



# Case Study: Building a Secure Foundation For AJX Security Consulting

## Section 1: Client Background

AJX Security Consulting is a cybersecurity firm specializing in Microsoft 365 security hardening for small and medium-sized organizations. Founded by Ahmad Jundi and Obaida Issa, both graduates in Networking and IT Security, the company was built on one core principle: to make enterprise-grade security accessible, affordable, and easy to understand for every business.

Before serving clients, AJX made it a top priority to secure its own Microsoft 365 environment. As a security-focused organization handling sensitive data, internal reports, and client communications, it was critical to build a strong cybersecurity foundation that reflected the same standards AJX delivers to its customers.

## Section 2: The Challenge

At launch, AJX Security Consulting's Microsoft 365 tenant operated under default settings, which are designed for convenience rather than security. These defaults left several potential entry points for attackers and lacked visibility into identity-based threats.

The primary challenges included:

- **Baseline vulnerabilities:** Default settings meant MFA was not enforced, and legacy authentication protocols were still active.
- **Limited visibility:** No centralized monitoring for phishing, impersonation, or risky sign-ins.
- **Scalability needs:** Security policies had to be structured to support future client onboarding and company growth.
- **Compliance readiness:** AJX needed to meet modern data protection and CIS Microsoft 365 Benchmark standards before engaging with clients.

## Section 3: Our Approach

AJX applied its own structured hardening methodology based on Microsoft's Zero Trust principles. This involved a complete tenant audit followed by a step-by-step implementation process focused on identity protection, data security, device control, and collaboration privacy.



Key measures implemented:

1. Enforced **Multifactor Authentication (MFA)** across all admin and user accounts.
2. Applied **Conditional Access** to restrict high-risk or unknown sign-in attempts.
3. **Disabled legacy authentication** to eliminate insecure connections.
4. Deployed **anti-phishing and impersonation protection** to defend against domain spoofing.
5. Activated **Safe Links** and **Safe Attachments** for continuous email and file scanning.
6. Configured **Data Loss Prevention (DLP)** policies across OneDrive, SharePoint, and Exchange.
7. Restricted **calendar visibility** and **anonymous Teams meeting access** to internal users only.
8. Implemented **SPF, DKIM, and DMARC** for authenticated email delivery.
9. Conducted ongoing **Secure Score audits** to measure and track improvements.

## Section 4: The Results

Within weeks, AJX Security Consulting transformed its Microsoft 365 tenant into a highly secure, benchmark-compliant environment that aligned fully with Microsoft's best practices.

### Key highlights:

- **Secure Score:** Improved from **36.19% to 84.25%**, a **133% overall improvement**.
- **MFA and Conditional Access:** 100% enforcement across accounts, blocking **99.9% of unauthorized sign-in attempts**.
- **Phishing exposure:** Reduced by **70%** after applying advanced threat policies.
- **Spoofing protection:** Fully implemented through DKIM and DMARC.
- **Anonymous access:** Disabled for Teams meetings and calendar sharing, increasing privacy.
- **Safe Links and Attachments:** Enabled across all applications for real-time protection.
- **No successful external login attempts** since deployment.
- **Spam and bulk mail filtering tightened**, cutting down the number of high-risk messages that reach user inboxes.

Policy	Result
Anti-Phishing & Impersonation	Strengthened identity and domain protection
MFA Enforcement	100% account protection coverage
Safe Links Enabled	Real-time malicious link scanning
Calendar Sharing Disabled	Improved data privacy
Anonymous Meeting Access Disabled	Secured collaboration environment



Anti-Spam & Bulk Filtering	Reduced spam and phishing reach
Other minor configurations	Overall system hardening & compliance readiness

Before Implementation	After Hardening
<p>Your secure score <span>Include ▾</span></p> <p><b>Secure Score: 36.19%</b></p> <p>76/210 points achieved</p> <p>0% 50% 100%</p> <p>09/24 09/25 09/26</p> <ul style="list-style-type: none"> <li>• Default Microsoft 365 security settings active</li> <li>• No MFA or Conditional Access policies applied</li> <li>• Legacy authentication protocols still enabled</li> <li>• Calendar and Teams meetings accessible externally</li> <li>• Phishing and spam protection at default (low) sensitivity</li> <li>• Secure Score: <b>36.19% (76/210 points)</b></li> </ul>	<p>Your secure score <span>Include ▾</span></p> <p><b>Secure Score: 84.25%</b></p> <p>230/273 points achieved</p> <p>0% 50% 100%</p> <p>09/24 09/26 09/28 09/30 10/02 10/04 10/06 10/08 10/10 10/12 10/13</p> <ul style="list-style-type: none"> <li>• Secure Score: 36% → 81.68% (+45.68 points)</li> <li>• 99.9% reduction in unauthorized sign-ins</li> <li>• 70% fewer phishing and spoofing attempts</li> <li>• 100% MFA + Conditional Access coverage</li> <li>• 60% drop in spam and bulk mail delivery</li> <li>• 0 successful external login attempts</li> <li>• Fully compliant with CIS Microsoft 365 Benchmark</li> </ul>

## Section 5: Key Takeaway

AJX Security Consulting's transformation demonstrates the importance of building security from within. By securing its own Microsoft 365 environment first, AJX proved its ability to deliver measurable, reliable, and scalable protection to clients.

Through disciplined implementation, detailed auditing, and continuous improvement, AJX ensures that every client receives the same high level of data protection, compliance readiness, and peace of mind that defines the company's own operations.



---

## Contact Us

AJX Security Consulting | [info@ajxsecurityconsulting.com](mailto:info@ajxsecurityconsulting.com) | [www.ajxsecurityconsulting.com](http://www.ajxsecurityconsulting.com)