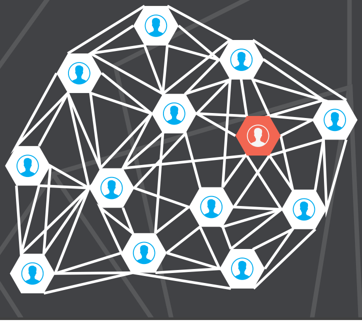
Next-Gen Endpoint DLP

Traditional endpoint DLP isn't working to stop enterprise-wide data exfiltration. Here's how Dtex is a more effective solution for protecting intellectual property and sensitive data.



DLP IS HEAVY

Huge agents bog down computers, choke networks, and require massive servers to deploy. Many companies report ripping out DLP after even small installations fail.

DLP LACKS VISIBILITY

What files were on a lost laptop? What data did a user take when they resigned? Or even something simple, like how many people try to use USB devices? DLP fails to answer even these basic questions.

DLP RULES ARE COMPLEX

Most organizations can't afford the large team it takes to configure and maintain the complex rules in an enterprise-wide DLP deployment. Instead, companies fall back to a few basic, intrusive rules (e.g. "block all USB devices" or "no usage of Facebook").

DLP IS UNFAIR

DLP penalizes everyone because of a few bad actors. DLP makes good employees less efficient and – if anything – encourages them to explore riskier ways of behavior.

DTEX IS LIGHT

Dtex generates 1MB per user per week with a 0.1% network impact. Users see no change or impact when it's installed.

DTEX PROVIDES FULL VISIBILITY

From the moment it's installed, you get real-time visibility into the files and data users touch, the applications they run, and the sites they use both on and off the corporate network.

DTEX MODELS HUMAN BEHAVIOR

Dtex is built on 15 years worth of data, which means it knows what behavior patterns indicate that a user is getting ready to steal data. Prediction is more effective than restriction.

TRUST BUT VERIFY

Companies that use Dtex move from "lock and block" to "trust but verify." Stop punishing the whole enterprise for a few bad actors.

DLP MISSES A LOT

In nearly every risk assessment we perform, we find DLP systems that are not performing as they should. DLP tells you what it catches, but has no way to identify and learn from data loss that it misses.

DLP VIOLATES PRIVACY

Since many DLP systems read the contents of files, emails, and websites, it captures personal and confidential data that companies really shouldn't possess. This invasion of privacy will damage employee morale – and all for very little benefit.

ENDPOINT DLP LEAVES GAPS

Endpoint DLP can be useful in small parts of the enterprise that directly handle high-risk or regulated data. But across an entire organization, even after all that effort, endpoint DLP still doesn't actually prevent employees from exfiltrating data. To use endpoint DLP properly is unmanageable – and improperly set up, it just isn't helpful.

DTEX SEES WHAT LOG FILES MISS

Dtex provides thorough enterprise-wide endpoint visibility that sees everything DLP and log files miss. If you're relying on log files to stop the insider threat, you're missing critical data.

DTEX RESPECTS PRIVACY

By anonymizing metadata, Dtex still finds bad actors without violating employee privacy. As a result, Dtex is compliant among even the strictest privacy laws in the world.

DTEX WORKS ✓

Dtex is lightweight, scalable, easy to manage, and – most importantly – it **works.** With true enterprise-wide visibility, you have no need for complex rules and heavy software. 15 years worth of analytics allow you to catch and stop the insider threat.

Take a Test Drive

With the tiny footprint and minimal network traffic, it is easy to test Dtex in your production environment with little risk of negatively impacting end users. We invite you to contact us for a trial period for up to 500 users to see the results Dtex provides risk free.

SANYO WILLIAMS MARTINI RACING vodafone ASTON MARTIN T··Mobile· MIZUHO Eni