CROWDSTRIKE

Data Sheet

Cyber Resilience for the Airline Industry

Helping regulated airport and aircraft operators meet TSA cybersecurity requirements

Prevent cyber breaches from disrupting critical airline operations

The U.S. Transportation Security Administration (TSA) is taking proactive measures to protect the nation's transportation system by issuing new cybersecurity requirements for TSA-regulated airports and aircraft operators.

These emergency actions from TSA are part of the plan to increase the cyber resiliency of critical infrastructure and prevent their degradation or disruption. These requirements are embraced by CrowdStrike's own best practices and solutions for protecting business operations and critical infrastructure:

- Network Segmentation
- Access Control Measures
- Continuous Monitoring and Detection
- System Patching

Key Benefits

Consolidate disparate point products with a single unified cybersecurity platform

Fortify your cybersecurity practices and controls, and enhance your cyber resilience

Prevent credential misuse and identity abuse

Protect your IT and OT environment with an integrated security solution

Hunt for threats and stop breaches on a continuous basis

Reduce the cost to operate and maintain a cyber resilient organization

Deliver expertise at scale to hunt, respond and remediate threats, enabling airlines to focus on their core mission: moving people and goods globally

Enhance your cyber resiliency to stop today's sophisticated attacks

Cybersecurity leaders in the airline industry need to enhance the cyber resiliency of their security operations to meet the new TSA requirements so they can prevent cyber breaches from disrupting the critical infrastructure supporting airport and airline operations.

CrowdStrike can help TSA-regulated airport and aircraft operators gain a deeper understanding of their threat landscape and meet the TSA mandates to enhance their cyber resiliency against threats actors looking to execute destructive attacks.

The CrowdStrike Falcon® platform delivers complete visibility to prevent attacks across endpoints, cloud workloads and identities in your information technology (IT) and operational technology (OT) systems and networks. CrowdStrike's advanced threat intelligence and human threat hunting stops even the stealthiest attacks, while CrowdStrike experts enable you to respond to incidents with speed and precision to prevent business degradation and disruption of airline operations.

Key solution features

Airport and aircraft operators run complex networks of IT and OT systems to move passengers and freight safely and efficiently across the United States.

Adversaries, on the other hand, are looking to disrupt those operations and compromise those systems, increasing the need for effective cybersecurity resiliency and controls.

Network Segmentation

- **CrowdStrike Falcon® Firewall Management** enables network segmentation through the creation, management and enforcement of firewall policies and controls with a simple, centralized approach across your IT and OT environment.
- **CrowdStrike's Red Team Exercises** can test that network segmentation policies and controls are working as intended and that threat actors are unable to move laterally and penetrate different segments of the network.

Access Control Measures

- **CrowdStrike Falcon® Identity Protection** prevents unauthorized access to critical cyber systems and reduces the opportunity for privilege escalation by threat actors using compromised credentials. The solution monitors and hardens your Active Directory environment, providing better identity protection.
- Given that more than 80% of today's threats begin with compromised credentials, go one step beyond identity and access management with **CrowdStrike Store** partner integrations of leading identity provider solutions like **Okta** and **Ping**, and use **Falcon Identity Protection** to deliver conditional-based access that enforces multifactor authentication when suspicious user activity is detected on the network.

Continuous Monitoring and Detection

- **CrowdStrike Falcon® Insight XDR** delivers industry-leading detection and response capabilities for your IT environment across your endpoints and cloud workloads. This AI-powered solution has powerful detection policies and automated response procedures for both malware and malware-free attacks, stopping the majority of breaches in real time.
- **CrowdStrike® Falcon OverWatch™** is CrowdStrike's managed threat hunting service that delivers continuous monitoring and hunting for those "hard to detect, never seen before" zero-day attacks and hands-on-keyboard activity that can evade even the best automated detection solutions. These expert hunters relentlessly scour for unknown and advanced threats targeting your organization.
- **CrowdStrike Falcon® Insight XDR plus Corelight** delivers network detection and response (NDR) for your IT and OT environment, including operational control systems and other anomalous devices on the network. This added layer of network protection aggregates network detections together with endpoint and cloud workload detections to give you complete visibility to threat activity and threat severity in the Falcon console.

Why choose CrowdStrike?

Advanced Threat Intelligence: Falcon Intelligence tracks over 200 adversaries across the globe with deep insight into threat actors targeting the transportation, aerospace and aviation industries, and the sophisticated tactics and techniques they use to attack business operations.

Superior Technology: The Falcon platform leads the industry in endpoint security, cloud workload security, identity protection and threat intelligence in a single unified solution.

World-class Threat Hunting: The Falcon OverWatch global threat hunting service operates 24/7 to unearth advanced threats wherever they operate.

Expert Detection and Response: The Falcon Complete fully managed detection and response (MDR) service stops breaches on endpoints, workloads and identities with expert management, threat hunting, monitoring and remediation.

- **CrowdStrike Falcon® Cloud Security** delivers unified visibility and security for hybrid and multi-cloud environments in a single cloud-native application protection platform (CNAPP). Falcon Cloud Security secures workloads, containers and serverless environments with one-click deployment, through a unified agent and an agentless platform.

System Patching

- **CrowdStrike Falcon® Spotlight** vulnerability management identifies unpatched systems and updates required for the OS, applications, drivers and firmware. Falcon Spotlight utilizes scanless vulnerability assessment technology, delivering always-on, automated vulnerability management that prioritizes risks in real time.
- **CrowdStrike Falcon® Discover** IT hygiene provides the additional benefit of a complete asset inventory with visibility across the network. Many breaches occur on unprotected devices on the network, so having real-time visibility of managed and unmanaged devices on the network helps in discovering, prioritizing and patching systems to mitigate risk of exposure.
- **CrowdStrike's Technical Risk Assessment** deploys Falcon Spotlight and Falcon Discover and provides you with prioritized actionable recommendations to improve IT hygiene across your environment.

Fully Managed Detection and Response

- **CrowdStrike Falcon® Complete** is CrowdStrike's fully managed detection and response (MDR) service for endpoints, cloud workloads, identities and data logging, using highly skilled CrowdStrike experts to administer the platform, respond to incidents and hunt for threats 24/7 using the full power of the Falcon platform.
- For organizations that lack the skills and resources to enhance their level of resilience in a timely manner, **Falcon Complete** offers the best and most cost-effective solution.

Incident Response and Advisory Services

- **CrowdStrike Incident Response Services** deliver incident response, forensic investigation and endpoint recovery when a breach occurs on an unprotected device on the network.
- **CrowdStrike Advisory Services** help customers fortify their cybersecurity practices and controls, prepare their teams to defend against the latest threats, and test components of their IT/OT environment to see if they can withstand an attack.
- **CrowdStrike's Services Retainer** provides on-demand access to CrowdStrike incident responders, forensic investigators, recovery specialists and cybersecurity consultants to help maintain a cyber resilient organization.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

The CrowdStrike Falcon Platform

Falcon Prevent
Next-generation antivirus (NGAV)

Falcon Insight XDR
Endpoint detection and response (EDR) and extended detection and response (XDR)

Falcon Complete
Managed detection and response (MDR)

Falcon OverWatch
Managed threat hunting

Falcon Intelligence
Automated threat intelligence

Falcon Identity Protection
Identity threat protection

Falcon Cloud Security
Cloud discovery, workload protection and posture management

Falcon Discover
Asset visibility and hygiene

Falcon Spotlight
Vulnerability and patch management

Falcon Firewall Management
Host firewall

Falcon Device Control
USB device security

Falcon Forensics
Forensic data collection and investigation

Falcon FileVantage
File integrity monitoring

Falcon Surface
External attack surface management

Falcon Intelligence Recon
Deep dark web monitoring

Falcon LogScale
Observability and log management

CrowdAlliance Partner Integrations

Falcon Insight XDR + Corelight
Network detection and response (NDR)

Falcon Insight XDR + Proofpoint
Email protection

Falcon Insight XDR + Ping/Okta
Access management and multifactor authentication

Free Trial

Learn more at **www.crowdstrike.com**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**