**Defender for EASM**

Microsoft Defender External Attack Surface Management (Defender EASM) continuously discovers and maps your digital attack surface to provide an external view of your online infrastructure. This visibility enables security and IT teams to identify unknowns, prioritize risk, eliminate threats, and extend vulnerability and exposure control beyond the firewall. Attack Surface Insights are generated by leveraging vulnerability and infrastructure data to showcase the key areas of concern for your organization.

**Data residency, availability and privacy**

Microsoft Defender External Attack Surface Management contains both global data and customer-specific data. The underlying internet data is global Microsoft data; labels applied by customers are considered customer data. All customer data is stored in the region of the customer’s choosing.

For security purposes, Microsoft collects users' IP addresses when they log in. This data is stored for up to 30 days but may be stored longer if needed to investigate potential fraudulent or malicious use of the product.

In the case of a region down scenario, customers should see no downtime as Defender EASM uses technologies that replicate data to a backup region. Defender EASM processes customer data. By default, customer data is replicated to the paired region.

The Microsoft compliance framework requires that all customer data be deleted within 180 days of that organization no longer being a customer of Microsoft.  This also includes storage of customer data in offline locations, such as database backups. Once a resource is deleted, it cannot be restored by our teams.  The customer data will be retained in our data stores for 75 days; however, the actual resource cannot be restored.  After the 75-day period, customer data will be permanently deleted.

**What is Discovery?**

Microsoft Defender External Attack Surface Management (Defender EASM) relies on our proprietary discovery technology to continuously define your organization’s unique Internet-exposed attack surface. Discovery scans known assets owned by your organization to uncover previously unknown and unmonitored properties. Discovered assets are indexed in a customer’s inventory, providing a dynamic system of record of web applications, third party dependencies, and web infrastructure under the organization’s management through a single pane of glass.