Infosys topaz

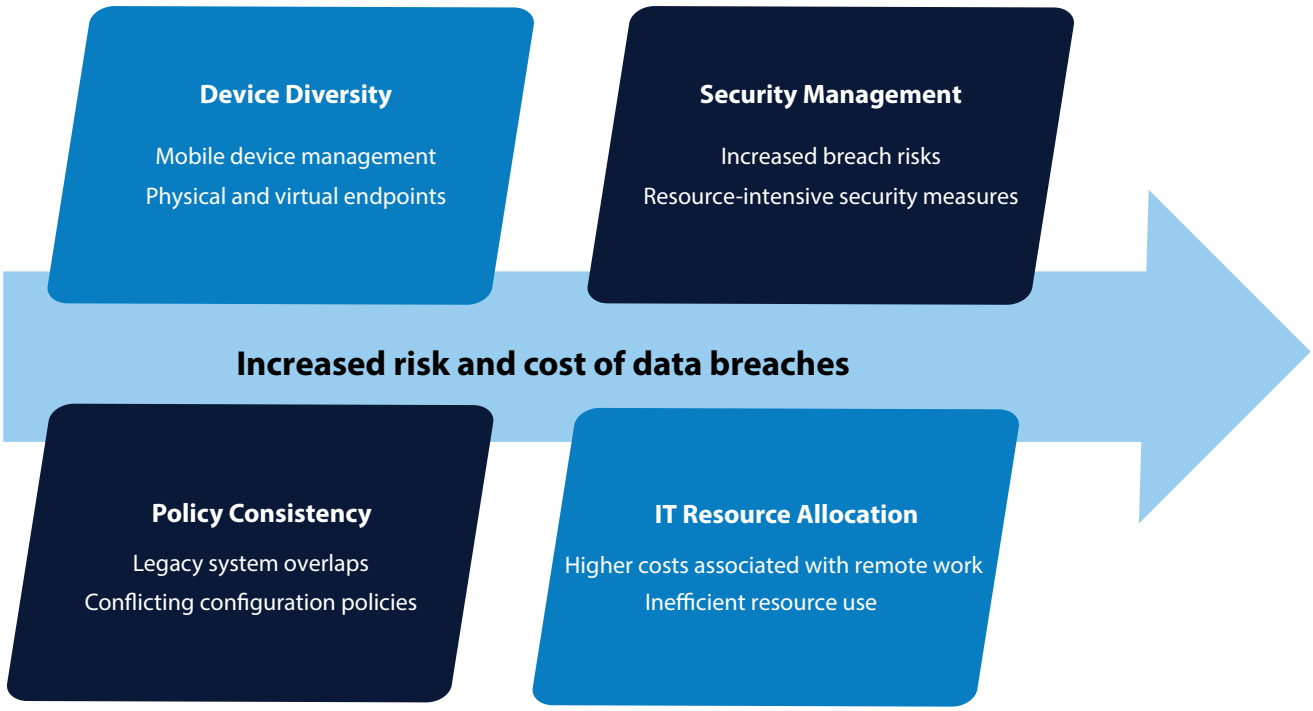
VIEW POINT

MODERNIZING ENDPOINT MANAGEMENT IN A HYBRID WORLD: RESOLVING COMPLEXITY WITH AI-DRIVEN SOLUTIONS

Infosys
Navigate your next

As organizations move towards a hybrid work culture, managing IT environments becomes more complex and diverse. Modern Endpoints now span physical desktops, laptops, mobile devices, and virtual Windows 365 Cloud PCs. However, for large organisations, managing device configurations, security and policy consistency across these platforms has introduced significant complexity—from conflicting configuration policies to legacy system overlaps. These issues increase the risk of breaches and consume valuable IT resources. [1]IBM reported that data breaches cost, on average, 28% more when remote work was involved (USD 4.96 million) compared to those without it (USD 3.89 million).

Challenges in Managing Hybrid IT Environments



Pain points: In today's hybrid work environment, organizations manage a diverse array of endpoints—including Windows, macOS, iOS, Android, and Linux—each with unique configuration requirements. This diversity can lead to misconfigurations, mismanagement and other issues. [2]As per Gartner, it causes major data security breaches.

Transitioning from legacy systems to modern cloud management often results in overlapping and inconsistent policies, creating security gaps and compliance issues. Additionally, multiple policies can generate false positives, overwhelm IT teams, and consume significant administrative resources. Forrester research indicates that manual resolution of these conflicts can consume up to [3]25% of an IT admin's troubleshooting time, significantly delaying incident response. Moreover, efficient power management across various devices is challenging, leading to increased energy consumption and operational costs. Without regular updates, legacy policies may deviate from current security standards, leading to inconsistency across endpoints. This also causes a manual support burden: some organizations report a [4]20–40% increase in helpdesk tickets related to configuration issues, driving up costs and diverting resources from strategic projects which ultimately increases operational costs.

Introducing the Total Endpoint Experience Platform: A New Paradigm in Total Endpoint Experience

In today's hybrid work environment, traditional endpoint security solutions often overlook the human experience and sustainability. Proposing a transformative **Total Endpoint Experience Platform** that unifies robust security, sustainable operations, and enhanced digital well-being through AI-driven innovation. This solution integrates advanced machine learning, edge computing, and real-time analytics to optimize endpoint management across diverse devices.

1. **AI-Driven Unified Endpoint Security:** Traditional endpoint security often struggles with misconfigurations and compliance issues, leading to security breaches. The **Total Endpoint Experience Platform** introduces **Autonomous Misconfiguration Remediation**, where AI continuously monitors system settings, predicts potential misconfigurations, and automatically corrects them before they cause vulnerabilities. This ensures a proactive security approach, reducing manual IT interventions. This will also help in policy management centrally.

   In addition, **Self-Healing Endpoints** empower devices to automatically roll back unauthorized changes or security threats without user intervention. This feature minimizes downtime and ensures endpoints always remain compliant with security policies. This will also reduce the IT team's interventions.

2. **Sustainability-Driven Endpoint Management:** Energy efficiency and sustainability are becoming critical for enterprise IT strategies. The **AI-powered energy Optimization** feature in this platform analyses power usage patterns across devices and intelligently manages the power usage for updates and other tasks. This reduces the organization's carbon footprint and helps meet sustainability goals and reduces the operational cost.

3. **Total Human Experience & Digital Wellbeing:** With increasing screen time and digital overload, IT systems must prioritize user well-being. The **AI-Powered Cognitive Load Reduction** feature in this platform ensures that security alerts are prioritized based on urgency, reducing non-critical notifications and allowing employees to focus on their core tasks without distraction. This will help to reduce Alert Overload.

   Personalized IT Support with NLP (Natural Language Processing) capability enables users to describe technical issues in plain language, while AI generates step-by-step remediation instructions – which will reduce the L1 ticket count significantly.

   This reduces dependence on IT helpdesks and speeds up issue resolution, enhancing the overall end-user experience.

4. **AI-Guided Cost Optimization & IT Efficiency:** IT budgets are often strained due to inefficient software licensing and hardware maintenance costs. The **Automated Software License Rationalization** feature analyses application usage patterns and flags unused or redundant software subscriptions, helping organizations cut unnecessary IT expenses.

   To further reduce costs, introducing **Predictive IT Maintenance dashboard**, which uses AI to monitor hardware health and forecast potential failures before they occur. This enables pre-emptive repairs, reducing device downtime and extending hardware longevity.

**Sources: [1,2,3,4] The business case for endpoint management modernization according to Microsoft | Microsoft 365 Blog*

Comprehensive Endpoint Security Solution

AI-Driven Security
Autonomous misconfiguration remediation and self- healing endpoints

Sustainability Management
AI-powered energy optimization to reduce carbon footprint

Human Experience
Cognitive load reduction and personalized IT support

Cost Optimization
Automated license rationalization and predictive maintenance

Business Impact

Enhanced Security Posture - Automated detection and remediation lower breach risk by *[5]30-50%.

Operational Efficiency - Automation cuts manual troubleshooting time by *[6]25-40%, freeing IT teams for strategic work.

Cost Savings - Streamlined device provisioning and reduced support tickets help lower the total cost of ownership across the device landscape.

**Sources: *[5,6]Cross-border GenAI misuse to drive 40% of AI data breaches by 2027*

Modernizing endpoint security with AI and automation can significantly enhance an organization's security and operational efficiency. Security misconfigurations are a leading cause of data breaches, [*7]accounting for approximately 31% of incidents. By implementing automated detection and remediation, organizations can swiftly identify and correct these vulnerabilities, thereby reducing the risk of breaches.

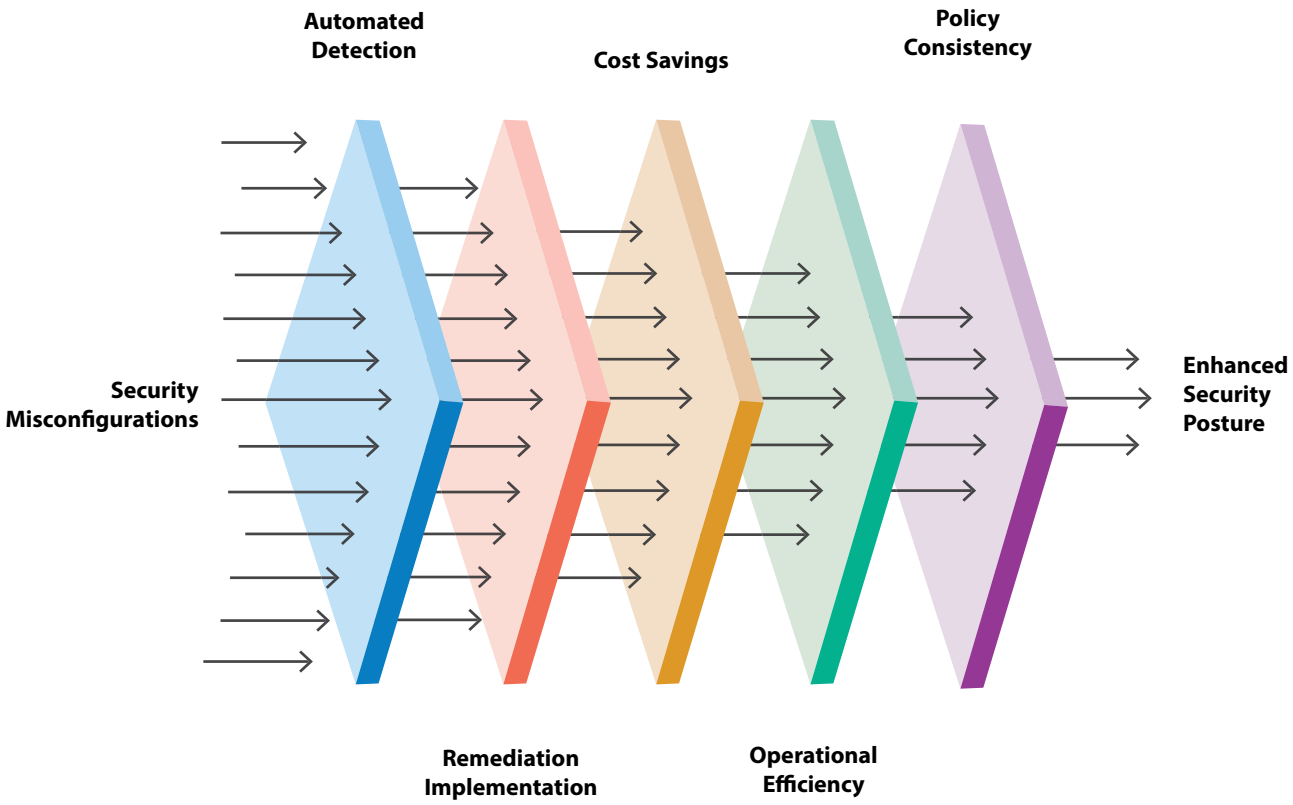
For large enterprises managing thousands of endpoints, automation offers significant advantages. Automating endpoint security and asset management can save organizations an average of [*8]$3.4 million annually. This substantial cost reduction is achieved through decreased manual intervention, fewer security incidents, and improved compliance.

In addition to cost savings, automation enhances IT operational efficiency. [*9]By automating routine security tasks and remediation workflows, organizations can reduce the workload on IT teams, allowing them to focus on more strategic initiatives. This shift not only improves productivity but also accelerates incident response times, further strengthening the organization's security posture.

Moreover, automating endpoint management ensures consistent enforcement of security policies across all devices, minimizing the risk of non-compliance, managing the power usage and associated penalties (SLAs). This consistency is crucial for maintaining a robust security framework and protecting sensitive data.

*Sources: [*7]*Cloud Breaches Impact Nearly Half of Organizations - Infosecurity Magazine*
*[*8]| Absolute Security*
*[*9]Endpoint Detection and Response (EDR) Buyers' Guide 2025*

Enhancing Security and Efficiency through Automation



Conclusion

AI-driven and automated endpoint security solutions are vital for organisations navigating today's complex IT environment. They enhance security, lower operational costs, and boost efficiency, making them essential rather than just an upgrade. However, challenges such as high implementation costs, integration with legacy systems, potential false positives in threat detection, and the need for compliance pose hurdles. Despite these issues, the long-term benefits of automation and improved security make AI-powered endpoint management a worthwhile investment for large future-ready enterprises.

About the Author

Souvik De
Pre Sales Consultant, Infosys Limited

Souvik De is a skilled Pre-Sales Consultant in Microsoft Modern Workplace, driving strategic deal pursuits across the US with expertise in RFX management, pricing strategy, and solution development. He collaborates with sales and solution teams to craft tailored, value-driven proposals that accelerate digital transformation for enterprise clients.

Infosys Topaz™ is an AI-first set of services, solutions and platforms using generative AI technologies. It amplifies the potential of humans, enterprises, and communities to create value. With a vast repository of AI assets, pre-trained AI models, 10+ AI platforms steered by AI-first specialists and data strategists, and a 'responsible by design' approach, Infosys Topaz™ helps enterprises accelerate growth, unlock efficiencies at scale and build connected ecosystems. Connect with us at infosystopaz@infosys.com.

For more information, contact askus@infosys.com

Infosys®
Navigate your next