Security Technology Recommendations

Leverage this reference list of security and compliance services to better understand industry technologies compared to Atmosera's best practices.

Many security functions are not included in cloud environments. This is a list of major technologies compared against Atmosera's Security Best practices and common industry compliance controls. This list includes some Azure components as they would apply to an environment in Azure, all other items are vendor agnostic.

ORANGE: *Atmosera uses non-Microsoft/Azure technology*
BLUE: *Atmosera uses Microsoft/Azure technology*

Service Type	Security Best Practices	Common Compliance Controls
Monthly System Patching	Recommended	Fulfills
End-Point Protection	Recommended	Fulfills
Multi-Layer Network Design	Recommended	Fulfills[1]
Azure NSG	Minimum Recommendation	Insufficient[2]
IPS/IDS	Recommended	Fulfills
Vulnerability Management	Recommended	Fulfills
Log Retention	Minimum Recommendation	Minimum to Fulfill
SIEM	Recommended	Recommended[3]
Web Application Firewall (Detect Mode)	Minimum Recommendation	Minimum to Fulfill
Web Application Firewall (Prevent Mode)	Recommended	Recommended
Web Application Scanning (DAST)	Recommended	Fulfills
Penetration Testing	Recommended	Fulfills
File Integrity Monitoring (FIM)	Only When Mandated[4]	Fulfills[5]
DDoS Protection	Recommended[6]	Not Required
Azure Defender	Recommended[7]	Recommended
Multi-Factor Authentication	Recommended	Fulfills
Azure Active Directory Free	Minimum Recommendation	Insufficient
Azure Active Directory P1 or P2	Recommended	Fulfills
Next-Gen Firewall	Recommended	Fulfills[8]
Azure Front Door	Recommended[9]	Recommended[9]

[1] This only applies to multi-function environments where the different functions would need to be segregated; this does not apply to single-function environments.

[2] Azure NSG is insufficient to meet common compliance controls due to its lack of Next Gen Firewall capabilities such as advanced logging and IPS/IDS

[3] Log Reviews are required by compliance frameworks and SIEM also satisfies this requirement by applying automation to the review process

[4] FIM is not recommended if it's not required. This is because FIM adds a lot of additional overhead in terms of management and data that is rarely used

[5] FIM is only required by the PCI compliance framework

[6] DDoS Protection is only recommended if you are a regular target of Denial-of-Service attacks

[7] Azure Defender is only recommended if the alerts will be regularly reviewed and investigated, otherwise this will provide no value

[8] This is required due to its IPS/IDS capabilities and advanced logging

[9] Azure Front Door combines capabilities of WAF, CDN and Load Balancer so it can be used in replacement of these technologies for security and compliance