Big Data for Security

A Dell Big Data White Paper

By Joey Jablonski

Big Data for Security

Big data has brought the ability to analyze large, complex, multisource data sets to many organizations that previously relied more on past experience and gut feelings to drive critical decisions. Particularly in the security realm, organizations are looking to big data to drive better visibility into events, actions, intrusions and behaviors than previously possible. Big data enables organizations to be more proactive in responding to threats, as well as more readily able as an organization to evolve and react to new threats to data assets or connected devices and applications.

Effective security in an organization – that is protecting data assets from compromise and misuse – is about effective layers in the security environment. These layers commonly include protections like patches, firewalls and VPNs, alerts through monitoring systems, and educating teams to avoid activities that are high-risk and unnecessary for the company to conduct business. Overarching all these layers is a process for responding to threats and intrusions and continually tweaking the systems in place to prevent future intrusions. Big data enables organizations to simultaneously monitor more data points, and better detail about activities to pinpoint unexpected patterns, as well as investigate events in more detail to prevent them from occurring in the future.

There are a multitude of ways that big data can be used to proactively monitor behavior and identify security threats to an organization. Some example projects proving successful for organizations include:

- ***Network Traffic Monitoring*** – The ability to ingest complete network traffic over long periods of time, from many devices, enables organizations to quickly identify anomalies in traffic patterns, as well as to investigate security breaches in greater detail than ever before.
- ***Insider Threat Identification*** – As more and more organizations begin to look inward for possible threats, proactive identification of rogue employees and contractors has become critical. By leveraging big data technologies, organizations can combine a multitude of information from access logs, to job descriptions and HR reviews to identify staff that are high risk for theft or compromise to organizational and customer data.
- ***BYOD Device Usage*** – With the proliferation of bring-your-own-device models within organizations, IT departments have had to change the way they monitor which locations contain proprietary company data, and then put controls in place to take appropriate actions to protect it.
- ***Job-Based Behavioral Correlation*** – Many organizations have created profiles to enable access to data with access tools based on job descriptions and levels within an organization. Many times these are static policies with little to no monitoring to ensure compliance as organizational changes and staff job changes occur, putting the organization at risk for data loss due to rogue players. Big data enables seamless monitoring of not only policies, but how they are being tested by staff, used and executed by staff.
- ***IP Protection*** - Many organizations have created, and must protect, intellectual property (IP) that is responsible for a competitive edge in their respective markets. This IP can cost a large amount of capital to research, create and protect. Big data can enable organizations to monitor both internal and external publications for occurrences where IP is used improperly.

The technology platforms supporting businesses today are more complex then ever. As staff moves from roles, locations and projects, the external threats to companies continue to multiply. Big data provides a mechanism for companies to proactively monitor a variety of data sources, building predictive models about expected behavior, while alerting security response teams when behavior falls outside the expected patterns. This is compounded by user behaviors that change as they evolve between projects and schedules. By leveraging modern big data platforms, companies can leverage this wealth of information created to more successfully identify and prevent threats, investigate intrusions and identify high-risk staff.

To learn more

To learn more about Dell big data solutions, contact your Dell representative or visit:
www.dell.com/bigdata
www.DellBigData.com