THREATLOCKER® CLOUD CONTROL

BENEFITS

Mitigate Microsoft 365 token theft and phishing attacks

Reduce risks of phishing attacks and token theft in your Microsoft 365 tenant.

Minimize downtime and business disruptions

Ensure business continuity, avoid the financial impact from breaches.

Reduce cyber risk

Limit attack surface and future-proof against evolving threats.

Some of the biggest challenges with Microsoft 365 are phishing and token theft. The problem is you can't control what users click on. They see a convincing email, are in a rush, or are simply distracted. Next thing you know, they enter their credentials, approve the MFA prompt—and just like that, the cybercriminals get in with full access to users' accounts.

Introducing ThreatLocker® Cloud Control, your new powerful ally to protect your Microsoft 365 tenant against phishing attacks and token thefts.

With a state-of-the-art built-in intelligence capability at its core, ThreatLocker Cloud Control automatically tracks your users' protected devices, records their IP addresses, and determines with high precision the trusted connections. It keeps you in the know. No more disruptions or manual updates.

The result?

Only users from IP addresses associated with your protected devices can get in—automatically blocking phishing and token theft attacks. So, no matter how successful cybercriminals are with their phishing attacks and stealing tokens—all their efforts are useless now.

How the ThreatLocker Cloud Control protects your users and organization

With the ThreatLocker Agent installed on users' laptops and ThreatLocker MDS on their phones, users' latest IP addresses are now logged.

- A user connects to a new network with their protected device, and their IP address changes.
- ThreatLocker tracks and learns commonly used IP addresses and automatically updates your Microsoft 365 named locations, maintaining a collection of the most up-to-date IP addresses associated with the protected device.
- Should a cybercriminal manage to intercept your user's token with an adversary in the middle attack, or steal login credentials through phishing, they simply won't be able to get in. Why? Because their IP address isn't in a permitted named location. **No match. No entry.**

Vulnerability	Microsoft 365 without ThreatLocker® Cloud Control	Microsoft 365 with ThreatLocker® Cloud Control
Token theft		
Bypassing MFA	VULNERABLE	PROTECTED
Persistent access	VULNERABLE	PROTECTED
Cloud exploitation (OneDrive, SharePoint, Outlook)	VULNERABLE	PROTECTED
Phishing attacks		
Credentials harvesting	VULNERABLE	PROTECTED
App consent scams	VULNERABLE	PROTECTED
QR code phishing	VULNERABLE	PROTECTED
Business email compromise		
Internal email fraud	VULNERABLE	PROTECTED
Financial theft	VULNERABLE	PROTECTED
Data exfiltration	VULNERABLE	PROTECTED

About ThreatLocker®

ThreatLocker® is a Zero Trust Endpoint Protection Platform that improves enterprise-level server and endpoint security with Zero Trust controls, including: Allowlisting, Ringfencing™, Storage Control, Network Control, ThreatLocker® Detect, Elevation Control, and Configuration Manager.

sales@threatlocker.com

+1-833-292-7732

threatlocker.com