A BIG DATA SOLUTION TO ADVANCED PERSISTENT THREATS

Cybersecurity Requires Real-Time Monitoring and Long-Term Analytics

82%

of breaches happen in minutes[1]

18

Minutes for state-sponsored attacks to completely compromise the network[2]

9

Months on average to detect and contain a breach, some go undetected for years[3]

Government systems and data are increasingly under attack. State-sponsored actors leverage an ever-expanding range of sophisticated cyber exploits, including Advanced Persistent Threat (APT) campaigns to steal sensitive data, conduct covert surveillance, and interrupt vital services. To combat these threats, new federal mandates to adopt Zero Trust Architecture are shifting the focus from securing the network perimeter to a holistic approach assuming that no person or thing should be trusted, inside or outside of the network—identities, applications, workloads, and data.

But the central core of Zero Trust is data. Agencies that have visibility into all of their data and related activity increase positive threat detection and remediation outcomes in case of a breach.

To secure operations, government agencies need to shift reliance from a patchwork of disparate point solutions, with inherent management, data, and analytics constraints and adopt an enterprise data solution that provides the means to query massive long context data sets and identify threats before they become active in the network and across cloud environments. With machine learning and advanced analytics, combined with a security platform and a single pane of glass, agencies increase threat visibility across legacy, hybrid, and multi-cloud environments, all while retaining the ability to both deploy packaged applications and build custom solutions specific to agency needs.

APTs in Focus

APTs present an especially high-risk category of cyber incursion for government systems. In this prolonged and targeted form of attack, bad actors sniff out vulnerabilities (zero-day, spear-phishing, or other social engineering techniques), and insert malware that may lie dormant and undetected in the system for months or years. In recent years, intrusion sets including APT28, 29, 30, 32, and many others attributed to State actors contained sophisticated attack malware targeting Federal classified information, industrial intellectual property, and the vast wealth of personally identifiable citizen data that resides in government hands.

Enterprise Scale Data Logging
CDP can ingest multiple terabytes of data per day, in real-time, and efficiently and scalably analyze and continuously monitor petabytes of recent and historical data.

Why Cloudera

Cloudera Data Platform enables organizations to effectively execute their data and analytics strategy to address current and evolving customer expectations.

EDGE TO AI ANALYTICS
Analytics for the complete data lifecycle combined in a single platform, eliminating the need for costly and cumbersome point products.

DATA SECURITY & COMPLIANCE
Maintains consistent data security and governance across all environments.

HYBRID AND MULTI-CLOUD
Delivers the same data management capabilities across all clouds and data centers.

100% OPEN SOURCE
Open compute and open storage ensures zero vendor lock-in and maximum interoperability.

Government agencies that rely solely on conventional SIEM (security information and event management) applications are especially at risk. Resource-constrained agencies typically lack the human capital to tackle the APT threat, and while SIEM is generally adept at real-time threat detection, they generally lack the resources to ingest data feeds at scale or correlate present-day data against historical, long context data in disparate environments—required to identify anomalies and contain malware. As traditional SIEM-based ecosystems struggle to leverage advanced analytics in order to discover such sophisticated threats, agencies are hard-pressed to identify potential vulnerabilities until it is too late.

Mitigating Risk in Hybrid Cloud Environments

As government agencies migrate workloads to the cloud, the benefits of hybrid cloud environments are proving indispensable. Hybrid cloud offers the flexibility of deployment options, the ability to scale computing resources, the huge advantages of cloud innovation, as well as the ability to store and share data and applications across public and private cloud and legacy infrastructure. Additionally, this diversity of compute/storage environments can mitigate cybersecurity risks by separating mission-critical data.

YOU CAN'T DETECT WHAT YOU CAN'T SEE

When SUNBURST (APT29) was detected in December 2020, it's believed the attack began as early as Spring 2020.

To investigate and mitigate a breach, agencies must leverage big data to query and analyze massive sets of data over long periods of time.

Cloudera Data Platform is a simple, effective solution that marries real-time threat detection with massive, long-term data storage, powered by sophisticated Artificial Intelligence and machine learning.

While this measured approach reduces the risk of intrusion between non-homogenous environments (for example, retaining recent, critical, or sensitive data on-premises while less sensitive data and workloads are run in a scalable, cost-effective public cloud), securing data in a hybrid cloud is much more complex. Do you know what data you have? Do you know who is accessing it? And can you control and manage it?

Cybersecurity architecture must be applied holistically across disparate cloud and on-premise environments and scale with them, equally distributing an organization's attack surface while maintaining command and control, delivering visibility into all data, actionable insights in context, and rapid threat detection and remediation. All virtually impossible with ad-hoc manual processes, incomplete data, and an assortment of point solutions.

Cloudera Data Platform for Threat Detection

Cloudera Data Platform (CDP) presents a big data approach to combating APTs. With a suite of high-end capabilities available across cloud environments, CDP makes available a common workbench where analysts can gain insight into both real-time and historic data, supported by machine learning and artificial intelligence. CDP can ingest telemetry data from a range of sources including both legacy and hybrid cloud applications, as well as the growing variety of edge data sources, and apply centralized data security, governance, and control.

By storing logs over the long term (many months)—literally, billions of rows of transactions and petabytes of storage—Cloudera is able to leverage machine learning to detect anomalies (failed login attempts, unusual resource utilization, increased network traffic from a specific host, or execution of unknown processes) common to APTs. This shifts cybersecurity from

About Cloudera
At Cloudera, we believe that data can make what is impossible today, possible tomorrow. We empower people to transform complex data into clear and actionable insights. Cloudera delivers an enterprise data cloud for any data, anywhere, from the Edge to AI. Powered by the relentless innovation of the open source community, Cloudera advances digital transformation for the world's largest enterprises.

Learn more at cloudera.com

reactive to proactive mode, enabling analysts to better identify APTs before bad actors can exploit them.

CDP puts big data to work as a critical tool for threat hunting in the fight against APTs, delivering a vital cybersecurity backbone for government agencies. There are three ways that CDP delivers direct benefits:

- **Built-in, enterprise-ready security, and governance with SDX (Shared Data Experience).** A feature of CDP, SDX gives agencies command and control over all of their data in a complete and easy-to-use solution—a single control pane to secure, govern, and track data lineage across disparate data locations.
- **Complete data lifecycle management.** Cybersecurity risk is rooted in a lack of visibility: If you can't detect it, you can't monitor or mitigate it. CDP gives agencies complete data visibility to expedite detection, investigate and respond to APTs.
- **Open data standards, cloud portability, data independence.** CDP is an open-source solution that frees government agencies from vendor lock-in and proprietary formats and technologies.

Conclusion

When even the largest, most sophisticated organizations struggle to keep up with the cyber-threats, CDP offers government agencies a platform-based approach that enhances cyber-readiness for APT detection, disposition, and remediation. CDP ingests and monitors data from all relevant sources, provides advanced analytics and machine learning on large disparate data sets to detect anomalous activity, and provides enriched recommendations to the SOC to mitigate impacts from APTs.

Unlike conventional SIEM solutions, with CDP, agencies acquire end-to-end visibility and control of their data, horizontal scaling architecture, and an open approach that ensures long-term flexibility to adapt to the constantly changing threats to data sources and network connections.

Learn how Cloudera enables government agencies to take control of their data and combat cyber-threats at **cloudera.com/solutions/public-sector.**

Sources:

[1] arsTECHNICA, Blame the Victim: eport Shows Fifth of Breaches Caused by "Miscellaneous Errors", April 2016

[2] Forbes, Russian Bears Need Less Than 20 Minutes To Hack Your Data, February 2019

[3] IBM, How Much Does a Data Breach Cost?, 2021