OVERVIEW

Messageware Exchange Protocol Guard

> *Messageware's EPG is monitoring and securing connections and logins from all over the world. It would be impossible for my team to manage all the data without this*
>
> **VP of Messaging, Multinational Telco**

Complete Exchange Server Security & Intelligence Software

Messageware Exchange Protocol Guard (EPG) provides advanced login intelligence and control for Microsoft Exchange Servers by monitoring potential risks from attacks through a variety of Exchange services and protocols. Enhance your on-premises Microsoft Exchange security with real-time threat detection and security controls.

Exchange services are not protected - even with 2FA/MFA. Hackers and bots are constantly probing your Exchange Server to find vulnerabilities. Brute force password guessing, password spraying, widespread AD lockouts, and zero-day attacks cause significant damage and create havoc in your support center.

EPG proactively secures Exchange services: Outlook Web, EWS, ECP, ActiveSync, Autodiscover, OAB, MAPI/RCP, MAPI/HTTP and REST.

- ☑ Be alerted to suspicious activity before attacks escalate
- ☑ Clear visibility of all traffic from legitimate and non-legitimate sources
- ☑ Automatic blocking and securing of suspicious login traffic
- ☑ Automatic alerts and reports for server probes and attacks
- ☑ Real-time banning of devices known to be infected or associated with cyber-crime

Messageware EPG Highlights

Stop Systems from Scanning Your Server
Real-time banning of suspicious connections, geographic locations, and fake email addresses. Only legitimate corporate users are allowed to connect to your Exchange Servers.

Customizable Rules and Policies
Configure a sophisticated set of access controls and monitoring features to match your corporate security plan.

Secure What 2FA Leaves Vulnerable
Popular Multi-factor solutions leave Exchange services vulnerable. By combining 2FA/MFA technologies with EPG, key Exchange services can be secured.

Detect and Analyze Threats
Constantly monitoring and analyzing connection data for patterns, EPG helps detect and stop malicious activity. EPG also provides a full range of out-of-the-box reports to help you create, deploy, and manage your organization's security policies.

Protect Against Low-Volume Attacks (LVA)
Identify targeted persistent attacks that typically evade traditional detection by attacking below Active Directory lockout thresholds.

Protect Against High-Volume Attacks (HVA)
Identify brute force attacks that typically trigger mass Active Directory lockouts that prevent all affected users from logging on. Or, successfully steal logon credentials that can be used in attacks on the whole network.

Reduce the Load on Your Support Desk
Implements a lockout system independent of Active Directory. This eliminates the need for constant password resets that can occur during brute force and password spray attacks.

Generate Automatic Alerts
Delays in recognizing attacks can be costly. Configure automatic monitoring to ensure rapid response to threat detections.

When connections to your Exchange Server are not from your users: Stop them from connecting and probing!