AvePoint

Securing the Modern Workplace: A Guide for MSPs to Protect Client Data and Unlock New Revenue

AvePoint

Securing the Modern Workplace: A Guide for MSPs to Protect Client Data and Unlock New Revenue

Introduction

Data has become the lifeblood of business operations. As organizations rapidly adopt cloud services, collaboration tools, and AI-powered technologies like Microsoft Copilot, the volume and sensitivity of digital information have skyrocketed. In the ***State of Human Risk 2025 report,*** 81% of organizations are concerned about GenAI leading to sensitive data leaks, and 55% are not fully prepared with specific strategies for AI-driven threats.

The harsh reality? Cyberattacks, data breaches, and ransomware incidents are now common threats, impacting businesses of all sizes. ***Gartner predicts*** AI agents will allow bad actors to exploit vulnerabilities 50% faster by 2027. With teams, workspaces, and now agents sprawled across multiple clouds and applications, the risk of a data security incident due to oversharing, misconfigurations, accidents, prompt engineering, and more is growing.

50% named **cybersecurity** as their clients' top concern.

Small and medium-sized businesses (SMBs) are particularly vulnerable due to limited IT resources and security expertise. This underscores the critical need for robust cybersecurity measures and data protection, creating an unprecedented opportunity for managed service providers (MSPs). By stepping up to become essential partners in safeguarding client data, MSPs can not only protect their clients but also unlock new revenue streams and solidify their position as trusted advisors in an AI-driven world.

Risks in Today's Digital Workplace and Struggles as an MSP

Digital transformation brings tremendous opportunities — but also significant risks. Data is everywhere; it no longer resides solely within controlled environments but is scattered across cloud applications, stored on countless devices, shared through collaboration platforms, and processed by AI systems. A dispersed data landscape creates multiple pathways for exposure: accidental oversharing of sensitive documents, excessive guest user access to resources, permission sprawl across collaboration spaces, shadow IT operations outside sanctioned channels, and AI tools potentially accessing and processing sensitive data.

In fact, 83% of organizations report that a lack of visibility into data weakens their security posture, and 87% find their current data discovery and classification tools inadequate. MSPs managing multiple client environments face these challenges exponentially:

- **Configuration drift:** Security configurations naturally deteriorate over time without proper tools, creating inconsistencies across client tenants.
- **Multi-tenant complexity:** Each client environment presents unique security needs, making standardized approaches difficult to implement at scale.
- **Security talent shortage:** The cybersecurity skills gap continues to widen, making hiring and retaining qualified security specialists increasingly difficult.
- **Tool overload:** Many MSPs juggle dozens of security tools, leading to alert fatigue, inefficient workflows, and diminished effectiveness.
- **Onboarding and knowledge transfer:** When security personnel leave, critical knowledge often leaves with them, creating dangerous gaps during transitions.

The shortage of security specialists leads to tool overload issues. Reskilling and upskilling talent can help shrink the cybersecurity skills gap.

Why Traditional Approaches Leave Gaps

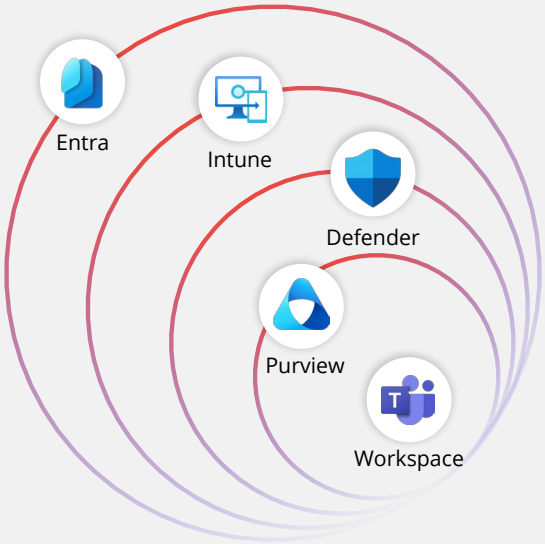
According to Microsoft's 2024 Digital Defense Report, 80% of organizations have paths to sensitive data that could be exploited, and 61% of attack paths target sensitive accounts with elevated privileges. MSPs face scalability challenges when managing security and compliance across multiple clients without effective tools:

- **Manual patching and updates:** Reactive rather than proactive security leaves windows of vulnerability.
- **Break/Fix mentality:** Waiting for incidents to occur before addressing security issues.
- **Visual verification and manual audits:** Human-dependent processes that can't keep pace with the scale and complexity of modern environments.

Relying solely on native security controls or manual management is no longer sufficient. For example, platform providers like Microsoft offer built-in security features, but these native controls often lack centralized management across multiple tenants, provide limited visibility into security posture, require significant manual configuration and monitoring, and miss critical cross-platform security issues.

The Microsoft Security Tech Stack

Protect identities, secure data, manage devices, and detect threats:



Moreover, backup solutions remain essential for disaster recovery. But backup alone cannot: prevent data exposure or leakage, control unauthorized access, ensure compliance with data governance requirements, and protect against emerging AI-related risks. As your MSP business grows, traditional approaches break down, consistent policy enforcement and granular access control are difficult to achieve, and managing numerous security alerts and tools can lead to alert fatigue and tool overload.

MSPs can deliver significant value by focusing on business outcomes such as improved security posture, reduced risks, and enhanced compliance and governance, which will establish AI readiness and a controlled digital workplace.

54% ***of respondents believe that a unified platform for access and identity management would benefit their organization's security strategy.***

Building a Proactive Data Security Service: A Guide for MSPs

With 90% of organizations exposed to at least one attack path, MSPs need to build comprehensive data security services that address key client priorities to effectively protect clients in the age of AI and deliver valuable business outcomes:

1 Improve Security Posture and Reduce Risk

To enhance your clients' overall security position while minimizing exposure:

- **Configuration integrity:** Ensure environments remain in a trusted state, establish and maintain security baselines across clients, automatically detect and remediate configuration drift, and implement least-privilege access models.
- **Vulnerability management:** Proactively address security weaknesses, identify and prioritize vulnerabilities before they're exploited, apply guided remediation steps to fix issues, and reduce mean time to remediate configuration problems.
- **Data exposure prevention:** Stop leaks before they happen, monitor and control external sharing, identify and secure overprivileged accounts, and reduce shadow IT through visibility and governance.

2 Control and Organize the Digital Workspace

To help clients maintain order in increasingly complex digital environments:

- **Collaboration governance:** Control sprawl and oversharing, implement lifecycle management for collaboration spaces, enforce consistent permissions policies, and automate provisioning and deprovisioning processes.
- **Workspace cleanup:** Reduce digital clutter and associated risks, identify and archive inactive workspaces, remediate orphaned resources, and apply retention policies consistently.
- **Real-time control:** Maintain ongoing oversight, monitor workspace creation and configuration, apply appropriate templates and policies, and ensure governance from day one.

3 Enhance Compliance and Governance

To support clients' regulatory and internal governance requirements:

- **Compliance baseline:** Establish reference points for ongoing compliance, document initial state and improvement actions, maintain evidence of security controls, and demonstrate continuous compliance over time.
- **Policy enforcement:** Implement and monitor compliance requirements, restrict external sharing based on content classification, ensure proper data labeling and protection, and address compliance blind spots.
- **Centralized oversight:** Streamline governance activities, automate routine compliance tasks, provide clear, actionable compliance reporting, and deliver executive-ready risk assessments.

4 Ensure AI Readiness and Adoption

As clients adopt technologies like Microsoft Copilot, they need guidance to do so securely:

- **Workspace optimization:** Identify and prepare collaboration spaces for safe AI integration, assess which workspaces meet the criteria for tools like Copilot, track optimization status across all client environments, and implement appropriate data boundaries.
- **Information management:** Control what information AI tools can access, manage search scope parameters across tenants, implement appropriate exclusions for sensitive data, and configure content boundaries to prevent AI from accessing protected information.

- **Adoption acceleration:** Remove barriers to secure AI implementation, identify workspaces eligible for semantic search and AI features, remediate security issues blocking AI adoption, and apply appropriate governance to enable responsible AI use.

The MSP Advantage: Scaling Efficiency and Profitability with AvePoint Elements

MSPs must be prepared to address risks and leverage AI to enhance security measures. Focusing on key areas like automating user and device management, policy enforcement, and risk reviews, MSPs can reduce manual effort and enable faster and more efficient client onboarding, creating sticky, high-value services that differentiate their offering and improve client retention.

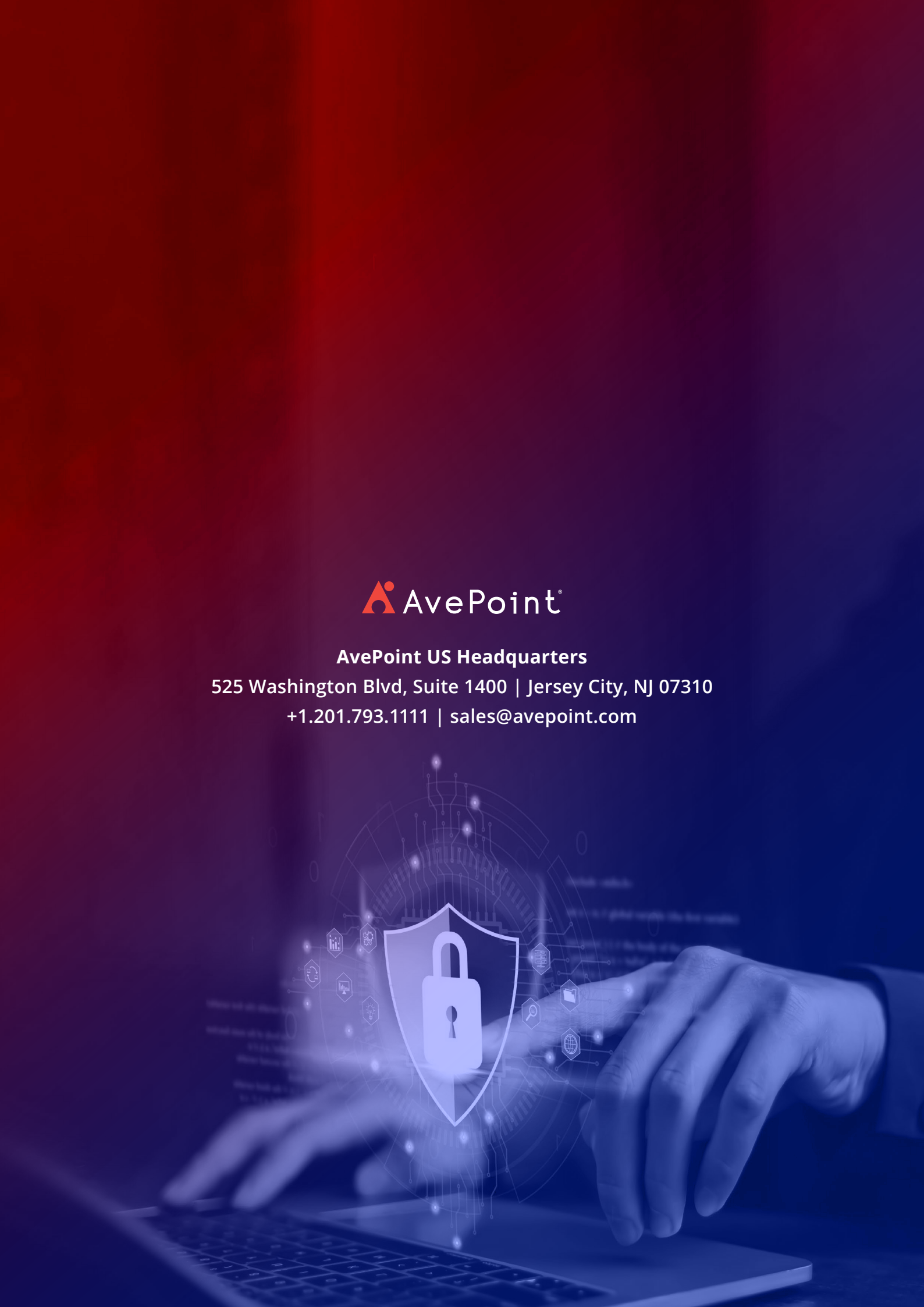
A unified platform approach helps MSPs streamline operations and overcome scaling challenges. Key benefits include turning data security into predictable monthly recurring revenue and becoming a trusted advisor by proactively addressing client risk and enabling safe AI adoption.

By using tools that are secure by design and avoiding point solutions, MSPs can empower their clients to enhance data security, governance, and resilience while driving business growth — positioning themselves as leaders in AI integration and data management.

Partnering for a More Secure Future

A proactive approach to data protection is critical in the modern, AI-driven workplace. Having a comprehensive data security service benefits your clients (reduced risk, compliance, AI confidence, controlled environment) and MSP business (efficiency, scalability, new revenue).

Build your data security service offerings with AvePoint's new Security Campaign in a Box Kit, exclusively available for AvePoint Partners. Empowering you with the tools and strategies needed to drive value for your clients and grow your business.



AvePoint US Headquarters
525 Washington Blvd, Suite 1400 | Jersey City, NJ 07310
+1.201.793.1111 | sales@avepoint.com