FPT SOFTWARE MICROSOFT SENTINEL WITH ALERTIQ

Engagement Summary

FPT Software and Microsoft provide unified service, ***AlertIQ with Microsoft Sentinel*** for comprehensive threat management, automating responses, ensuring real-time information sharing, self-healing and preventing cross-domain attacks effectively. We not only deploy the solution just, but we also optimize your instance according to your budget and the security value of your potential log sources. Our security experts lead your team through a security goals exercise to help you clarify your priorities, help to reduce ***90% alert fatigue***, save ***20-40% run operations vs legacy approach*** and reduce ***50% average time for SIEM go-live support.***

5 weeks or fewer for you to see ROI quickly

ANALYZE

We analyze your requirements, your priorities, your budget and your environment for a SIEM deployment with recommended integration in your setting.

DEFINE

Define scope and detailed plan for integrating Microsoft Sentinel with AlertIQ in your production environment to provide a cost estimate along the way.

DISCOVER

We carry out a Security Goals Exercise and implement over 130 analytic rule sets and 100 threat hunting queries aligned with MITRE ATT&CK, a custom security dashboard, and 20 automation playbooks.

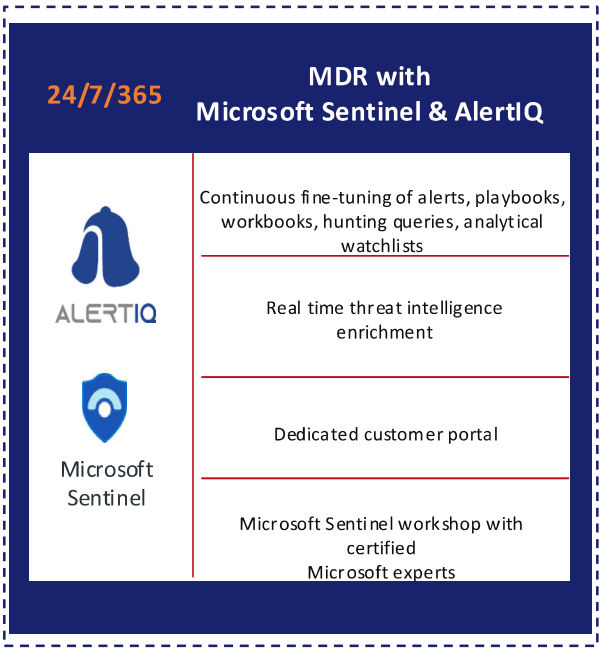
CLOSEOUT & PROCEED

We deliver an Engagement Summary outlining the work completed, along with a prioritized set of recommendations to help you maximize the value of Microsoft Sentinel.

Keep ahead of evolving security challenges

Our service is built for:

- **Rapid Response:** Quickly detect and remediate breaches to protect your finances and reputation.
- **Enhanced Defense:** Strengthen your security with a co-managed approach that elevates your defenses.
- **Proactive Protection:** Identify threats as they emerge, enabling preemptive action.
- **Insightful Intelligence:** Amplify your investments with targeted threat insights from a global perspective.
- **Optimized Value:** Streamline oversight and orchestration across your assets to maximize returns.



FPT SOFTWARE MICROSOFT SENTINEL WITH ALERTIQ

24/7, Microsoft-focused threat coverage

Our team provides 24/7 threat monitoring and proactive hunting, combining Microsoft security tools with AlertIQ. Upon confirming a threat, we alert you instantly, delivering a unified timeline with enriched insights from both platforms, giving you a clear and comprehensive security perspective

Delegate alert analysis and investigation

Our automated playbooks seamlessly integrate with Microsoft security tools and AlertIQ to contain threats and notify teams upon confirmation. With Active Remediation, our Threat Hunting Team can respond directly, banning IPs, collecting forensics, quarantining files, and more for swift resolution

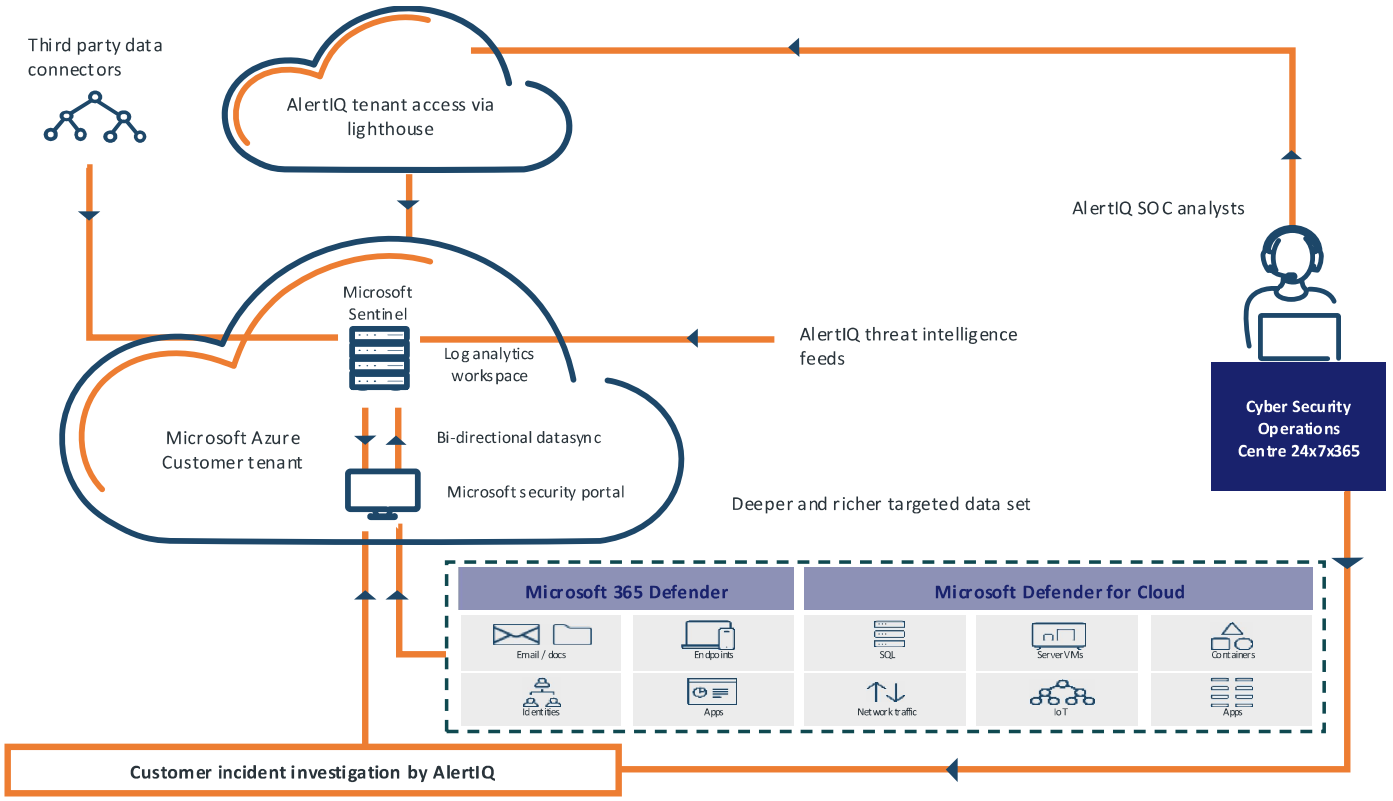
Identify threats that could be overlooked

Route your Microsoft alerts to AlertIQ, where our experts and automated systems filter out noise, notifying you only of confirmed suspicious activity. We can dive into Microsoft Sentinel as needed for further investigation, allowing you to review critical alerts in either Sentinel or AlertIQ—whichever you prefer.

Speed up detection and recovery

Our unique detection capabilities significantly boost your threat visibility, uncovering nearly four times more threats than Defender alone. By applying advanced, behavior-driven detections across raw telemetry from your endpoints and cloud, we ensure broad and precise security coverage

How our co-approach with Microsoft works



To learn more about FPT Software, please visit our website at **www.fpt-software.com/service/cyber-security**