighting the reasons that make Scalefusion the best choice of many industry-leading businesses.



Why should you choose Scalefusion UEM for your Windows device management?

Scalefusion UEM solution helps businesses streamline their device management process, ensuring that devices are secure, updated, and compliant with company policies. There are many reasons why you should choose Scalefusion UEM over other vendors; let’s spill the tea:

Salient product features-
Every feature of Scalefusion UEM has the ultimate focus and aim of making the lives of IT teams easier so that all organizational endpoints are managed as desired and remain secure—and Windows is no different. The range of Scalefusion UEM features cover all the elements that are key to ensuring productivity and safety at all levels—endpoints, employees, customers. Some most wanted capabilities that are in high demand amongst our customers are Remote Cast and Control, Patch Management, DeepDive, Workflows, Private App Store Space, ProSurf Kiosk Browser, Content Management, and App Management and many more.

Always dependable, free customer service-
Scalefusion always goes the extra mile to satisfy customers at the end of every interaction. We pride ourselves on our exceptional ability to actively listen to and comprehend the pain points of our valued customers, taking every necessary measure to rectify any issues and providing unwavering support to resolve their queries with utmost urgency, including pre- and post-sales assistance.

Customers can also reach us directly via our active chat support. Our median response time stands at an average of less than 5 minutes and we are available 24*6.

Don’t take our word for it! Ace peer-to-peer review site G2 ranked Scalefusion UEM at 36th position in its 2023 Best IT Management Software rankings. To top it up, Scalefusion holds a 4.5 average rating at G2.

Ultimate Cost Efficiency-
Scalefusion UEM solution offers competitive pricing at a per-device per-month model. Our plans start from $2 and range to $6 per device. Our pricing plans are flexible, with no setup fees and a free 14-day trial period for customers who want to test our product. Businesses can schedule a demo with our team of experts to get started with Windows endpoint management.

Stable, Secure, and Scalable-
Scalefusion is an extremely dependable mobile device management solution that offers a stable and comprehensive set of features and capabilities. We are consistent with our product development, innovation, updates, and patches, which makes us a dependable UEM solution. We prioritize protecting company data by regularly upgrading our security settings and policies, including file, document, and message encryption. Our multi-OS support extends to various endpoints, including company-owned and employee-owned devices like kiosks, smartphones, tablets, desktops, digital signage, mPoS, Android TVs, MacBook Pros, iPads, rugged devices, and more.

Scalefusion is a reliable unified endpoint management solution with proven levels of security. As digitalization shapes the tech future, scalability of any SaaS product is critical. Scalefusion UEM is an ideal solution for organizations because it can adapt to scalability needs. Whether it’s retiring endpoints or an addition of many endpoints, Scalefusion UEM for Windows covers all the bases for organizations.

At Scalefusion, ‘the buck never stops’. We keep updating our current features and add new ones along the way consistently. Our focus will always remain on meeting the customer needs, and thus, we will keep evolving. All the scalability comes with industry-leading technology flexibility.

The Future of Endpoint Management

Famous Roman Philosopher Epictetus once said: “Circumstances do not make the man; they reveal him”, what a mouthful, yet it rings true in the case of endpoint management. The trends governing endpoint management are undergoing a revolutionary change, and it is not enough for organizations to adhere to conventional methods. While present endpoint management systems may efficiently tackle older threats, emerging ones demand a paradigm shift. Hence, embracing change, which is the very law of life, is imperative.

Organizations must not succumb to the easy comfort and routine of the existing system but rather prepare themselves for the expanded and complex world of endpoint management. To navigate through the treacherous waters of the digital world, a robust UEM solution like Scalefusion, known to be up to speed with the market trends, is indispensable. Scalefusion promises to keep organizations enterprise-ready for 2023 and beyond with constant evolution.

Don't miss the opportunity to equip your enterprise with the best Windows endpoint management solution—Scalefusion UEM.

References

1. The Future Of Endpoint Management by Forrester

2. McKinsey Technology Trends Outlook 2022

Scalefusion

Harness the Power of Scalefusion to Manage the Endpoints of Today and Tomorrow

partners@scalefusion.com

sales@scalefusion.com