



DATASHEET (DIGITAL GUARDIAN)

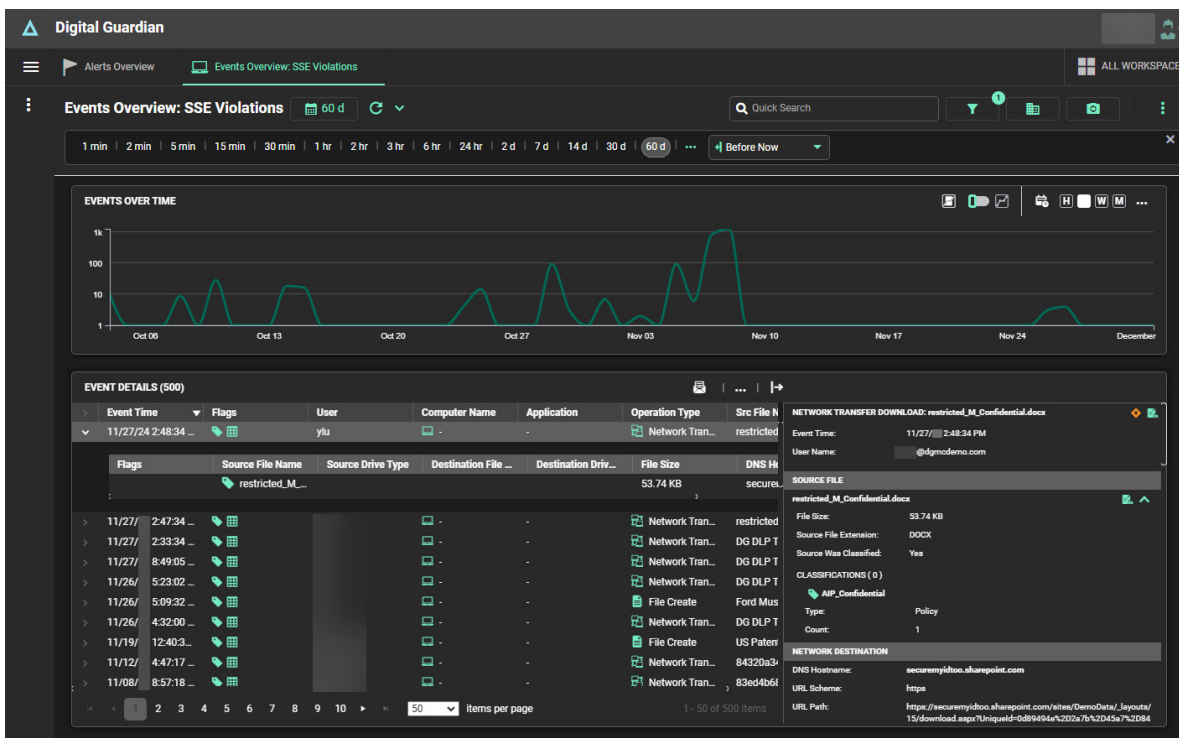
# Digital Guardian Analytics & Reporting Cloud (ARC) Integrated with SSE

Digital Guardian’s Analytics and Reporting Cloud (ARC), powered by Amazon Web Services (AWS), provides deep insights into data usage, policy violations, and security workflows. By analyzing endpoint and network events, ARC enhances visibility and enables effective responses to both insider and outsider threats.

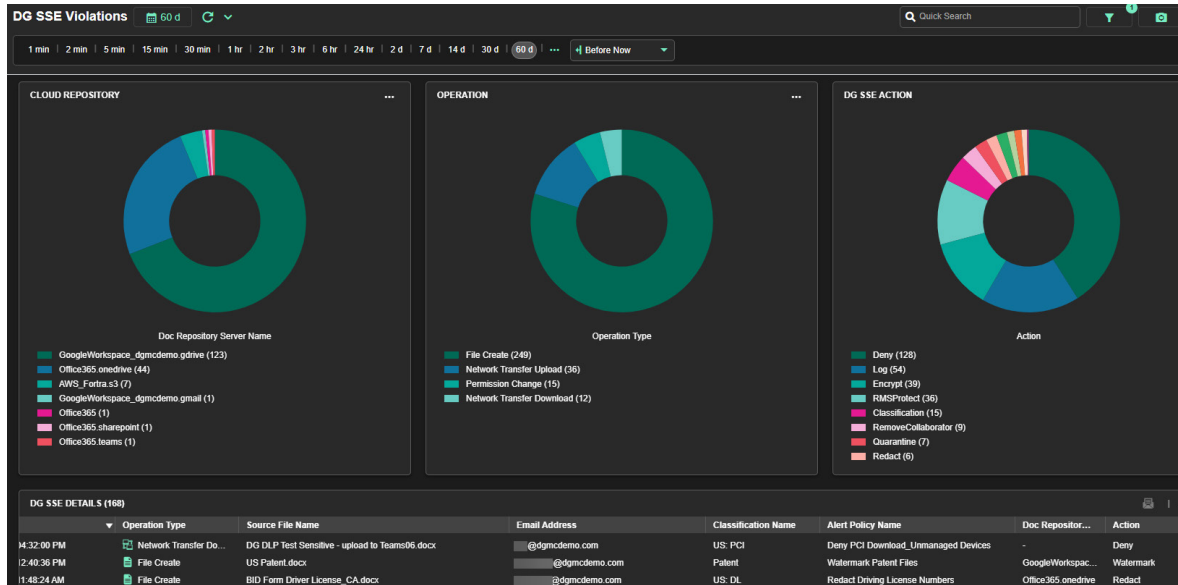
With the integration of Digital Guardian’s Security Service Edge (DG SSE) into ARC, organizations gain unified security capabilities across endpoints, cloud, web, and internal access channels. This integration includes Endpoint Data Loss Prevention (DLP), Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), and Zero Trust Network Access (ZTNA), delivering robust data protection and threat prevention.

SWG mitigates web threats by analyzing real-time traffic, blocking malicious sites, and ensuring compliance. ZTNA replaces traditional VPNs with zero trust, identity-based access to internal resources, ensuring granular control over user permissions.

Together, Digital Guardian SSE empowers security teams with comprehensive visibility and unified policies, enhancing data protection and incident response across all key access points.



Summary of Reported Violations According to DG SSE Control Policies covering multiple IT Channels and File Operation Activities.



Summary of Reported Violations According to DG SSE Control Policies covering multiple IT Channels and File Operation Activities.

## Comprehensive Threat Prevention and Visibility

The combination of SWG and CASB delivers robust threat prevention by blocking web-based threats, monitoring cloud usage, and controlling shadow IT. ZTNA complements these measures by authenticating every access request, ensuring that only authorized users can interact with sensitive systems. ARC serves as the central hub for these efforts, providing real-time monitoring and reporting to help security teams detect anomalies, address potential risks, and maintain compliance with regulatory standards such as GDPR, HIPAA, and PCI-DSS.

By integrating these capabilities, Digital Guardian SSE empowers organizations with visibility across endpoints, cloud services, and web traffic. This unified perspective enables security teams to respond swiftly to incidents while maintaining seamless operations and user experiences.

## Enhanced Compliance and Remote Work Security

For organizations striving to meet regulatory requirements, Digital Guardian SSE simplifies compliance by generating detailed reports on data access, transfers, and security events. These insights ensure adherence to industry regulations and provide the necessary documentation for audits. **Endpoint DLP** secures data in use, at rest, or in motion across devices like USBs and email, while **CASB** expands this protection to cloud applications, helping prevent data breaches in SaaS, IaaS, and PaaS environments. **Secure Web Gateway (SWG)** blocks malicious websites, filters web traffic, and inspects encrypted data to stop web-based threats. Additionally, Digital Guardian's **ZTNA** and SWG make remote work more secure by replacing traditional VPNs with zero trust access controls and extending web traffic protections to users outside corporate networks.

## Resilience Against Emerging Threats

As threats evolve, Digital Guardian SSE provides organizations with the tools to stay ahead. ZTNA ensures that even compromised credentials cannot bypass its strict access controls. SWG and CASB work together to identify and mitigate emerging risks, such as ransomware and phishing attacks, while ARC's centralized monitoring ensures continuous improvement in threat detection and response. With ARC's **centralized visibility and reporting**, security teams can effectively monitor data flows, address potential threats, and ensure adherence to regulatory standards, including GDPR and HIPAA. Fortra's solutions support a **seamless user experience** and consistent security enforcement across all platforms, strengthening organizational resilience against new and emerging threats.

POLICY NAME	CONTENT INSPECTION TYPE	CLOUD APPLICATIONS	POLICY ACTIONS	PRIORITY	STATUS
Remove Ext User_MRN from Project Venus	DLP Scan	(1)	Allow & Log, Remove Collaborator	1	On
Remove Public from Sourcecode files	DLP Scan	(1) (1) (1) (1)	Allow & Log, Remove Shared Link	2	On
Remove Untrusted Users from PCI Files	DLP Scan	(1) (1) (1)	Allow & Log, Remove Collaborator	3	On
Encrypt All Files_Corporate Assets Folder	None	(1)	Content Digital Rights	4	On
Quarantine Bank Account Number Files	DLP Scan	(2) (1) (1)	Quarantine	5	On
Watermark Patent Files	DLP Scan	(1) (1) (1) (1)	Content Digital Rights	6	On
Redact Driving License Numbers	DLP Scan	(2) (1) (1) (1) (1)	Content Digital Rights	7	On
Apply AIP Label (Confidential)_KW_Mercury	DLP Scan	(1) (1) (1) (1)	AIP Protect	8	On
Apply AIP Label (General)_KW_Venus	DLP Scan	(1) (1) (1) (1)	AIP Protect	9	On
Apply AIP Label (Encrypted)_KW_Mars	DLP Scan	(1) (1) (1) (1)	AIP Protect	10	On
Apply GLabel (Confidential)_KW_Jupiter	DLP Scan	(1)	Content Digital Rights	11	On
Apply GLabel (Restricted)_KW_Saturn	DLP Scan	(1)	Content Digital Rights	12	On

Example of DG SSE Control Policies covering multiple IT Channels.

Digital Guardian’s ARC and SSE integration deliver a holistic approach to data protection, combining DLP, CASB, SWG, and ZTNA into a unified solution. This pairing delivers a robust foundation for proactive, informed, and adaptive security strategies, empowering companies to safeguard sensitive data, ensure compliance, and maintain business continuity in a rapidly changing digital environment. With comprehensive threat prevention, enhanced visibility, and robust compliance support, this solution empowers organizations to secure sensitive data across all channels while meeting the demands of today’s dynamic security landscape. Whether protecting cloud environments, securing web traffic, or enabling secure remote work, Digital Guardian ensures resilience, compliance, and peace of mind.



Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We’re creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We’re the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at [fortra.com](https://fortra.com).