CDN NETWORK DEFENDER & THE TRUSTED PARTNER NETWORK (TPN)

The deployment of CDN Network Defender's automated threat detection and blocking solution addresses certain controls in virtually every cybersecurity compliance standard, including the Motion Picture Association's *Content Security Best Practices Common Guidelines*[1], the governing document for the TPN.

The table below lists the Best Practices controls that are addressed either partially or in full by the deployment of CDN Network Defender's solution.

Trusted Partner Network (TPN) Best Practices Guidelines Addressed by Celerium

DS-1.0	Firewall / WAN / Perimeter Security	Separate external network(s)/WAN(s) from the internal network(s) by using inspection firewall(s) with Access Control Lists that prevent unauthorized access to any internal network and with the ability to keep up with upload and download traffic.
DS-1.1	Firewall / WAN / Perimeter Security	Implement a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the business every 6 months.
DS-1.2	Firewall / WAN / Perimeter Security	Deny all incoming and outgoing network requests by default. Enable only explicitly defined incoming requests by specific protocol and destination. Enable only explicitly defined outgoing requests by specific protocol and source.
DS-1.2.1	Firewall / WAN / Perimeter Security	Firewalls should be configured to actively alert security members of key security events
DS-2.0	Internet	Prohibit production network and all systems that process or store digital content from directly accessing the internet, including email. If a business case requires internet access from the production network or from systems that process or store digital content, only approved methods are allowed via use of a remote hosted application / desktop session. (Access to restricted sites is prohibited, including web-based email sites, peer-to-peer, digital lockers, and other known malicious sites)
DS-2.1	Internet	Implement email filtering software or appliances that block the following from non-production networks: ▪ Potential phishing emails ▪ Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.) ▪ File size restrictions limited to 30 MB ▪ Known domains that are sources of malware or viruses
DS-2.2	Internet	Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites.

1https://www.motionpictures.org/what-we-do/safeguarding-creativity/additional-resources/#content-protection-best-practices