Security and Privacy, Hand-in-Hand: Dtex's Anonymization Makes it Possible

With the new data anonymization feature in the Dtex Analytics Server, personal data is safer and more privacy-conscious than ever before. Dtex now anonymizes personal data – including user name and machine/domain name – as soon as the data is received by the Dtex server. This new approach allows enterprises to respect company culture, maintain security, and establish privacy regulation compliance seamlessly.

Why Anonymization?

At Dtex, we have always believed that security should not come at the cost of privacy, and we have built the Dtex User Behavior Intelligence Platform to strike that critical balance. Our data is far less invasive than many security solutions (no keylogging, no screenshots), but it can still potentially include personally identifiable information (PII). There are a few reasons why an enterprise might want to anonymize this data:

COMPANY CULTURE

Too many enterprises achieve internal visibility at the cost of privacy, damaging employee morale. Anonymization means that PII isn't even revealed to internal analysts, ensuring employees that their personal data is safe from prying eyes.

LAWS AND REGULATIONS

Privacy laws vary drastically between different countries and industries. Dtex's collection methods and anonymization abilities ensure that Dtex is legal even under some of the strictest privacy regulations in the world.

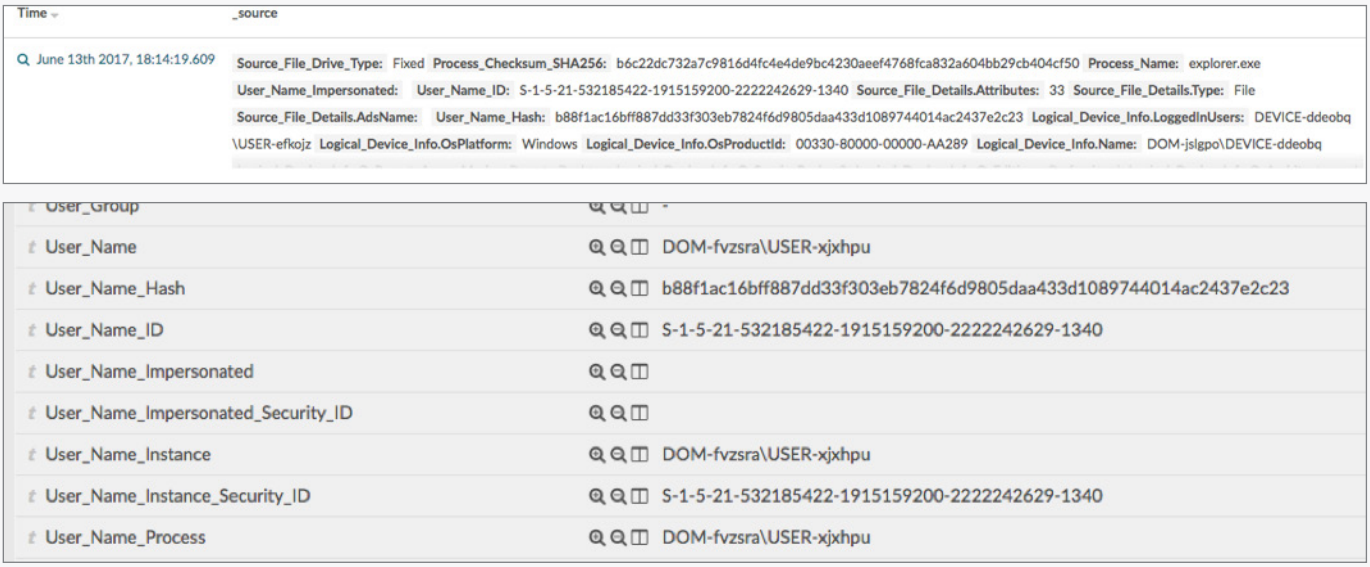
DATA SECURITY

Dtex's data can be sent to Dtex for analysis or exported into reports. Anonymization makes sure that even when your data is exported for external viewing, you're still keeping your employees' PII and your company information safe.

Data Anonymization in Dtex

Name	Status	Last Checked In	Operating System	
DOM-jslgpo\DEVICE-lsnvug	✓ Online	2017-06-13, 18:15:37	Windows 10 Enterprise	1 1
DOM-jslgpo\DEVICE-jiohuq	✓ Online	2017-06-13, 18:15:36	Windows 10 Enterprise	1 1
DOM-jslgpo\DEVICE-dqscrm	✓ Online	2017-06-13, 18:15:36	Windows 10 Enterprise	1 1

This is anonymization in action. The above screenshot depicts the Dtex endpoints page, where all the device names –including the domain names – are anonymized. Data Fields, including username, domain name and device name, are anonymized, and are stored as anonymized data in the Dtex big data platform as soon as they are received by the Dtex server. This ensures that all the anonymized data always shows anonymized in the Dtex UI irrespective of the Dtex UI screen. The anonymization feature is configurable and optional.



Time	_source
June 13th 2017, 18:14:19.609	Source_File_Drive_Type: Fixed Process_Checksum_SHA256: b6c22dc732a7c9816d4fc4e4de9bc4230aeef4768fca832a604bb29cb404cf50 Process_Name: explorer.exe User_Name_Impersonated: User_Name_ID: S-1-5-21-532185422-1915159200-2222242629-1340 Source_File_Details.Attributes: 33 Source_File_Details.Type: File Source_File_Details.AdsName: User_Name_Hash: b88f1ac16bff887dd33f303eb7824f6d9805daa433d1089744014ac2437e2c23 Logical_Device_Info.LoggedInUsers: DEVICE-ddeobq \USER-efkojz Logical_Device_Info.OsPlatform: Windows Logical_Device_Info.OsProductId: 00330-80000-00000-AA289 Logical_Device_Info.Name: DOM-jslgpo\DEVICE-ddeobq

User_Group	-
User_Name	DOM-fvzsra\USER-xjxhpu
User_Name_Hash	b88f1ac16bff887dd33f303eb7824f6d9805daa433d1089744014ac2437e2c23
User_Name_ID	S-1-5-21-532185422-1915159200-2222242629-1340
User_Name_Impersonated	
User_Name_Impersonated_Security_ID	
User_Name_Instance	DOM-fvzsra\USER-xjxhpu
User_Name_Instance_Security_ID	S-1-5-21-532185422-1915159200-2222242629-1340
User_Name_Process	DOM-fvzsra\USER-xjxhpu

As can be seen in the above screenshots, the PII data is displayed in the anonymized form when analysts are hunting for specific activities on the Dtex discover page. All anonymized fields are given a prefix, like “DOM” or “USER,” followed by the anonymized value to indicate the type of the field that was anonymized. This prefix enables analysts to easily identify and hunt for specific types of data fields without compromising privacy.

De-Anonymization

Dtex’s anonymization can be unlocked, but only by a very few select, privileged users.

During the initial configuration of the anonymization feature, server administrators – or other authorized personnel who have the authority to act on security violations – can set their own anonymization keys and store them in a safe place.

To de-anonymize the data, authorized individuals would need to provide their specific anonymization keys in addition to their login credentials. Every instance of de-anonymization will be logged in Dtex. This way, there is always a trail of who has de-anonymized data.

Generally, security analysts would perform alert triage and hunting to identify security breaches and the anonymized usernames associated with the breaches. The anonymized usernames would then be handed over to authorized individuals, who would de-anonymize the usernames in order to identify the real culprits.

With Dtex’s anonymization, enterprises can now more easily achieve regulatory compliance, protect their employee’s privacy, and maintain a secure, open workplace culture. Contact us today to see how Dtex can fit into your organization.

Get a User Threat Assessment

to see firsthand how Dtex maintains security & privacy in your organization.

E-mail: info@dtexsystems.com
Phone: +1 (408) 418 - 3786