FORTRA

DATASHEET (FORTRA DLP)

Fortra DLP Analytics & Reporting Cloud (ARC) Integrated with SSE

Fortra DLP 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.

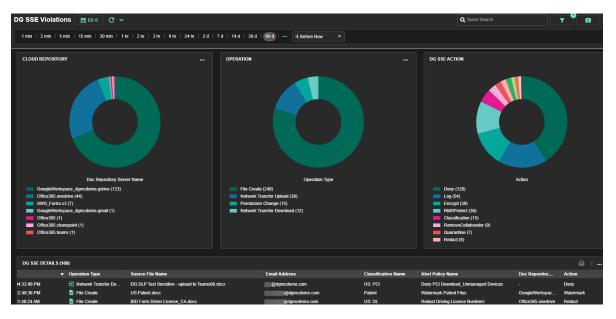
With the integration of Fortra SSE into ARC, organizations gain unified security capabilities across endpoints, cloud, web, and internal access channels. This integration includes Endpoint Data Loss Prevention (DLP), Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), and Zero Trust Network 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, Fortra DLP SSE empowers security teams with comprehensive visibility and unified policies, enhancing data protection and incident response across all key access points.

Digita	l Guardian												
	lerts Overview	Events Overview: SSI	E Violations									ALL	WORKSF
Even	nts Overview: S	SE Violations	🛱 60 d 🖸 🗸				Q Quick	Search		T O			
1 m	min 2 min 5 mir	n 15 min 30 min	1 hr 2 hr 3 hr	6 hr 24 hr 2 d	7 d 14 d 30	d 60 d 4	Before Now						
EV	VENTS OVER TIME									▶ 2	i	H 🗌 W M)
	1k												
10	00												
	10												
	Oct 06	Oct 13	Oct 20	Oc	t 27	Nov 03	Nov 10	Nov 1	17	Nov 3	24	D	lecembe
EV	VENT DETAILS (500) Event Time	▼ Flags	User	Computer Name	Application	Dperation Type	→ Src File N	NETWORK TRANSFER DOW	INLOAD: restricted_	M_Confidenti	ial.docx		♦
>		-	User ylu	Computer Name	Application				NLOAD: restricted_ 11/27/ 2:48:34		ial.docx		♦
>	Event Time 11/27/24 2:48:34 _	•	ylu		•	Operation Type	Src File N restricted	NETWORK TRANSFER DOW		I PM	ial.docx		◆ ■
>	Event Time	Source File Name	ylu Source Drive Type		Application - Destination Driv	Operation Type	Src File N	NETWORK TRANSFER DOW	11/27/ 2:48:34	I PM	ial.docx		• •
>	Event Time 11/27/24 2:48:34 _	•	ylu Source Drive Type		•	Operation Type Operation Type Network Tran File Size	Src File N restricted DNS He	NETWORK TRANSFER DOW Event Time: User Name:	11/27/ 2:48:34 @dgmcdemo.	I PM	ial.docx		 ♦ ■ ■
>	Event Time 11/27/24 2:48:34 _	Source File Name	ylu Source Drive Type		•	Operation Type Network Tran_ File Size 53.74 KB	Src File N restricted DNS He	NETWORK TRANSFER DOW Event Time: User Name: SOURCE FILE restricted_M_Confidential.d File Size:	11/27/ 2:48:34 @dgmcdemo. locx 53.74 KB	I PM	ial.doex		
>	Event Time 11/27/24 2:48:34 _ Flags	Source File Name restricted_M	ylu Source Drive Type	Destination File	•	Operation Type Compared Network Tran_ File Size 53.74 KB 2	Src File N restricted DNS Ha secured	NETWORK TRANSFER DOW Event Time: User Name: SOURCE FILE restricted M_Confidential.d File Size: Source File Extension:	11/27/ 2:48:34 @dgmcdemo. locx 53.74 KB DOCX	I PM	ial.doex		
>	Event Time 11/27/24 2:48:34 _ Flags : 11/27/ 2:47:34 _	Source File Name Prestricted_M Employed Employed Source File Name	ylu Source Drive Type	Destination File	•	Operation Type The Network Tran_ File Size 53.74 KB , Network Tran_	Src File N restricted DNS H secures	NETWORK TRANSFER DOW Event Time: User Name: SOURCE FILE restricted_M_Confidential.d File Size: Source File Extension: Source Was Classified:	11/27/ 2:48:34 @dgmcdemo. locx 53.74 KB	I PM	ial.docx		
>	Event Time 11/27/24 2-48:34 Flags 11/27/ 2-47:34 _ 11/27/ 2-33:34	Source File Name Prestricted_M Employed Employed Source File Name Prestricted_M	ylu Source Drive Type	Destination File	•	Operation Type Network Tran File Size 53.74 KB Network Tran Network Tran Network Tran	Src File N restricted DNS He secured restricted DG DLP T	NETWORK TRANSFER DOW Event Time: User Name: SOURCE FILE restricted, M, Confidential d File Size: Source File Entension: Source Via Classified: CLASSIFICATIONS (0)	11/27/ 2:48:34 @dgmcdemo. locx 53.74 KB DOCX	I PM	ial.doex		
>	Event Time 11/27/24 2:48:34 Flags 11/27/ 2:47:34 11/27/ 2:33:34 11/27/ 8:49:05	Source File Name Source File	ylu Source Drive Type	Destination File	•	Operation Type Network Tran File Size 53.74 KB Network Tran Network Tran Metwork Tran Metwork Tran Metwork Tran	Src File N restricted DNS Hk secureL restricted DG DLP T DG DLP T	NETWORK TRANSFER DOW Event Time: User Name: BOURCE FILE Frestricted, M. Confidential d Fils Size: Source Was Classified: CLASSIFICATIONS (0) AP_Confidential	11/27/ 2:48:34 @dgmodemo. loex S3.74 KB DOCX Yes	I PM	ial.doex		
>	Event Time 11/27/24 2:48:34 Flags 11/27/ 2:47:34 11/27/ 2:33:34 11/27/ 8:49:05 11/26/ 5:23:02	Source File Name • estricted_M • = = • = = • = = • = = • = = • = = • = = • = =	ylu Source Drive Type	Destination File	•	Operation Type Prile Size 53.74 KB Prile Size 54.74 KB Prile	Src File N restricted DNS He secure. restricted DG DLP T DG DLP T DG DLP T	NETWORK TRANSFER DOW Event Time: User Name: SOURCE FILE restricted, M, Confidential d File Size: Source File Entension: Source Via Classified: CLASSIFICATIONS (0)	11/27/ 2:48:34 @dgmcdemo. locx 53.74 KB DOCX	I PM	ial.docx		
>	Event Time 11/27/24 2:48.34 Flags 11/27/ 2:47:34 11/27/ 2:33:34 11/27/ 8:4905 11/26/ 5:23:02 11/26/ 5:09:32	Source File Name • estricted_M • = = • = = • = = • = = • = = • = = • = = • = =	ylu Source Drive Type	Destination File	•	Operation Type	Src File N restricted DNS He secure. restricted DG DLP T DG DLP T Ford Mus	NETWORK TRANSFER DOW Event Time: User Name: SOURCE FLE restricted (M. Confidential di File Size: Source File Extension: Source Was Classified: CLASSIFICATIONS (0) AP_Confidential Type: Count:	11/27/ 2:48:34 @dgmodemo. loex 53:74 KB DOCX Yes Policy	I PM	ial.docx		
>	Event Time 11/27/24 2:43:34 Rags 11/27/ 2:33:44 11/27/ 2:33:44 11/27/ 2:33:44 11/27/ 2:33:44 11/27/ 2:33:44 11/27/ 2:33:44 11/27/ 2:33:42 11/26/ 4:32:00	Source File Name Source File Name File Name Source File Name S	ylu Source Drive Type	Destination File	•	Operation Type ☆ Network Tran ✓ ✓ ✓ ✓ ✓ Network Tran ↔ ✓ ✓ ✓ ✓	Src File N restricted DNS He secureL restricted DG DLP T DG DLP T Ford Mus DG DLP T	NETWORK TRANSFER DOW Event Tene: User Name: BOUNCE FILE Testricted, M. Confidential File Size: Source Was Classified: CLASSFICATIONS (0) A P_Confidential Type:	11/27/ 2:48:34 @dgmodemo. loex 53:74 KB DOCX Yes Policy	I PM com	_		
>	Event Time 11/27/24 2-4834 Flags : 11/27/24 2-4834 11/27/24 2-4834 11/27/24 2-4834 11/27/24 2-4834 11/27/24 2-4834 11/27/24 2-4834 11/27/24 2-4834 11/27/24 2-4834 11/27/24 2-4834 11/26/24 2-484 11/26/24 2-484 11/26/24 2-484 11/26/24 2-484 11/26/24 2-484 <	Source File Name File Name File Na	ylu Source Drive Type	Destination File	•	Operation Type R Network Tran File Size 53.74 KB , Network Tran Network Tran Network Tran Network Tran Network Tran File Create R Network Tran File Create	Src File N restricted DNS H secureu restricted DG DLP T DG DLP T DG DLP T Ford Mus DG DLP T US Pateri 84320a3/	HETWORK TRANSFER DOW Event Terne: User Name: SOURCE FILE restricted, M., Confidential di File Size Source: File Extension: Source Was Classified: CLASSIFICATIONS (0) AP_Confidential Type: Count: HETWORK DESTINATION	liv27 2483 @dgmcdemo. 53.74 KB DOCX Yes Policy 1	I PM com	_		◆ B. B. ∧

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, Fortra DLP 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, Fortra DLP 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, Fortra DLP'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, Fortra DLP 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.

Access Policy				
Real Time Cloud Data Discovery				
New †		Search D		34
POLICY NAME	CONTENT INSPECTION TYPE	CLOUD APPLICATIONS	POLICY ACTIONS	PRIORITY * STATU
Remove Ext User_MRN from Project Venus	DLP Scan	(1)	Allow & Log, Remove Collaborator	1
Remove Public from Sourcecode files	DLP Scan	🔹 (1) 👝 (1) 🔥 (1) 💤	Allow & Log, Remove Shared Link	2
Remove Untrusted Users from PCI Files	DLP Scan	🔥 (1) 🔹 (1)	Allow & Log, Remove Collaborator	3
Encrypt All Files_Corporate Assets Folder	None	(1)	Content Digital Rights	4
Quarantine Bank Account Number Files	DLP Scan	🔼 (2) 🔹 (1)	Quarantine	5
Watermark Patent Files	DLP Scan	🔼 (1) 🔹 (1) 📲 (1) 📥 (1)	Content Digital Rights	6
Redact Driving License Numbers	DLP Scan	🔼 (2) 💞 (1) 🔹 (1) 💼 (1)	Content Digital Rights	7
Apply AIP Label (Confidential)_KW_Mercur	y DLP Scan	🔥 (1) 🛐 (1) 📲 😭 (1)	AIP Protect	8
Apply AIP Label (General)_KW_Venus	DLP Scan	🔥 (1) 🔹 (1) 📲 (1) 🌨 (1)	AIP Protect	9
Apply AIP Label (Encrypted)_KW_Mars	DLP Scan	🔼 (1) 🔹 (1) 📲 (1)	AIP Protect	10
Apply GLabel (Confidential)_KW_Jupiter	DLP Scan	(1)	Content Digital Rights	11
Apply GLabel (Restricted)_KW_Saturn	DLP Scan	(1)	Content Digital Rights	12

Example of DG SSE Control Policies covering multiple IT Channels.

Fortra DLP'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, Fortra DLP ensures resilience, compliance, and peace of mind.



About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.