Meeting the TSA Cybersecurity Requirements for Airports and Aircraft with SentinelOne Singularity XDR

By Neil Torpey

The new TSA cybersecurity requirements mandate robust cybersecurity measures to protect against cyber threats in the aviation industry. These requirements apply to all U.S. airports and aircraft, and non-compliance can result in penalties, legal action, and reputational damage for affected entities.

The following are the key functionalities of SentinelOne Singularity XDR and their business outcomes that can help enterprises meet these requirements:

**Dynamic Policy Assignment Based on Endpoint Tags and Location Awareness**

- Improved security posture.
- Reduced operational overheads.
- Simplied policy management.
- Streamlined security operations.
- Improved visibility.
- Reduced attack surface.

**SentinelOne Singularity XDR for Meeting the TSA Cybersecurity Requirements**

- The new requirements highlight the need for a comprehensive and proactive cybersecurity approach. By leveraging solutions such as Singularity XDR, enterprises can improve their security posture, reduce the risk of cyber attacks, and ensure compliance.

**Business Outcomes:**

- Improved security posture.
- Reduced operational overheads.
- Simplied policy management.
- Streamlined security operations.
- Improved visibility.
- Reduced attack surface.

**Reduced operational overheads**

- SentinelOne's rewall control solution is highly scalable and easy to manage. It has a central management architecture that simplifies policy management and ensures consistency, making it easier to meet the TSA's requirements. Unlike Microsoft solutions, which can be difficult to manage, SentinelOne supports cross-OS management, enabling enterprises to manage micro-segmentation policies dynamically across multiple operating systems, including Windows, macOS, and Linux.

**Simplied policy management**

- SentinelOne Singularity XDR's advanced multi-tenancy provides a centralized console for managing security policies, alerts, and incidents for multiple customers, making it ideal for enterprises with multiple sub-agencies, such as federal agencies. Additionally, SentinelOne's advanced multi-tenancy provides a centralized console for managing security policies, alerts, and incidents for multiple customers, making it ideal for enterprises with multiple sub-agencies, such as federal agencies.

**Scalability and Manageability**

- The tagging of policy assignments across different scopes and the ability to assign policies per application instead of per machine makes SentinelOne Singularity XDR a highly scalable solution.

**Micro-segmentation to reduce the attack surface**

- SentinelOne Singularity XDR enables enterprises to dynamically and automatically determine what rewall policies to assign to specific machines based on location, simplifying policy management and enhancing security.

**SentinelOne Singularity XDR for Large-Scale Enterprises**

- For large-scale environments, SentinelOne Singularity XDR provides easy-to-implement micro-segmentation, which improves visibility and strengthens overall security posture.

**Improved visibility**

- Micro-segmentation is critical to reducing the attack surface in enterprise environments.

**Regular vulnerability assessments**

- SentinelOne's rewall control solution is highly scalable and easy to manage. It has a central management architecture that simplifies policy management and ensures consistency, making it easier to meet the TSA's requirements. Unlike Microsoft solutions, which can be difficult to manage, SentinelOne supports cross-OS management, enabling enterprises to manage micro-segmentation policies dynamically across multiple operating systems, including Windows, macOS, and Linux.

**Reduced operational overheads**

- SentinelOne's rewall control solution is highly scalable and easy to manage. It has a central management architecture that simplifies policy management and ensures consistency, making it easier to meet the TSA's requirements. Unlike Microsoft solutions, which can be difficult to manage, SentinelOne supports cross-OS management, enabling enterprises to manage micro-segmentation policies dynamically across multiple operating systems, including Windows, macOS, and Linux.

**Simplied policy management**

- SentinelOne Singularity XDR's advanced multi-tenancy provides a centralized console for managing security policies, alerts, and incidents for multiple customers, making it ideal for enterprises with multiple sub-agencies, such as federal agencies.