Avanan Email and Collaboration Cyber Threat Protection

Key Features changes side by side

Feature	Current (Retired)	Advanced Protect (New)
AI Anti-Phishing	☑	☑
Anti-Spam Filtering	☑	☑
Known Malware Prevention	☑	☑
Reputation-Based URL Protection	☑	☑
File Sandboxing	☒	☑
Real-Time URL Sandboxing	☒	☑
Account Takeover Protection	☒	☑
Shadow IT Detection	☒	☑

What changes might I notice while the upgraded Avanan protection is keeping me safe?

Some clients may experience a change in how their email and other collaboration tools protection works such as:

Email Handling

- Emails may be delayed slightly more often due to deeper inline scanning and sandboxing.
- Fewer suspicious emails will reach inboxes, so users may see less need to report phishing.

Quarantine

- Quarantine notifications and portals may look different or show more detailed threat reasons.
- Users might see additional categories for blocked items (eg “Advanced Threat” instead of just “Malware”).

Link Behaviour

- When clicking links in emails, users may notice redirects or brief checks before opening (click-time protection).
- Some links may open in a safe preview mode first.

File Access

- Attachments could open in a sanitised version (e.g., stripped macros) without warning.
- Larger or unusual files might take longer to download due to advanced scanning.

Notifications

- Users may receive more frequent security alerts or informational banners explaining blocked content.
- Language in alerts may reference “Advanced Protection” or “Sandbox” instead of generic terms.

Collaboration Apps

- Teams, SharePoint, OneDrive, etc., users might see blocked file messages in those apps where previously they didn’t.

If you have any questions about Avanan or to find out how well your business is protected against the latest Cyber Security Threats, please reach out to your T4B Account Manager to discuss.

AVANAN

Avanan sits at the cutting edge of email security with its patented inline protection and innovative machine learning.

Block sophisticated social engineering attacks

Effective defence before the inbox securing inbound, outbound and internal emails from impersonation, zero-day phishing and Business Email Compromise.

Protection from malware and ransomware

Scans every message, file and application for malware, blocking attacks that evade traditional scans. Cleans files to deliver a safe version in under two seconds.

Identifies and remediates compromised accounts

Analyses login events and end user activities across every cloud application, identifying unusual, potentially malicious behaviour.

Data Loss Prevention

Detects sensitive data sharing via email and collaboration apps and immediately limits data exposure. Inappropriately shared data is blocked or "unshared" to prevent data leaks.

Protects against account takeover and insider threats

Monitors over 100 indicators to identify compromised accounts. Real time scan and quarantine of internal emails + deny and block suspicious logins to prevent lateral attacks.