jamf

The Emerging Technology Playbook: Managing, Securing and Scaling the Modern Enterprise

Emerging mobile technology growth and the enterprise

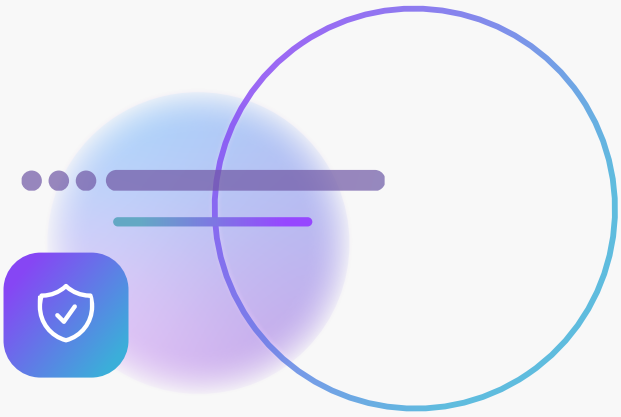
Much like workspaces have evolved where work is performed, emerging technologies, like wearables, spatial computing, and AI are changing how work is done. As business tools, they are enhancing user experiences, transforming productivity and accelerating innovation globally across industries.

But in doing so, business leaders, IT and security teams must evolve their endpoint strategies so that data remains secure, devices are managed holistically and enterprises scale intelligently to mitigate risk from expanded attack surfaces, fragmented visibility and intensified demand on operational resources.

This paper not only outlines why organizations should modernize management but also provides platform-agnostic guidance to build and enforce a resilient foundation based on real-world context and actionable steps to reduce complexity, close visibility gaps and prepare for the era of hybrid computing.

In this paper, you will learn to:

- Adapt management and compliance strategies to emerging technologies
- Recognize why traditional approaches fail to deliver security parity
- Leverage automation and continuous enforcement as core strategies
- Align management, identity, security and compliance with business goals
- Adopt zero trust as a core tenant of modern endpoint security



Executive summary

Enterprises are entering a period defined by rapid advances in hybrid computing models, including wearables, IoT and AI. These emerging technologies are reshaping business operations and fueling innovation across every industry – but they also introduce complexity, fragmentation and new risk avenues. As diversity within device fleets grows, so does the need for holistic management, context-based access policies, continuous posture validation and zero trust adoption. Organizations that invest in automated workflows, deep visibility and policy-driven controls will be better positioned to safeguard data, meet evolving regulations and scale emerging technologies with assurance.

Key takeaways:

- Ruggedized devices projected CAGR by 2028: **8.4%**
- Spatial computing projected CAGR by 2030: **33.16%**
- Enterprise adoption of hybrid computing paradigms by 2028: **40%**
- Customer service issues resolved autonomously by 2029: **80%**
- Expected wearable shipments in 2025: **590.7 million units**

Emerging technologies – 2026 and beyond

A new era of computing is accelerating as wearables, IoT and AI move from pilot programs to enterprise tools that deliver business outcomes. These technologies are reshaping how people work, learn and engage – blurring the realities of our physical world and digital workspaces – unlocking new levels of creativity, productivity, collaboration, insight and automation. Organizations harnessing this momentum will strategically align, strengthen resilience, scale intelligently and seize opportunities that define the next stage of innovation.

Spatial computing

The game Virtual Reality (VR) Vortex, found in late-90s arcades, served as the first foray into alternate reality experiences for many. This technology – including Augmented Reality (AR) and Extended Reality (XR) – have evolved to form a Mixed Reality (MR), bridging our understanding of physical and logical worlds.

Known collectively as spatial computing, it represents the next evolution of learning and productivity, with **an estimated compound annual growth rate (CAGR) of 33.16% by 2030**.

Despite spatial computing being in its relative infancy, the nuance of the nascent tech is being **felt across multiple industries globally**, including education, manufacturing and healthcare to name a few.

A few use cases of how spatial computing is being used in the real-world:

- **Streamline onboarding:** Employees familiarize themselves by touring and exploring workspaces to better orient new hires from day one.
- **Rapid prototyping:** Engineers develop and iterate products faster, while manipulating them to test integrity and collaborate in real-time.
- **Specialized training:** Surgeons practice in realistic settings while 3D overlays are used to create an immersive simulation to learn procedures and increase precision.
- **Enhancing experiences:** Retail customers use their smartphones to scan and visualize products in-home or try on clothing, meeting customers where they are.
- **Just-in-time troubleshooting:** Machine operators use Apple Vision Pro to identify issues and perform analysis to resolve problems from the production floor.

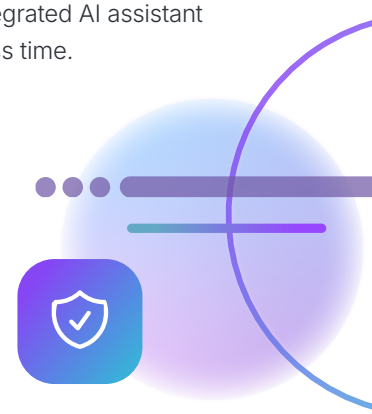
Wearables

Consider this: an Apple Watch contains the hardware components, albeit miniaturized, that were once only possible in Pentium 4-class desktop computers.

With multi-core processing, Neural Engines, a whole host of microscopic sensors and the ability to run independently as its own computing source – work (and play) are possible today in a capable, energy efficient design wrapped around your face, hand, finger and/or wrist.

Here are a few use cases for the **590.7 million wearables shipped in 2025**:

- **Watches:** Simplify travel (domestic and international) with GPS + Cellular-enabled smartwatches to stay in communication with the office and loved ones without having to futz with confusing or costly data roaming plans.
- **Trackers:** Get up-to-minute health information to proactively monitor vital signs, stay on track with goals or quickly respond to accidents and health-related incidents to receive life-saving care.
- **Earbuds**: Noise-cancelling technology limits external distractions to aid focusing on what's important; also, when paired with a smartphone, live translation is possible to understand multiple languages being spoken in real-time.
- **Glasses**: Take pictures and video as you respond to urgent messages, while following directions to the meeting spot – hands-free with integrated AI assistant helping you accomplish more in less time.



Internet of Things (IoT)

Efficiency is a driver of business continuity. And since automation serves as a building block for efficiency, it's no surprise that reliance on IoT devices to build business intelligence, such as across process flows, which are essential for the kind of data-driven decision-making used to streamline business operations at scale.

Additionally, **energy cost savings of approximately 20-30% i**n certain business models is made possible through a combination of sensors and automation. Moreover, **a reduction in maintenance costs by up to 50%** may be realized, thanks to a strategic shift, like predictive maintenance, that favors a proactive approach (instead of a reactive one) to cut unplanned downtime.

Several examples of the benefits of IoT in the enterprise are:

- **Asset tracking and logistics network:** Simplify inventory monitoring, and when paired with predictive analytics, improve capacity planning and stock forecasting.
- **Personalizing customer experiences:** Strengthen brand loyalty with customized interactions that better meet customer's unique needs while improving service delivery.
- **Building and facilities management:** Reduce energy footprints while increasing the efficiency of building functions by automating HVAC, lighting and security.
- **Interconnect** sophisticated systems: Gain added value from existing systems by integrating sensors and IoT, enabling new services and revenue opportunities.

Artificial Intelligence (AI)

The promise AI holds affects enterprise and personal users alike. With applications spanning industries globally, the transformative benefits of GenAI for businesses appear limitless:

- **Greater value:** Employees are empowered to focus their skills on strategic work while repetitive tasks are performed automatically.
- Increase ROI: Optimizing resources and greater efficiency optimize processes and reduce operational costs, in addition to qualitative benefits from innovation and enhanced customer experiences.
- **Streamline processes:** Maximize resources by visualizing concepts, summarizing content or developing sample code rapidly.
- **Supercharge analysis:** Gain valuable insights, perform trend evaluations and make proactive, data-driven decisions, reducing go to market (GTM) times.

Moreover, Agentic AI (making decisions without human interaction) offers key advantages that expand upon the benefits listed above. For example, Gartner research estimates that **80% of common customer service issues will be resolved autonomously by 2029**. Other key benefits lie in its ability to be proactive (threat hunting) and adaptive (learning in real-time). One segment where it's poised to revolutionize crucial enterprise processes is cybersecurity software. Agentic AI-based security solutions continuously monitor and assess risk factors while taking actions to mitigate threats quickly and without requiring human intervention – shrinking response times and maintaining resilience.

Hybrid computing

Businesses across the globe see challenges to efficiency and workload handling, resource provisioning and scaling, alongside regulatory requirements and capital spending that traditional computing models like on-premises or public/private clouds alone simply cannot effectively address. Even lower latency models that process data closer to the device for faster turnaround, like edge computing, still do not address all the concerns of the rapidly changing digital landscape.

Hybrid computing is a new paradigm that expands to not only include emerging technologies but mixes existing compute models to solve for the obstacles mentioned, such as:

- **Agility**: Leveraging multiple computing models allows organizations to optimize traffic handling, boost response times and reduce latency inexpensively during unexpected peak times.
- **Performance**: Achieve productivity gains by implementing AI-driven tools and automation to intelligently distribute workloads across the most efficient environment.
- **Compliance**: Geopatriation gives organizations control over where data and applications reside, ensuring sovereignty while meeting privacy and regulatory demands.
- **Resilience**: Streamline continuity to ensure that business operations are maintained during outages by leveraging cloud, on-premises and legacy system integration.

By 2028, Gartner predicts that **over 40% of leading enterprises will have adopted hybrid computing paradigm architectures** into critical business workflows, up from the current 8%.

Challenges for enterprise IT

When devices fall outside management scope, visibility gaps emerge, limiting the ability to:

- Assess security postures
- Respond to threats quickly
- Maintain data security

Platform and device diversity, mixed with varying ownership models and hybrid work environments introduce variables that expand an organization's attack surface. Moreover, it increases the strain on teams already responsible for mitigating risk from an evolving threat landscape. Vis-à-vis, evolving regulations and fragmented standards around AI and IoT respectively, raise the stakes for governance and responsible adoption globally, for organizations and the industries they operate within.

Enrollment and provisioning

A comprehensive management and security strategy begins with device enrollment and is following with the ability to provision devices with the tools and configurations necessary for organizations to remain compliant, data safeguarded and employees productive. This best practice is baked into holistic IT workflows and is the subject of many deployment standards and frameworks.

When devices are not enrolled with management suites or aren't provisioned with the tools its users depend on to accomplish tasks, a slow yet consistent chain of events is set off that introduces risk to:

- Device usability
- Data confidentiality
- Communication integrity
- User privacy
- Endpoint availability

Each risk factor affects service delivery and regulatory compliance and ultimately results in compounding impacts to business continuity.

Policy and visibility gaps

Device insight is the cornerstone of any security strategy. The inability to view or analyze endpoint health statuses means IT and Security teams are effectively unable to see what's going within the emerging technology devices connecting to, communicating on, and requesting and using company resources within their infrastructure.

Due to telemetry blind spots, a host of issues may be present that admins are unable to mitigate without first knowing what threats may exist nor how resources should be prioritized given limited resources and/or mitigation options.

Some common examples that contribute to visibility gaps are:

- Multiple OS platforms
- Physical tampering
- Mixed ownership models
- Unsupported device types
- Device misconfigurations

Threat and risk mitigation

While threat actors targeting hardware and software looking for entry points is nothing new to cybersecurity, the challenge of reducing risk is compounded by hybrid environments, and varying device types – each running multiple software platforms – introduces a variety of risk to the organization.

The mix of open source, proprietary, and closed systems and device types, places a greater strain on IT and Security teams tasked with managing and securing endpoints. When combined with a lack of visibility into endpoint health and limited ability to securely configure devices at scale, the following challenges exponentially increase the difficulty of keeping enterprise resources secure:

- Data security
- Vulnerability exploitation
- Network resilience
- Patch management
- Expanded attack surfaces

Regulatory and compliance pressures

Unlike existing or legacy systems, emerging technologies face a number of varied and rapidly evolving challenges across the global landscape. In some cases, given the fragmented nature of technologies like IoT, the lack of a unified standard raises many data security concerns. When it comes to AI, many agree on the performative benefits of utilizing the technology, yet less so seem to understand or subsequently agree on the implications of its use on humanity or the environment.

While many of these concerns are being worked out in real-time, in the case of laws that have caught up to the technology, strict data protections like the California Consumer Privacy Act (CCPA) and Europe's General Data Protection Regulation (GDPR) add immense scrutiny to how emerging tech is used. Other considerations that require methodical evaluation by enterprise leaders to determine if they can be used and where are:

- Data residency
- Operational resilience
- Third-party risk management
- Governance factors
- Ethical considerations

Forward-looking solutions and best practices

When solving for the challenges of implementing emerging technologies, enterprises should anchor their approach in proven best practices to optimize risk reduction. This disciplined approach supports scalable, resilient endpoint management as fleet's grow more diverse and new use cases evolve that more specifically benefit growing business needs.

Endpoint inventory

Before an enterprise is able comprehensively assess risk, they first need to know what the infrastructure looks like. And the best way to paint a picture of what's there is to perform a complete inventory of all hardware, software, services and processes. A detailed understanding of:

- Every device
- Their dependencies
- Workflows and policies

Identifying each component and how they interconnect offers a holistic view of the entire infrastructure, how it communicates and with which devices, providing enterprises a solid foundation toward implementing forward-looking solutions.

Risk assessment

The next step is assessing risk factors to determine their criticality. The aim during this phase is not just to reduce risk but aligning each with the organization's overall risk tolerance or appetite.

Using a combination of both qualitative and quantitative methods enables a programmatic cyber risk index, providing decision-makers a data-driven overview based on key attack indicators, such as:

- **Vectors**: The path or method used to execute an attack or compromise a system.
- **Complexity**: The skill and resources required for an adversary to exploit a weakness.
- **Impact**: The business and operational consequences of a successful attack.
- **Exposure**: The weaknesses or gaps that leave an environment open to exploitation.
- Severity: A measure of how likely a threat is and how damaging it could be.
- **Remediation**: Whether a fix exists, what it is and how quickly it can be deployed.

Threat modeling

The third step is a proactive approach to identify and prioritize risk in devices, systems and applications. More specifically, performing threat modeling before penetration testing (we talk more about this in the next section) places focus on prioritizing risks from the highest severity to the lowest. In turn, this helps to not only reduce device risk but maintain a fortified organizational security posture.

Multiple threat models exist and may be used to assess specific types of risk, or as an integrated approach to systematically find and quantify threats; or put another way, the best way to mitigate an attacker is to think like one.

Common threat modeling methodologies and their uses are:

STRIDE:
Spoofing, tampering, repudiation, informative disclosure, denial of service and elevation of privilege.
WHAT IT DOES:
This model categorizes risk based on it performs in each of the six categories.

DREAD:
Damage potential, reproducibility, exploitability, affected users and discoverability.
WHAT IT DOES:
This model produces an averaged score based on the five factors to rank risk severity. (It's often used in concert with STRIDE to prioritize mitigation of high-risk threats).

LINDDUN:
Linking, identifying, non-repudiation, detecting, data disclosure, unawareness and non-compliance.
WHAT IT DOES:
This model provides a structured method to identify and mitigate privacy-based threats, based on analysis of how data flows within applications and systems.

PASTA:
Process for attack simulation and threat analysis.
WHAT IT DOES:
This model focuses on risk impact to businesses, including technical requirements (ex. defining objectives and scope, analyzing vulnerabilities and simulating attacks), for the development of risk mitigation strategies.

OCTAVE:
Operationally critical threat, asset and vulnerability evaluation.
WHAT IT DOES: This model also focuses on business risk that align cybersecurity with business goals across three phases: building asset-based threat profiles, identifying infrastructure vulnerabilities and developing risk management strategies.

Penetration testing

Arguably the most common risk assessment task is the pentest, which is often performed to find and prioritize vulnerabilities in devices and software. The choice to include this last on the list goes back to the previous section on threat modeling. When performed after threat modeling, the pentest adds a layer of efficiency and effectiveness to the risk assessment process.

It achieves this for the former by:

- Allowing pentesters to focus on higher severity risks (since threat modeling likely identified lower-risk threats)
- Facilitating mitigation of risks by IT earlier in the assessment process

For the latter:

- Pentesting validates previously deployed remediations
- Another layer of scrutiny is added to finding vulnerabilities that may have gone previously unnoticed

Device posture and identity-first access (zero trust journey)

Emerging technologies require identity-first strategies and continuous device posture validation to safeguard sensitive data and maintain operational integrity. Modernizing management to continue supporting increasing diversified fleets must automate enforcement, reduce operational overhead and seamlessly scale zero trust.

The following solutions provide variable tools to aid IT in lifecycle management of emerging technologies:

- **Mobile Device Management (MDM)**: Integrates device and identity management, alongside endpoint security comprehensively – **from zero touch deployment to secure disposal** – on-premises or cloud-based.
- **Unified Endpoint Management (UEM)**: On-premises or cloud-based, offering cross-platform support but often exchanged for a narrower capability scope.
- **Amazon Web Services (AWS):** Cloud-based model that offers manageability and security limited to specific technologies, like IoT devices and supporting multiple vendors.
- **Autonomous Endpoint Management (AEM):** The future of cloud-based UEM, reducing operational cost through automation and enforcing zero trust by continuously validating and correcting device posture – for diversified fleets – at scale.

App and data controls

When stripped down to its base level, regardless of the device type or OS it runs – data is data. Protecting data remains at the core of each control, process and task performed in service to managing and securing emerging tech.

Deploying configurations is one effective method to secure devices, and the data processed and contained within them. While the methods supported will depend largely on the OS platform, the aim is to establish secure configurations based on best practices, such as standards and frameworks, that translate across OS borders to keep data safe.

Examples of tools used to create secure configurations include:

- **Android**: **OEMConfig** and **Android Open Source Project** (AOSP)
- **Apple**: **Apple Configurator**, **Jamf Pro** and **Declarative Device Management** (DDM)
- **Linux**: Bash scripts, **SOTI MobiControl** and **Microsoft Intune**
- **Proprietary:** Review the manufacturer's support site for information on where to obtain tools specifically tailored to the technology

Monitoring and response

Visibility into endpoint health statuses is an essential component of proactive cybersecurity. The sooner issues are identified; the quicker incident response can mitigate the risk or remediate the threat. Active monitoring of endpoints within your infrastructure is not only highly recommended, but it's a crucial component of zero trust architecture.

On-device and in-network protections are the two aspects of zero trust protections. While the network side is covered in the next section, here are endpoint-centric guidelines for maintaining strong device postures across your infrastructure:

- Actively monitor device health telemetry and compliance levels
- Integrate management and security solutions to automate response
- Implement zero trust to verify endpoint health before granting access to resources
- Deploy operating system updates, security and app patches in a regular cadence

Network security

Emerging technologies often outpace standards, adding difficulty to managing certain endpoints or misaligned with business objectives. Because risk is subjective, security strategies are not one-size-fits-all. This elevates the focus to securing data from endpoints. The following solutions – whether deployed standalone or combined – help maximize data security across local and cloud environments:

- **Demilitarized Zones (DMZ)**: Segments high-risk devices, such as IoT, allowing only controlled communication with internal systems or external networks based on policy.
- **Virtual Local Area Network (VLAN):** Isolates network traffic – limiting lateral movement and enforcing least-access communications – providing IT granular control over traffic between devices and mission-critical systems.
- **Security Orchestration, Automation and Response (SOAR)**: Unifies security tools and workflows through automation to accelerate threat detection, response and containment.
- **Zero Touch Network Access (ZTNA)**: Applies continuous, context-based device verification, microtunneling (per connection requests) and health checks to ensure only compliant devices can access protected resources.

Baselines and benchmarks, standards and frameworks

It's important to view each section as a cyclical phase instead of a linear one. Lifecycles in IT and security are iterative – they're not a destination but a never-ending path – that informs what comes after and is shaped by what came before. With that in mind, the synergy between each of the following is paramount to maintaining security while introducing emerging technologies into your tech stack:

- **Baselines:** A collection of controls and processes that **define a foundational security posture.**
- **Benchmarks:** Performance metrics used to **measure compliance with security best practices.**
- **Standards:** Globally recognized best practices that identify how secure hardware, software and/or services should be **secured to meet a specific requirement**.
- **Frameworks:** Structured guidelines that detail how controls, policies, processes, and **standards should be deployed to minimize risk** and maximize security.

Conclusion

With an understanding of emerging technologies and their impact of business goals, now is the moment business leaders and IT teams to take the next step to align existing manage and security strategies with future-focused best practices. By acting now, organizations can stay ahead of emerging risks, streamline operations and confidently embrace the next era of innovation.

Checklist: Next steps for business leaders and IT managers

1. Identify business use cases

- Evaluate where emerging technologies (AI, IoT, spatial computing, wearables) align with business objectives.
- Determine potential ROI and operational improvements against existing workflows.
- Prioritize initiatives that deliver measurable business outcomes and compliance readiness.

2. Establish a cross-functional evaluation team

- Form a committee with IT, security, legal and operations stakeholders.
- Assign ownership for risk assessment, compliance review and lifecycle management.
- Define communication channels for rapid feedback and escalation.

3. Conduct a comprehensive asset and dependency inventory

- Document all devices, software, APIs and cloud services used within the infrastructure.
- Identify integration dependencies across hybrid environments (cloud, on-prem and edge).
- Tag ownership models (COBO/COPE/BYOD/CYOD) to ensure visibility and accountability.

4. Perform risk and threat assessments

- Use both qualitative and quantitative methods to gauge risk tolerance and impact.
- Map threats using models for accuracy and consistency.
- Rank vulnerabilities by severity, exploitability and remediation timeframes.

5. Perform threat modeling

- Simulate potential attack paths using accepted threat modeling frameworks.
- Identify privacy, data flow and operational exposure points.
- Document mitigations to reduce risk before production rollout.

6. Validate compliance and governance requirements

- Review regional and industry-specific regulations.
- Confirm data residency, sovereignty and third-party vendor risk management.
- Incorporate ethical considerations for AI and data-driven technologies.

7. Define enrollment and provisioning processes

- Standardize onboarding workflows for all device types and ownership models.
- Automate configuration, patching cadence and access controls to minimize manual error.
- Use secure enrollment and identity-based authentication to verify endpoints.

8. Integrate identity-first access strategies

- Require continuous verification of credentials and device posture before resource access.
- Enforce least-privilege principles across endpoints and applications.
- Integrate Zero Trust and context-aware policies into access control systems.

9. Establish secure configuration and data controls

- Define security baselines to set configuration and compliance expectations.
- Encrypt sensitive data at rest and in transit.
- Implement granular data policies for classification, storage and sharing.

10. Segment and harden network communications

- Use VLANs and DMZs to isolate high-risk devices like IoT and wearables.
- Apply micro-segmentation and Zero Trust Network Access (ZTNA) for adaptable, in-network security controls.
- Ensure data security is a core to network security – regardless of device type, ownership model, OS platform or where users are working from.

11. Implement continuous monitoring and automated response policies

- Collect telemetry from all endpoints for real-time visibility and health insights.
- Deploy automated workflows for anomaly detection and incident response.
- Stream alerts into centralized tooling to automate threat detection and remediation tasks.

12. Apply baselines, benchmarks and gather productivity metrics

- Apply baseline configuration standards for a holistic security across the enterprise.
- Use benchmarks to measure performance and security postures.
- Review KPIs to assess compliance status and demonstrate risk reduction.

13. Conduct regular validation: penetration testing and audits

- Schedule recurring penetration tests and vulnerability scans post-deployment.
- Validate remediations identified during threat modeling.
- Review findings against established baselines and update policies accordingly.

14. Automate lifecycle management and policy enforcement

- Leverage unified endpoint or autonomous management systems for ongoing compliance.
- Automate patch processes, compliance policies and device retirement workflows.
- Continuously align configurations with evolving frameworks and standards.

15. Document findings and conduct regular training

- Establish feedback loops for emerging threats and lessons learned.
- Provide ongoing training for admins and users to recognize risks.
- Reassess suitability and iterate controls as technologies and regulations evolve.