PROTECT & RESPECT

7 Endpoint DLP Capabilities that Empower the Virtual Workforce

DTEX
WORKFORCE CYBER INTELLIGENCE™

For well over two decades, data loss prevention (DLP) solutions have been an integral component of the enterprise security framework to reduce organizational risk and protect sensitive digital assets.

First generation DLP solutions rely on complex content rules that require configuration and frequent maintenance, and lack the context and behavioral analysis to understand threats. These technologies monitor communication channels such as ports, protocols, storage locations, and applications and inspect the content of each individual file, email, web request, etc. and compare the content with the DLP content policies that are configured. Detection techniques are based upon keywords, keyword patterns, regular expressions, and hashing.

While this approach has been effective in identifying content that may contain sensitive data it lacks any key contextual data and behavioral analysis to truly be effective in understanding true data loss versus normal business activities.

Content detection technology triggers on every file and transaction with sensitive keywords and pattern matching rules which has the downside of creating incredibly high levels of false positives and alert fatigue. In many instances, data-centric events that are triggered create more questions than they answer: Is this legitimate business activity? Is this negligent or malicious behavior? Was the event triggered from a compromised system? Is this normal or abnormal behavior in the company, the department, the role or for the user? These key questions are critical to truly understanding the data loss events in an enterprise environment and are not answered with first generation DLP technologies.

First generation DLP solutions rely on complex content rules that require configuration and frequent maintenance, and lack the context and behavioral analysis to understand threats

More Questions than Answers

- ***Is this legitimate business activity?***
- ***Is this negligent or malicious behavior?***
- ***Was the event triggered from a compromised system?***
- ***Is this normal or abnormal behavior in the company, the department, the role or for the user?***

The data-centric approach with these first-generation solutions also comes at a huge cost for administrators, as configuration and investigation of rules and policies must be constantly tuned by IT and security staff to remain effective.

Analysts also have to rely on multiple 3rd party solutions (SIEMs, UEBA, Proxies, System logs, etc.) to stitch forensic data together to understand the full intent and context of each data loss incident. Another huge cost comes with DLP Endpoint agents. Traditionally these endpoint agents create a large footprint, require excessive CPU and have high bandwidth requirements.

Privacy concerns and regulations are another area of concern with data-centric DLP solutions. Opening up every file, email, IM, web request has created many issues with privacy regulations such as GDPR. Inspecting everyone and everything without probable cause has created blurry lines from a compliance perspective and has resulted in even more barriers for traditional content aware DLP technologies to do their job.

Behavioral Endpoint DLP: Supporting the Needs of the Virtual Workforce

The next evolution of Data Loss Protection must take a new and innovative approach to solving the needs of the modern enterprise and virtual workforce.

Human-Centric Behavioral Intelligence

The old DLP adage that it is all about the data is no longer sufficient. Next GEN DLP supports the virtual workforce by understanding the human behaviors associated with a potential data loss incident, without violating the trust and privacy of employees. The human behavior aspect is key to understanding intent and context around a true data loss incident. Profiling and baselining each user by role, department, and across the company provides a complete picture of where risk lies within an enterprise. A next generation DLP solution must be able to produce a full audit trail of behavioral activity and understand the "who, what, when, why and how" of a possible data loss incident with a real-time, scoring-based audit trail of all events.

Adaptive Analytics

Unlike first generation DLP, a virtual workforce solution is all about gaining context and intent to fully understand and quickly triage data loss events. Using adaptive analytics that baseline normal user behavior and alert on deviation, artificial intelligence, and real-world-tested threat patterns is key to accurately detecting truly malicious and negligent behavior from normal business activity.

Complete and Continuous Visibility

DLP relies on rules to determine what it sees or doesn't see. A behavioral intelligence architecture and design should not require "rules & triggers" to determine when meta-data should be collected. Continuous capture and monitoring across the enterprise for both endpoint and server systems, both on and off the network, is critical. Analysts must be able to go back in time for forensic investigations or to analyze historical behavior for new patterns.

File Lineage Audit Trail

A full audit history and single pane of glass detailing file activity is paramount to building out the severity and understanding 'indicators of intent' of a data loss event. Not only file movement but a full audit trail of who and when each file is created, modified, aggregated, obfuscated, archived, encrypted and deleted. These added attributes provide a clear distinction between normal activity and true data loss events.

Sensitive Data Profiling

Profiling data with a content-based approach using keywords, patterns, and regular expressions create an abundance of false positives which has limited the effectiveness of traditional DLP solutions. Sensitive data profiles and analytics addresses this by inferring sensitivity based upon file lineage, file location, creation, user role, file types and many additional file attributes. Correlated with a user behavior profiles, as well as leading data classification tools, this technology can detect the potential loss of sensitive and suspicious data without the need of content aware rules. This dramatically decreases false positive events and the time needed for administrators to constantly tune rules and policies and an analyst time to investigate data loss alerts.

Employee Privacy Compliant

A modern DLP and Workforce Cyber Intelligence platform must deliver holistic, real-time awareness about the workforce's activities without invading personal privacy. Employee Privacy and regulatory privacy regulations such as GDPR require a balanced and proportional approach to the monitoring of activity vs the protection of customer data. A modern approach must capture meta data of activity and should not inspect and present content of sensitive files. Data such as PII, CCNs, and emails should never be exposed.

Lightweight and Enterprise Scalability

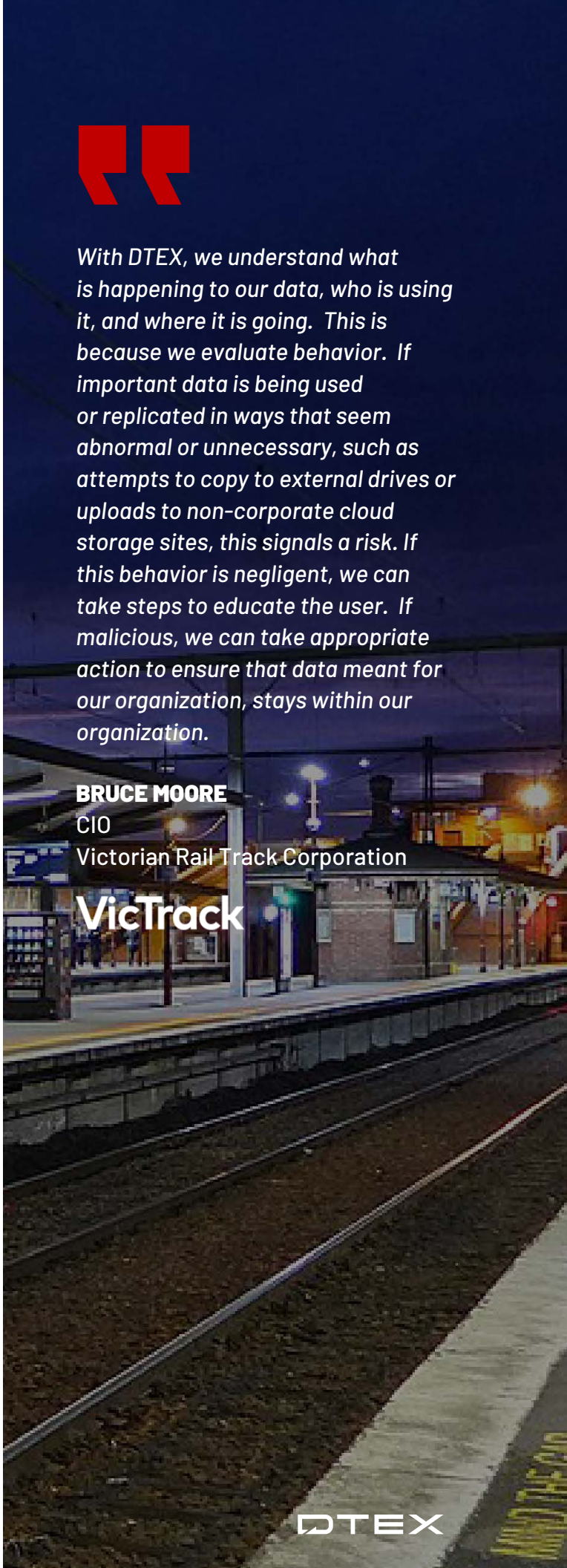
A cloud first solution that is scalable to millions of devices and the ability to quickly and efficiently deploy across the enterprise is a must. In the age of agent fatigue and limited resources, the solution must be extremely lightweight from both a CPU and bandwidth perspective and be able to scale to the needs of small and large organizations alike.

Data Loss and IP Exfiltration Protection for the Modern Enterprise

Data Loss Prevention from DTEX takes a behavioral approach to data loss by monitoring and auditing all user activities based upon "out of the box" behavior indicators. Using this method, DTEX InTERCEPT is able to see the full lifecycle of behavior activity and understand the who, what, when and how of a possible data loss incident. No false positives, simply a real-time, scoring-based audit trail of all events.

Unlike heavy Endpoint DLP tools, DTEX InTERCEPT is a lightweight forwarder that requires no more than 3-5MB of bandwidth per day per endpoint and utilizes less than 1% CPU. With DTEX InTERCEPT, processing of DLP policies is not performed on the endpoint. Instead, all data is streamed in real-time to the cloud for analysis and detection, thereby avoiding many of the endpoint interoperability issues associated with traditional endpoint agents.

DTEX InTERCEPT's modern architecture and design does not require "triggers" to determine when meta-data should be collected and supports continuous monitoring of all console and web-based applications. Likewise, DTEX's innovative human-centric scoring mechanism is based upon a series of activities, vs DLP's rule-based trigger, which means DTEX only notifies on truly suspicious events, saving time and empowering the analyst with full context about any given incident.



With DTEX, we understand what is happening to our data, who is using it, and where it is going. This is because we evaluate behavior. If important data is being used or replicated in ways that seem abnormal or unnecessary, such as attempts to copy to external drives or uploads to non-corporate cloud storage sites, this signals a risk. If this behavior is negligent, we can take steps to educate the user. If malicious, we can take appropriate action to ensure that data meant for our organization, stays within our organization.

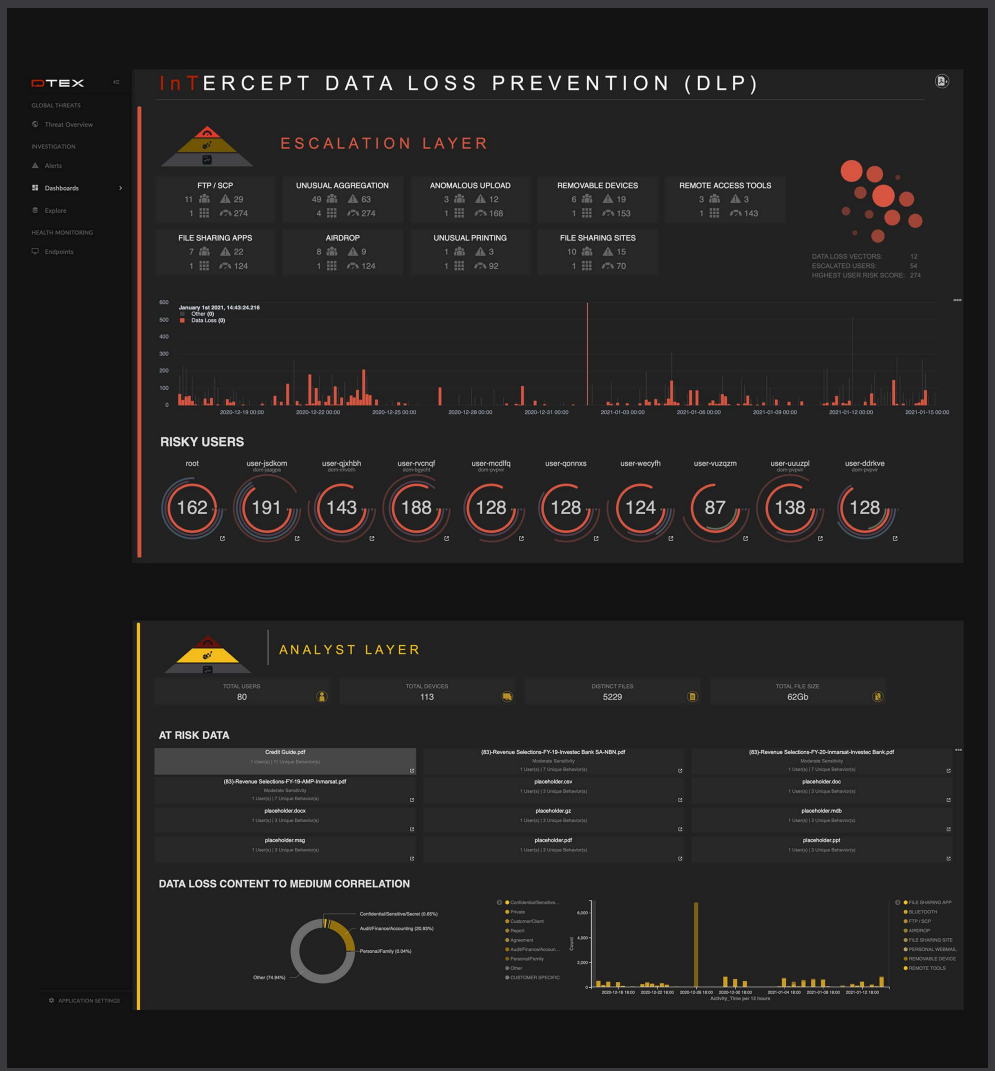
BRUCE MOORE
CIO
Victorian Rail Track Corporation

VicTrack

DTEX InTERCEPT's behavior-based anomaly detection technology baselines user/device activity and can compare suspicious events based upon anomalies for the individual user, the department, and the organization as a whole. As an example, a user in the IT department may need to use certain tools that someone in the sales department would not. DTEX automatically baselines these activities by peer group to understand what is normal and what is abnormal or suspicious.

To learn more about DTEX's modern approach to Endpoint Data Loss Protection, visit dtexsystems.com/data-loss-prevention.

DTEX InTERCEPT provides an all-in-one, interactive Data Loss Prevention dashboard with dynamic, drill-down capabilities that allow analysts to quickly investigate synthesized alert sequences, understand file lineage and what user behaviors indicate malicious intent and/or potential compromise by external attacker.



About DTEX

We are the leading experts in Workforce Cyber Intelligence.

DTEX Systems is the world leader in Workforce Cyber Intelligence and committed to helping enterprises run safer and smarter by providing context-rich user behavior and asset utilization analytics that deliver a first-of-its-kind human-centric approach to enterprise operational intelligence. Hundreds of the world's largest enterprises, governments and forward-thinking organizations leverage DTEX to prevent insider threats, stop data loss, maximize software investments and deployments, optimize workforce productivity, and protect remote workers. DTEX has offices in San Jose, California and Adelaide, South Australia and is backed by Northgate Capital, Norwest Venture Partners, Wing Ventures, and Four Rivers Group. Visit: www.dtexsystems.com.