

TOOL CONSOLIDATION & OPTIMIZATION (TCO) ASSESSMENT

The increasing complexity of cyber threats and growing importance of cybersecurity's role in business strategy place CISOs under immense pressure to expertly balance protection, business operations and compliance.

The **Tool Consolidation & Optimization (TCO) Assessment** helps Microsoft Security and Modern Work users to streamline their Microsoft and third-party tool usage, reduce costs, and enhance security and compliance. By evaluating current tool sets and Microsoft capabilities, **this service provides a roadmap for consolidation, simplifying operations and supporting a zero-trust security model.** Avertium's unique methodology and consultative approach ensures objective analysis and actionable recommendations, leading to improved security posture, adherence to compliance and potentially significant cost savings.

BUSINESS VALUE

Provides Clarity → Improves overall awareness of current inventory and likely optimization and consolidation.

Reduces Cost → Identifies potentially substantial savings by educating customers about included security capabilities in their Microsoft licenses and highlighting redundant third-party tools. **Revealed savings:**

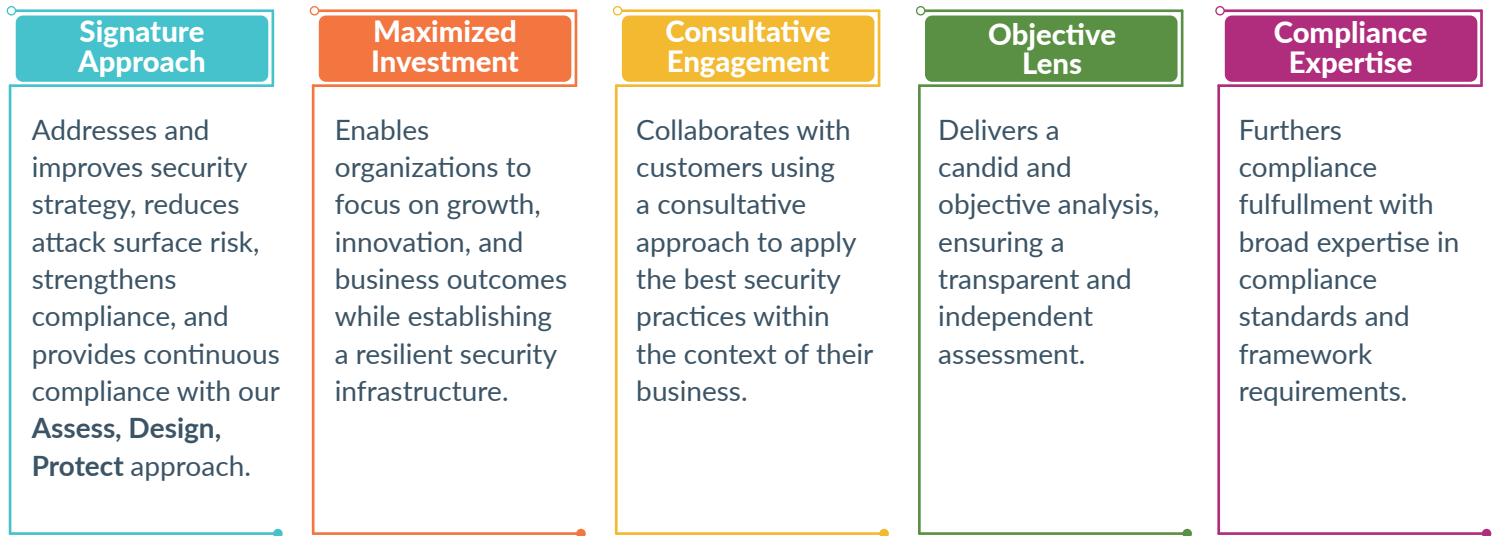
- **Customer Zero (Avertium):** Estimated savings of approximately **\$100,000 annually** by implementing E5 licenses and eliminating redundant tools such as Okta.
- **Customer 1:** Estimated savings of **\$390,000 annually** in licensing costs by sunsetting Cisco AMP, MobileIron, and LogRhythm. Moved to Sentinel and began leveraging E5 Security as replacement, which they had already contracted but hadn't leveraged.
- **Customer 2:** Savings of **\$240,000 annually**, in support of their Citrix VDI instance and large licensing fees to Citrix. Developed customer roadmap from E3 to E5 so that they could take advantage of Microsoft Security as an upgrade.

Manages Complexity → Facilitates streamlined operations by consolidating tools and reducing redundancies.

Enhances Cybersecurity → Matures security posture by identifying risks associated with duplicate or overlapping tools and providing recommendations for improvement.

Advances Compliance → Recommends ways to remediate compliance gaps using the proper tools, assuring compliance adherence.

DIFFERENTIATORS



PAIN POINTS ADDRESSED

Companies face several main challenges when it comes to optimizing their tool usage and ensuring effective cybersecurity and compliance.

1. **Clarity:** Many companies lack a comprehensive understanding of their tool inventory, leading to duplicated functionality and security gaps. Additionally, they may not fully understand their Microsoft licensing.
2. **Cost:** Overbuying and underutilizing tools leads to wasted expenses. IT departments often face budget constraints and pressure to use Microsoft E5 licenses effectively, though they find it expensive.
3. **Complexity:** Managing multiple third-party tools adds operational complexity and interactivity issues, making it hard to have a holistic security view and respond quickly to threats.

→ Complexity Takes a Human Toll

- **Staff Burnout** - Security teams report a **38% higher burnout rate** when dealing with siloed tools (ESG Research, 2023).
- **Vendor Overload** - Enterprises use an average of **76 security tools**, and 57% of IT leaders believe managing multiple vendors reduces the effectiveness of their security strategy (Gartner, 2022).
- **Amplified Skills Shortage** - Siloed solutions exacerbate the cybersecurity skill gap, with **52% of organizations struggling** to find skilled professionals (ISACA, 2023).

4. **Cybersecurity:** Multiple tools can create security gaps and reduce visibility. Alert fatigue can overwhelm teams, leading to ignored alerts. Additionally, many companies struggle but want to start a zero-trust security approach.
5. **Compliance:** Managing compliance across multiple tools can be complex and may lead to adherence gaps, increasing the risk of regulatory penalties.

Alongside Avertium's expertise, our TCO Assessment helps overcome these challenges by optimizing resources, potentially reducing costs, and achieving robust security.

HOW IT WORKS

Avertium's Tool Consolidation and Optimization Assessment is collaborative and interactive, featuring group discussions and a round-table format.



Phase 1: Kickoff

Hold initial meeting to introduce the project and collect necessary information.



Phase 2: Engagement Setup and Scope Definition

Define and formalize the engagement scope, key objectives, and required data sets.



Phase 3: Data Collection

Gather and analyze inventory data on Microsoft Security and Modern work tools and licenses.



Phase 4: Exploration and Analysis

Conduct a structured workshop to evaluate current state and collaboratively determine the desired future state.



Phase 5: Results Presentation and Final Deliverables

Present the Tools and Optimization Assessment results, including findings, key insights, and recommendations. **FINAL DELIVERABLES:** Assessment Report, Financial Analysis, and Roadmap



Phase 6: Engagement Decommissioning

Remove all stored customer data from Avertium SharePoint systems unless otherwise authorized.

ABOUT AVERTIUM

[Avertium](#) is a cyber fusion and MXDR leader, delivering comprehensive security and compliance services to mid-market and enterprise customers. Our unique “Assess, Design, Protect” methodology addresses and improves security strategy, reduces attack surface risk, strengthens compliance, and provides continuous threat protection. Avertium maximizes customer security investments and enables customers to focus on growth, innovation, and business outcomes, while assuring that their security infrastructure is resilient and adaptive to evolving threats. That's why customers trust Avertium to deliver better security, improved compliance, and greater ROI.