



The Executive Guide to **Autonomous Endpoint Management**

Why enterprise IT leaders are making the shift to Autonomous Endpoint Management, and what it takes to get there

Introduction

Most IT leaders we talk to already have a clear view of the pressures reshaping endpoint operations. Patch cycles are harder to sustain. Critical vulnerability response demands more coordination than ever. Audit readiness depends on confidence in data that is often spread across multiple fragmented systems.

The question is no longer whether endpoint management needs to evolve. It is whether organizations can continue to meet the demands of speed, scale, security, and governance with a management model built for a different era. Incremental improvements are no longer enough. The next step is a fundamental operating model shift: Autonomous Endpoint Management. By combining trusted data, AI-driven intelligence, automation, and governance, Autonomous Endpoint Management enables organizations to move from reactive administration to proactive, self-healing operations. This eBook explores why that shift is necessary, how to adopt it safely and confidently navigate the journey from traditional management to autonomous operations, and the outcomes leading organizations are already achieving.

What you'll learn



Why autonomous endpoint management is becoming a strategic necessity



What success looks like in practice



A roadmap for adoption



The business and operational outcomes leaders can expect

CHAPTER 1

Autonomous Endpoint Management: a strategic imperative

Increasing risk, operational complexity and AI-accelerated expectations demand a new endpoint operating model

Enterprise IT is Entering Its Next Evolution.

AI has compressed the window between vulnerability discovery and active exploitation from weeks to hours. Threats today don't wait for the next patch cycle. Yet most organizations are still operating endpoint management and remediation models designed for a slower, more predictable era, one where environments were relatively static, maintenance windows were reliable and manual validation was a reasonable approach to confirming compliance.

That world no longer exists. And the gap between how fast threats move and how fast most organizations respond has become both the defining operational challenge and the defining business risk of the moment.

In today's environment:

- Vulnerabilities are identified continuously, not monthly
- Exploits spread in hours or minutes
- Devices join and leave the environment dynamically
- Work happens everywhere, not just on the network

AI has compressed response time expectations across IT and Security. What once took days now must happen in minutes. What once required manual review must now be automated or eliminated entirely.

Only 32% of organizations currently operate at advanced automation maturity.

The problem isn't a shortage of tools. We find that most organizations have invested significantly in endpoint management capabilities. The problem is visibility and trust. Tech sprawl has fragmented data. Asset inventories don't align with vulnerability scanners. Compliance status depends on manually reconciled reports. Security and IT teams lack a shared, authoritative view of what exists, what state it's in and whether remediation has succeeded. Without that foundation, even well-resourced teams operate on assumed compliance rather than verifiable truth.

This is why autonomous endpoint management has shifted from an emerging concept to a business requirement. It enables organizations to continuously discover, prioritize, remediate, verify and heal endpoint

issues at machine speed and at enterprise scale. But autonomy cannot safely operate on fragmented data.

It requires a unified system of record: A governed, continuously updated operational record that Autonomous Endpoint Management activates.

This chapter builds the case. It examines why traditional models have reached their structural limit, how visibility and patching failures persist despite growing investment and why data authority is now the non-negotiable prerequisite for operating with confidence in an AI-accelerated world.

The AI Speed Mismatch: Why Traditional Models Fall Behind

AI has fundamentally changed the pace of endpoint operations.

Threats emerge faster, environments change constantly, and vulnerabilities can be exploited within hours of discovery. Yet many organizations still rely on manual processes, scheduled maintenance windows, and periodic verification to manage endpoint health and security.

This creates a growing gap between how quickly risk appears and how quickly organizations can respond.

Traditional approaches were designed to help teams manage endpoints.

Autonomous Endpoint Management is designed to help organizations continuously discover, assess, remediate, verify, and heal endpoint issues at machine speed while maintaining human oversight and governance.

The goal is not simply faster patching. It is continuous resilience.

When endpoint operations become autonomous, organizations can reduce exposure windows, improve compliance confidence, and free IT teams to focus on higher-value strategic initiatives rather than repetitive manual tasks.

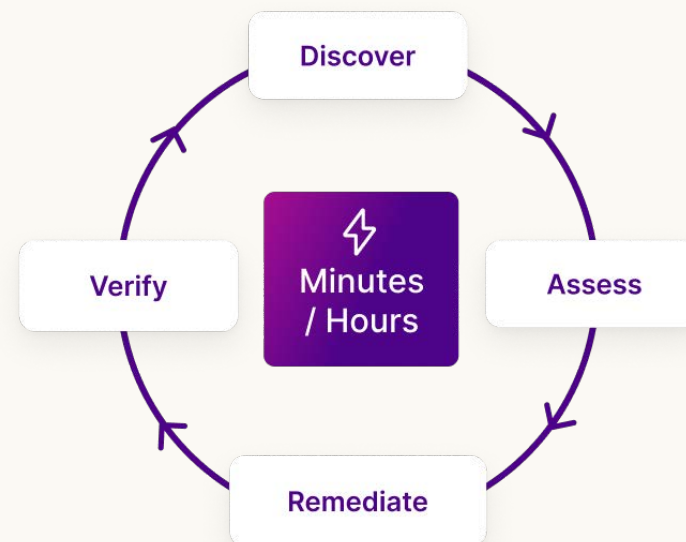
Traditional Endpoint Operations

Periodic discovery, manual decision-making, scheduled remediation, and delayed verification create gaps between identifying risk and resolving it.



Autonomous Endpoint Management

Continuous discovery, contextual decision-making, automated remediation, and verified outcomes help organizations respond at the speed modern environments demand. This loop is powered by trusted data and operates within policy and human oversight.



Visibility Gaps Are The Real Risk Multiplier

Most organizations don't struggle with endpoint management because they lack tools. They struggle because they lack a trusted view of their environment.

As endpoint ecosystems grow more complex, visibility gaps create uncertainty across security, compliance, and operations. When IT teams can't confidently identify devices, vulnerabilities, configuration drift, or remediation failures, risk increases while confidence falls.

Autonomy requires trusted visibility. Without it, organizations hesitate to automate and remain stuck in reactive operations.

Autonomy can't operate in uncertainty.
Without trusted visibility, organizations hesitate to automate, and that hesitation creates exposure. Patch management has evolved from a task to a systemic problem.

Autonomous Patching: The Foundational Autonomous Endpoint Management Use Case



Patching is no longer about deploying updates. It is about continuously reducing risk and verifying outcomes.

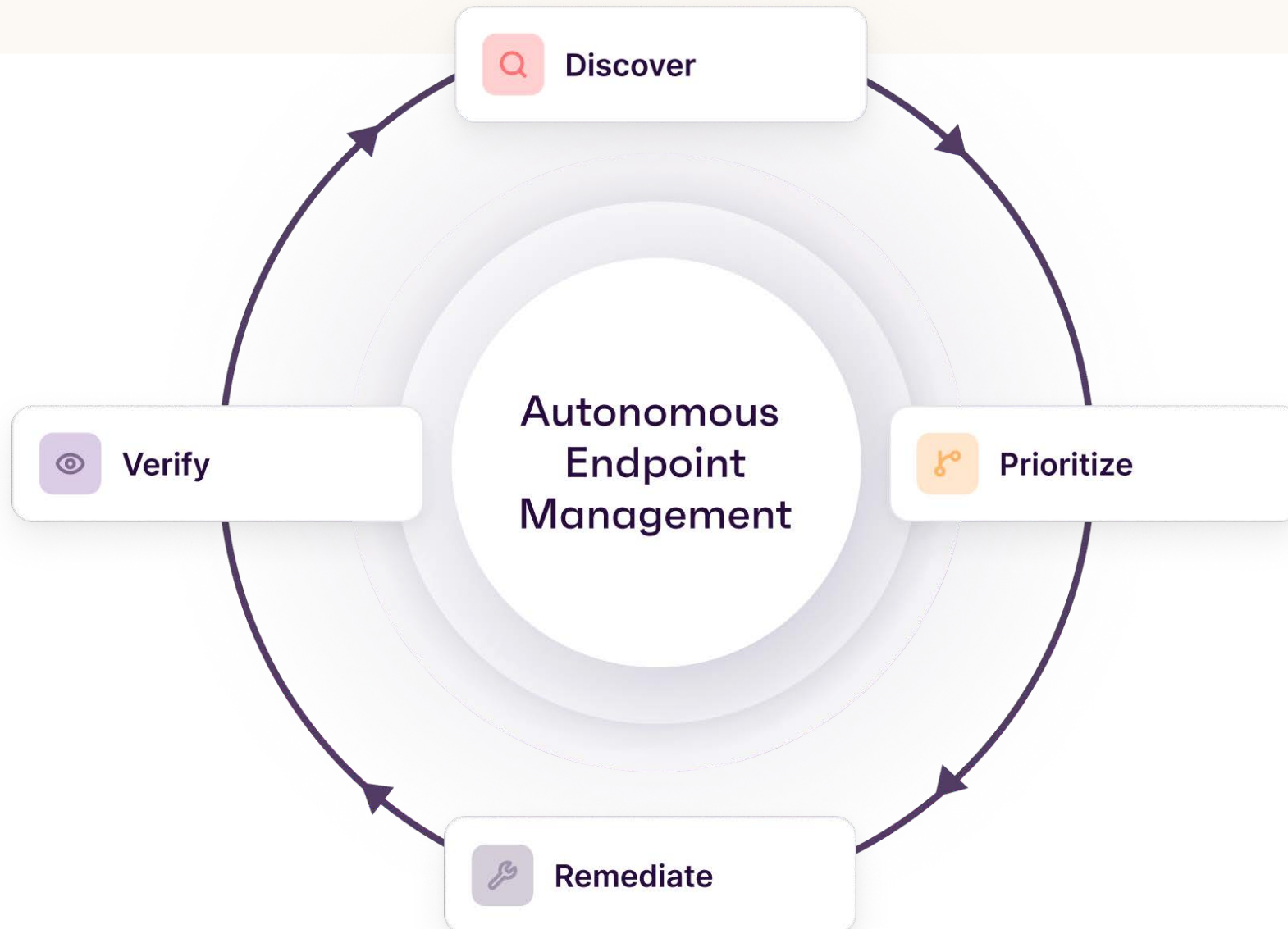
Traditional approaches measure deployment success, but often miss whether vulnerabilities were eliminated, endpoint health improved, employees remained productive, or business objectives were achieved.

Autonomous Endpoint Management (AEM) changes the model. Powered by trusted data, business context, AI, automation, and governance, AEM creates a closed loop of discovery, prioritization, remediation, and verification. Autonomous patching is a foundational AEM use case that demonstrates how endpoint operations can move from reactive administration to autonomous, outcome-driven execution.

Success is no longer measured by patches deployed. It is measured by verified outcomes: reduced exposure, improved resilience, better employee experiences, and stronger business performance. This closed-loop model provides the foundation for Autonomous Endpoint Management as the next operating model for endpoint operations.

What is Autonomous Endpoint Management?

Autonomous Endpoint Management is a modern operating model that continuously discovers, assesses, remediates, verifies and heals endpoint issues at enterprise scale. Unlike traditional automation, which follows predefined rules, autonomy continuously evaluates conditions, acts based on context, and verifies outcomes while maintaining human oversight.



How Autonomous Endpoint Management Changes The Operating Model

Organizations adopting Autonomous Endpoint Management move from periodic maintenance activities to continuous outcome-driven operations. The result is greater resilience, stronger compliance, and more time for teams to focus on strategic priorities.



Traditional Operations

Episodic Patching

Reactive Response

IT Firefighting

Manual Validation



Autonomous Operations

Continuous protection

Verified compliance

Improved Employee Experience

Increase in IT teams capacity

Looking ahead

In Chapter 2, we dive into a real Autonomous Endpoint Management use case. See how SouthStar Bank successfully implemented Autonomous Endpoint Management inside a compliance environment where a misconfigured endpoint or a missed patch has regulatory consequences.

CHAPTER 2

What Does Successful Autonomous Endpoint Management Look Like in Practice?

SouthStar Bank demonstrates how organizations can move from fragmented visibility and manual remediation to continuous compliance, autonomous remediation, and verified outcomes.

Executive Summary

SouthStar Bank demonstrates what Autonomous Endpoint Management looks like in practice. Faced with growing compliance requirements, fragmented visibility, and increasing endpoint complexity, the bank established a unified system of record and adopted Autonomous Endpoint Management to move from reactive operations to continuous, verified remediation.

Challenge

- Fragmented endpoint visibility
- Manual validation processes
- Increasing compliance pressure
- Lack of confidence in remediation outcomes

Approach

- Unified system of record
- Continuous endpoint visibility
- Autonomous remediation workflows
- Automated verification

Outcome

- Verified compliance
- Faster response to vulnerability events
- Increased operational confidence
- Reduced manual effort

“I was able to reach out and touch everything and really get information, and see the power of viewing, analyzing, solving problems quickly..to where we could basically see what was happening and solve problems before our customers knew they had them.”

— Jesse Miller, SouthStar Bank





**“I don’t want to just respond.
I want to remediate before they
know or be able to remediate
with one click.”**

— Jesse Miller, SouthStar Bank

The Operational Reality in Regulated Environments

Banks operate with little margin for uncertainty. Endpoint failures can interrupt frontline staff, disrupt customer interactions and introduce regulatory exposure. At the same time, vulnerability discovery is accelerating, and device environments are constantly changing.

At SouthStar Bank, IT teams were responsible for managing endpoints across a highly dynamic environment. Traditional workflows depended on manual confirmation and delayed validation, leaving teams uncertain whether remediation efforts had actually succeeded.

ivanti

This clarity did not exist before autonomy. Leadership recognized that without continuous visibility and verification, patching cycles created anxiety rather than confidence.

Why SouthStar Needed A Different Operating Model

SouthStar’s challenge was not a lack of tools. It was a lack of certainty. Teams needed a way to continuously understand endpoint health, verify remediation outcomes, and respond to issues before they impacted users or introduced compliance risk.

The First Step: Establish Data Authority

SouthStar first established a trusted system of record, creating a single source of truth for endpoint visibility, configuration state, remediation status, and compliance posture.

With trusted data in place, teams could confidently identify risk, prioritize action, and verify outcomes.

Autonomous Endpoint Management in Practice

With trusted data in place, SouthStar connected visibility, remediation, and verification into a continuous operating model.

Endpoint issues could be identified, remediated, and validated automatically, while exceptions were escalated to IT teams when human intervention was required.

This allowed engineers to focus on complex issues rather than managing routine endpoint operations.

Continuous Patch Compliance During High-Risk Events

The value of autonomy became most apparent during critical vulnerability incidents.

Rather than scrambling to coordinate patching efforts, SouthStar relied on autonomous workflows to:



“We have bots that are built into the device, and it’s almost a one click resolution. It makes it less stressful and makes it better for everyone involved.”

— Jesse Miller, SouthStar Bank

Business Outcomes Beyond Efficiency

SouthStar achieved more than operational efficiency. Continuous visibility and verified remediation increased confidence, reduced exposure, and allowed IT teams to focus on higher-value work.

Key Lessons For Enterprise Leaders

SouthStar Bank's experience highlights lessons applicable to any enterprise:

1

Trust Enables Autonomy

Organizations cannot automate decisions they do not trust.

2

Continuous Compliance Is The New Standard

Periodic validation can no longer keep pace with modern risk.

3

Autonomous Operations Create Strategic Capacity

Teams spend less time reacting and more time driving business outcomes.

Looking ahead

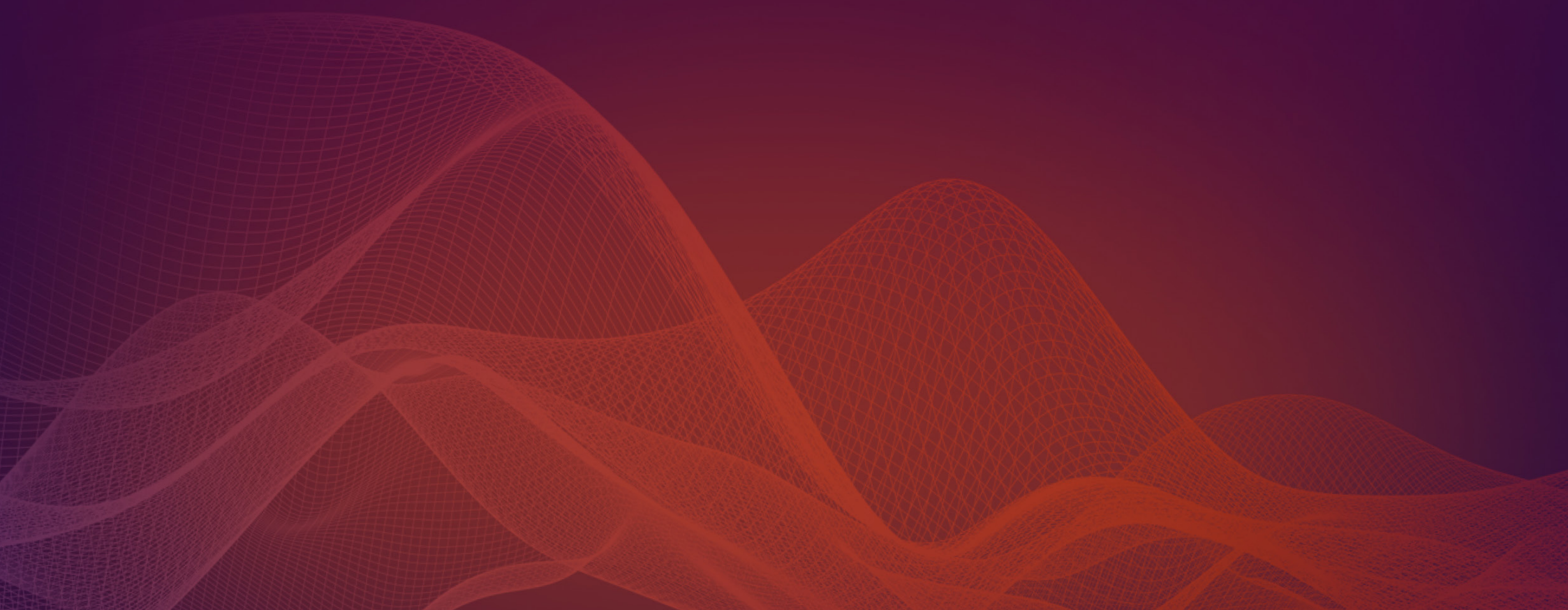
SouthStar Bank resolved the proof question. The harder question for most leadership teams is: how do you move toward an autonomous operating model without creating new exposure along the way?

The answer is a phased approach, and the order of the phases isn't negotiable. Skipping steps accumulates risk that surfaces later at a worse time.

CHAPTER 3

A Leader's Roadmap to Autonomous Operations

A phased framework for sequencing the shift with confidence



Executive Summary

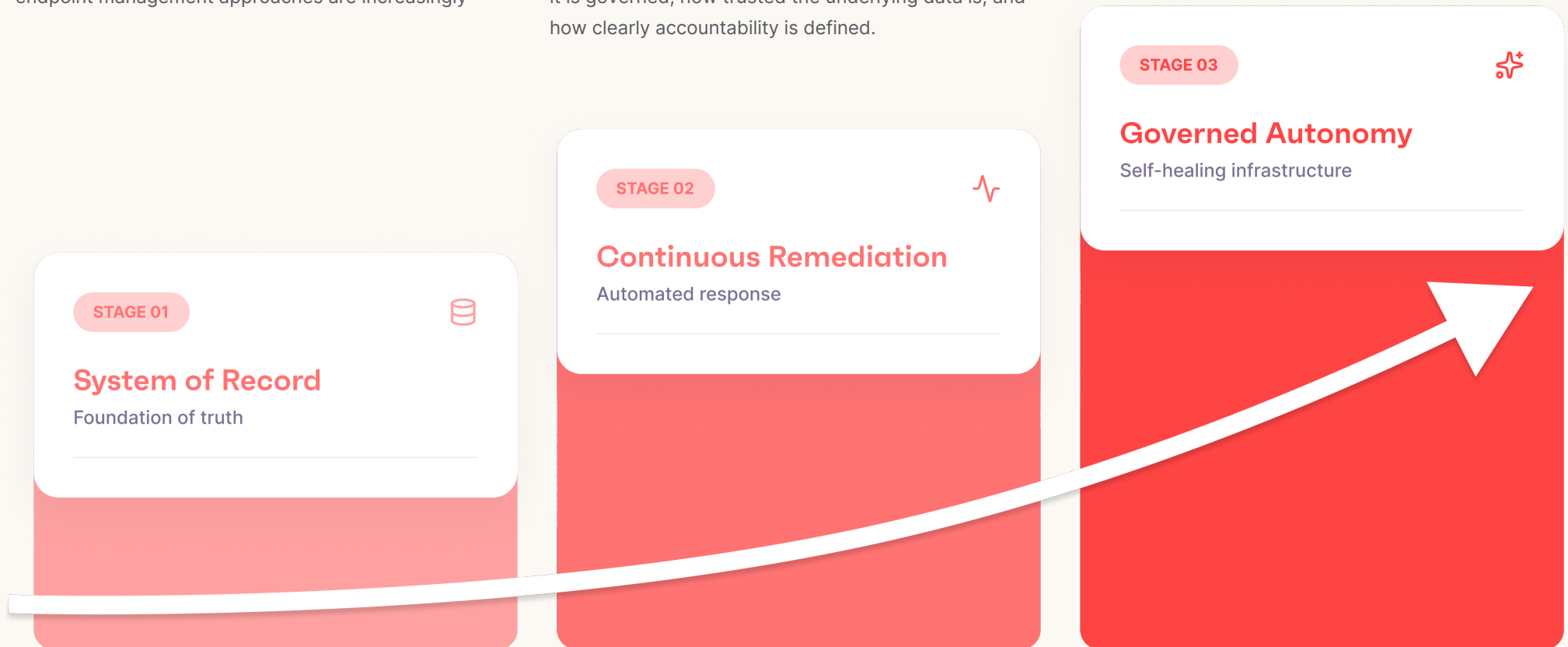
Organizations that treat Autonomous Endpoint Management adoption as a single decision, a capability to deploy rather than a foundation to build, consistently stall or introduce unintended risk.

As enterprise environments become more dynamic and threats move at machine speed, traditional endpoint management approaches are increasingly

unable to deliver the confidence, control and resilience business leaders require. Manual processes, periodic patching and fragmented visibility may have been enough in the past, but they cannot scale to meet modern expectations.

Leading organizations recognize that autonomy must be introduced deliberately. Success depends not on how quickly automation is deployed, but on how well it is governed, how trusted the underlying data is, and how clearly accountability is defined.

The framework below is designed for organizations that want to move with operational confidence. It covers the maturity stages, governance requirements and accountability structures that determine whether an autonomous model delivers durable value. How well it is governed matters more than how fast it is deployed.



Confidence, automation and business value increase



Why Autonomy Is a Leadership Decision

Autonomous Endpoint Management is not simply an IT initiative. It influences cyber resilience, compliance posture, employee experience, and operational efficiency across the enterprise.

As systems begin making decisions and orchestrating remediation at scale, leaders must define the policies, guardrails, and outcomes that govern autonomy.

The organizations seeing the greatest value from autonomy treat it as an operating model transformation, not a technology deployment.

The Maturity Reality: Autonomy Is a Journey

Organizations do not become autonomous overnight.

Leaders typically progress through three stages:

Stage 1: Establish Trusted Visibility

Stage 2: Enable Continuous Remediation

Stage 3: Scale Governed Autonomy

Each stage increases organizational confidence, operational resilience, and business value.

Stage 1: Establish Trusted Visibility

Every autonomous journey begins with visibility. Organizations must first create a trusted view of endpoint health, risk, compliance, and ownership across the environment.

This foundational layer creates the confidence needed to make decisions based on data rather than assumptions.

Key Capabilities:

- Trusted endpoint inventory
Unified visibility across tools
- Real-time compliance insight
- Reliable asset intelligence

Without this foundation, teams spend time reconciling data instead of reducing risk. Automation initiatives stall because leaders hesitate to allow systems to act on incomplete or inconsistent information.

For executives, this stage is about confidence. When leaders can trust the data, they can trust the decisions built on it.



BUSINESS OUTCOME

Better Visibility

Leaders gain a trusted understanding of what exists, what is at risk, and where action is required.

Stage 2: Enable Continuous Remediation

Once trusted visibility is established, organizations can move beyond periodic maintenance and begin operating continuously.

Endpoint issues are detected, prioritized, remediated, and verified in an ongoing cycle, reducing exposure and improving operational responsiveness.

Key Capabilities

- Continuous monitoring
- Risk-based prioritization
- Autonomous remediation
- Outcome verification
- Exception management
- AI-guided recommendations



BUSINESS OUTCOME

Faster Outcomes

Issues are identified and resolved more quickly, with less manual effort and greater confidence in remediation success.



Stage 3: Scale Governed Autonomy

At the highest level of maturity, organizations enable systems to take action at scale while maintaining oversight, accountability, and business control.

The goal is not to remove humans from the process. The goal is to ensure routine decisions happen autonomously while exceptions are escalated to the right people.

How Governed Autonomy Works

Assist

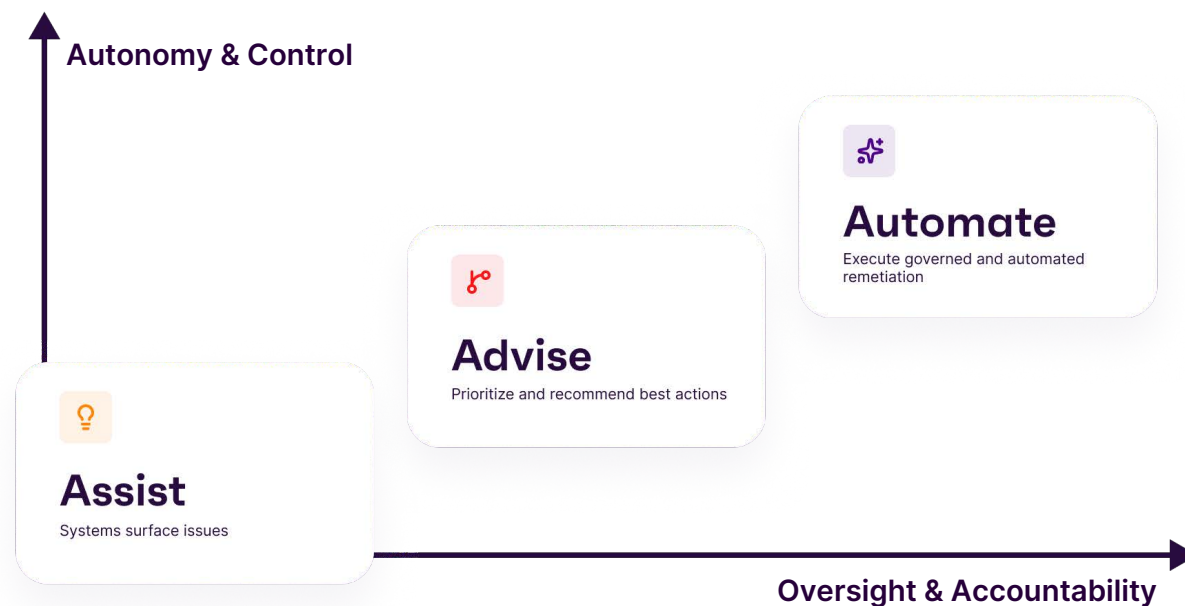
Systems identify issues

Advise

Prioritize and recommend the best actions

Automate

Systems execute approved actions autonomously and escalate exceptions when human involvement is required



Key Capabilities

- Human-in-the-Loop Governance
- Policy-Driven Automation
- Autonomous Decision Execution
- Exception-Based Workflows
- Continuous Optimization



BUSINESS OUTCOME

Increased Resilience

Organizations improve security, compliance, and operational performance while enabling teams to focus on higher-value work.

Redefining The Roles of IT and Security Teams

As autonomy increases, the role of IT and security teams evolves.

Instead of spending time on repetitive tasks like manual checks, remediation, retries and data reconciliation, teams instead:

- Tune and optimize automated workflows.
- Define and refine policy and governance.
- Focus on high impact exceptions and emerging risks.
- Partner more closely with the business on strategic initiatives.

Autonomous Endpoint Management does not reduce the need for human expertise. It elevates it by removing noise and enabling teams to work where informed decision making and judgment matters most.

Measuring Success at the Executive Level

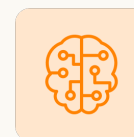
Because Autonomous Endpoint Management is a strategic shift, success must be measured differently. Executive-level metrics focus on outcomes, not activity. These metrics tell leaders whether autonomy is delivering on its promise:

faster response times, lower risk and greater resilience.



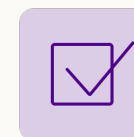
Time to Remediate

How quickly issues are resolved



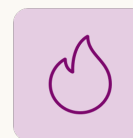
Autonomous Resolution %

Issues solved without intervention



Compliance Confidence

Real-time compliance visibility



User Experience Improvement

Reduction in employee disruption



Strategic Capacity Created

Time returned to IT teams

The Advantage of Acting Now

Organizations that establish trusted visibility, implement continuous remediation, and scale governed autonomy gain a measurable advantage in security, compliance, operational efficiency, and employee experience.

Those that continue relying on fragmented data, manual validation, and reactive remediation will find it increasingly difficult to keep pace with modern endpoint complexity.

The question is no longer whether organizations will move toward autonomy.

The question is how quickly they can realize its value.



3 Foundations of Autonomous Endpoint Management



Trusted Visibility



Continuous Remediation



Governed Autonomy

Looking ahead

The next chapter explores the business outcomes organizations can achieve when these capabilities work together.

CHAPTER 4

The Business Case for Autonomous Endpoint Management

The operational and financial case for acting now

Executive Summary

Enterprise IT and security leaders face a structural imbalance: operational complexity is increasing faster than human led processes can scale. Distributed endpoints, AI accelerated vulnerability discovery, and continuous compliance requirements have exposed the limits of traditional endpoint management models.

Autonomous Endpoint Management addresses this imbalance by replacing periodic effort with continuous, verified outcomes. Rather than relying on manual intervention and reactive workflows, autonomous systems discover, prioritize, remediate, verify, and heal issues automatically, at enterprise scale.

The business case rests on four measurable dimensions:

1. **Operational efficiency**
2. **Security and compliance effectiveness**
3. **Cost reduction**
4. **Strategic capacity creation**

Operational Efficiency Gains

The efficiency advantage of autonomous endpoint management is measurable, and the gap between organizations that have built toward it and those that haven't is widening faster than most expect. Our [2026 Autonomous Endpoint Advantage Report](#) found that only **32%** of organizations currently operate at advanced automation maturity, and those organizations consistently outperform their peers on threat response speed, operating cost predictability and the strategic capacity of their IT teams. The rest rely on partial automation that still requires human intervention for complex or high-risk issues.

Ivanti validated this internally as [Customer Zero](#):



Autonomous Endpoint Management enables teams to scale outcomes without scaling operational complexity.

66,000

manual tasks automated annually.

60%

 of IT operations automated.

Thousands

Users supported globally by a lean IT organization.

Faster Issue Resolution

Traditional endpoint workflows wait for users to experience problems before remediation begins. Autonomous systems reverse this model.

Issues are detected early, remediated immediately and verified automatically, often within minutes.

The productivity implications are significant. That same [research](#) revealed that today's employees experience 6.3 technology interruptions per month, costing 1.6 hours of productivity per employee.

Autonomous remediation directly reduces these interruptions by preventing incidents before users are impacted.

Every endpoint disruption carries a measurable business cost.

6.3 Technology disruptions per employee each month

1.6 HOURS Monthly productivity lost per employee

Improved End-User Experience

Of the more than 3,900 global IT and cybersecurity professionals we surveyed, 66% said that they believe AI and automation improve end-user service.

And our [Customer Zero](#) data confirms this effect: automated healing reduced downtime, minimized disruption and improved service delivery without increasing support burden.

More effective security and compliance efforts / faster threat response

Manual patch management struggles with both speed and coverage. We found that **38%** of organizations have difficulty tracking patch status, widening vulnerability windows during critical threat periods.

Autonomous Endpoint Management detects exposure continuously, prioritizes based on risk, deploys remediation autonomously, and verifies outcomes, compressing response cycles from weeks to hours.

Ivanti applied this model internally to strengthen security while reducing emergency workload, proving that speed and control are not mutually exclusive.

Continuous Compliance Over Periodic Assurance

We consistently find that the organizations most exposed to audit risk aren't those that lack controls; they are those whose controls operate on a schedule while their environments change continuously.

35% of organizations struggle to maintain compliance using manual tracking.

Autonomous Endpoint Management enables **continuous compliance**:

- Configuration drift is detected immediately.
- Out-of-compliance endpoints are remediated automatically.
- Audit-ready documentation is continuously updated.

A continuous compliance model eliminates the gap between scheduled patching and regulatory reality by continuously monitoring endpoint state, validating remediation outcomes and surfacing exceptions without adding manual oversight.



Reduce Risk

45%

lack visibility into shadow IT

41%

struggle identifying vulnerabilities

38%

cannot identify all devices

Improve Efficiency

55,600

productivity hours gained

20,000

automated tenant requests



Create Capacity

67%

believe AI frees teams for strategic work

86%

believe AI improves IT efficiency



The Maturity Advantage

Automation maturity is not evenly distributed, and that asymmetry is already creating measurable competitive separation in how organizations respond to threats, manage costs and build capacity for strategic work.

Organizations operating at advanced automation maturity consistently achieve faster response, stronger compliance, and greater strategic capacity.

- Faster threat response
- More predictable operating costs
- Higher end-user satisfaction
- Stronger compliance posture
- Greater strategic capacity

As complexity increases, this gap becomes a competitive advantage.

Real-world results show that autonomy compounds value over time, not just operationally, but economically.

Proven business value from
autonomous operations.

483%
ROI 8-Month
Payback Period

*Please note these are ROI results from a specific implementation; customer results will vary based on environment, configuration, usage.

Conclusion: what comes next

The shift to Autonomous Endpoint Management is a progression, not a project. It begins with a decision to build upon trusted data, moves through deliberate governance and eventually changes the economics and resilience of endpoint operations at scale. The technology to support it is mature. What most organizations are building now is the internal confidence and governance model to deploy it responsibly.

By establishing data authority and governing autonomy intentionally, organizations change the economics of endpoint operations while strengthening security, compliance and resilience.

Autonomous Endpoint Management is both an IT modernization initiative and a total business transformation. The remaining question for leaders is simple: how quickly do you want to capture this advantage?

The Autonomous Endpoint Advantage



Trusted Visibility



Stronger Security



Continuous Compliance



Lower Operational Cost



Faster Remediation



Greater Strategic Capacity



Start building toward Autonomous Endpoint Management on your terms

The shift to Autonomous Endpoint Management doesn't begin with deploying new technology. It begins with understanding where your organization stands today, and where greater visibility, continuous compliance and governed autonomy can deliver the most immediate impact.

Whether you're addressing visibility gaps, improving patch confidence or reducing operational drag, the next step is to evaluate how your current endpoint model compares to a more autonomous approach, and what it would take to move forward with confidence.

[Explore Autonomous Endpoint Management](#)



About Ivanti

Ivanti is a global leader in enterprise IT and security solutions, focused on unlocking human potential by making technology work better for people. Our platform helps organizations discover, manage, secure and service their IT assets, from cloud to edge, so teams can deliver exceptional digital experiences.

Powered by the Ivanti Neurons platform, our solutions enable organizations to automate workflows, reduce complexity and proactively resolve issues before they impact users. With a flexible architecture that supports cloud, on-premises and hybrid environments, Ivanti empowers organizations to scale securely and efficiently.

More than 34,000 customers worldwide, including over 85 of the Fortune 100, trust Ivanti to improve visibility, strengthen security and accelerate digital transformation.

Learn more at [ivanti.com](https://www.ivanti.com).