White Paper

Real-Time Data-Centric Visibility for Breach Detection and Investigation

HoloNet Delivers the First
Real-time Data-Centric Audit and Protection Solution
For Breach Detection and Investigation

The Challenge: Siloed-Views of Data in Motion

Data breaches that have resulted in the exposure and theft of millions of personal, corporate and government records and files have become a hot topic recently due to the growing frequency of high-profile cases. Strange as it may seem, there is not a single product in the market that was purposely designed to address the need for real-time visibility and detection of breaches that involve sensitive business data in motion.

Data Loss Prevention (DLP), Cloud Access Security Broker (CASB), End-point Detection and Response (EDR), and Firewall (FW) products ***each provide only a partial and isolated view of how sensitive data is being moved*** inside a corporate network or to the cloud. But none of them present a complete view of how sensitive data is being moved in real time, by whom, using which applications and devices.

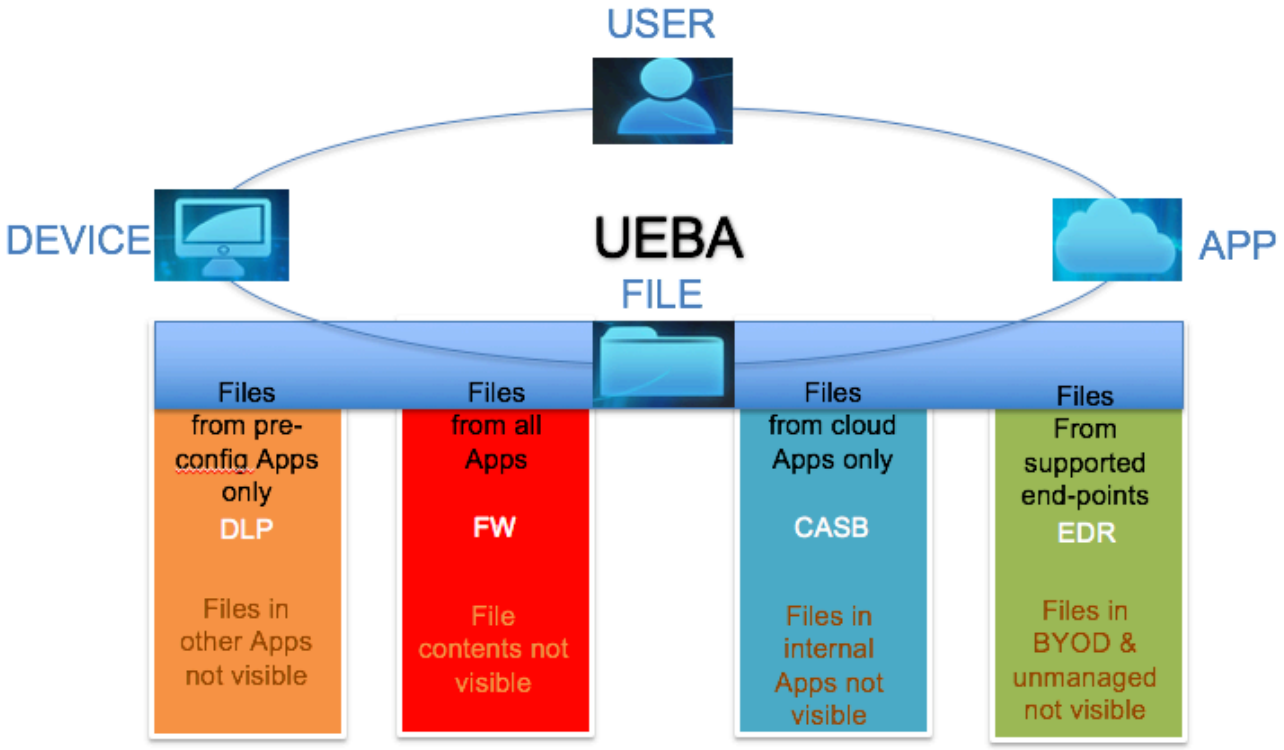

Fig. 1 Existing security products provide only partial and isolated views of sensitive data in motion

Take unstructured data (files) being transferred across the corporate network as an example. Many organizations have deployed multiple instances of DLP CASB, EDR and FW products, but not even one of these provides a holistic view of all moving data and its relationship with actual users in real-time.

- DLP products can see files transferring to and from the applications that are pre-configured through policy settings. However, for the ***applications that are not configured or supported by DLP*** (such as hundreds and thousands of SaaS applications) files embedded in those non-supported applications are completely ignored.

- CASB products can track files going to and from SaaS applications, but cannot see ***files moving to and from internal servers or applications***.

- EDR products can see everything on each individual device that is controlled by the enterprise IT department, but can't view ***BYO or unmanaged devices*** (no vendor can support all versions of all operating systems). EDR also lacks a ***global view*** of all files moving across networks (the same file may be accessed by multiple users from multiple servers/services in different but correlated timelines).

- A firewall can monitor all files going through the security perimeter, but it has *absolutely* ***no awareness of what data in those files is sensitive***, and what data is not.

While each of these products has its limitations, viewing files alone doesn't provide the critical information necessary to conduct meaningful security incident investigations. In these situations, what matters most is the visibility of ***the relationship between the file movement, the actual user and the user's device.***

Only when specific data is linked to a user, and the inherent relationships among the four security vectors (user, data, application and device) are fully revealed and profiled, can behavior-based anomaly detection be precise, and with an absolute minimum of false positives. The HoloNet OnFire data-centric audit and protection (DCAP)platform was designed and built from the ground up to meet this unique challenge.

What Compelling Problem Can HoloNet Solve?

The alleged data theft by ex-Google employees in the Waymo v. Uber lawsuit is a perfect use case that highlights the unique ability of HoloNet's data-centric visibility and anomaly detection solution to detect and prevent unauthorized data exfiltration. According to reports, the data leakage occurred over a four-week period and more than 14,000 documents were copied illegally.

Had the HoloNet OnFire solution been deployed, real-time alerts would have been sent out automatically to security staff, as the number of files copied clearly represented a high watermark when compared to the user's baseline pattern. Thus alerted, the security team would have been able to respond and prevent further data exfiltration.

By discovering the hidden relationship between moving data and its actual user through our patent-pending Network Hologram technology, the HoloNet OnFire solution can re-construct the relationship among four key security vectors: user, data, application and device, automatically

connecting every data movement with its actual user, device, and associated application in real-time. This unique relation-based data-centric visibility can help security teams answer the following four fundamental questions immediately, and avoid a lengthy manual process assembling logs through a SIEM platform.

1. What data has been compromised?
2. Who was the user?
3. What device was used?
4. From where?

By providing precise answers to these critical questions in real-time, HoloNet can support the post-breach investigation in ways that no other product can. As a security investigator, you'll have "suspects" instantly identified. Highly granular and constant visibility of each user and his/her associated sensitive business data provides a solid foundation for user behavior analytics, delivering unmatched anomaly detection accuracy when compared to network-based approaches.

Network-based solutions may detect anomalous patterns from the activities at network or application layers, but have no way to distinguish if that indicates the improper movement of sensitive data without the intelligence of the relationship between the sensitive data and their users.

If we compare data traffic to actual road traffic, imagine that sensitive data is "gold" being transported by certain vehicles on a highway. Any vehicle's driving pattern may change whether it is carrying gold or not. If the security system is simply tracking changes in all driver behavior, that will lead to too many false positives. The challenge is to be able to identify which vehicles are carrying gold and who are the drivers.

HoloNet OnFire outperforms network security solutions by showing which vehicles are carrying gold, who the drivers are and where they're going. By establishing precise profiling, and focusing on the vehicles carrying gold (i.e., sensitive data), the HoloNet solution effectively eliminates virtually all false positives based on changes in driving behavior.

What Security Operations Gaps Can HoloNet Fill?

A data breach can be simply defined as the unauthorized access of sensitive or confidential data. Data access through a network represents a movement of data from one device (physical or virtual) in one part of the network to another device, typically in a different part of the network. Consider another analogy: that of the elephant and the blind men. The movement of sensitive data is like the elephant and existing data security products (DLP CASB, EDR and FW) can be compared to the group of blind men. Each man touches a part of the elephant, but can only describe his limited, isolated experience. None of the men can tell the complete story and describe the elephant in its entirety because no one has a top-down, holistic view.

Complete visibility of how sensitive data is being moved is the foundation for any meaningful data breach detection – you can't protect what you can't see. HoloNet's ***OnFire solution eliminates isolated siloes and fills this holistic visibility gap*** through its patent-pending technology. This instant top-down visibility is the essential ***first step for any data-related security incident investigation***.

HoloNet's relation-based visibility can also ***complement and enhance your existing security technologies,*** thus providing new capabilities as well as protecting your existing security infrastructure investments***.***

- Accelerate and reduce the investigation time by feeding "stateful" logs to **SIEM** products (e.g., Splunk) – OnFire automatically builds the relationship between moving data and its user in real-time for every piece of data flowing through a corporate network. The stateful logs created by OnFire provide immediate visibility linking four key vectors – user, data, application, and device, eliminating the need to write complicated SIEM-based scripts or applications to manually re-create this critical relationship, which can ***save weeks or months of investigation time***.

- Turn a **DLP** product into an "intelligent data firewall" – Significant configuration and fine-tuning must be done upfront in order to use a DLP product. However, without having complete visibility into how sensitive data is being moved in real-time, using which devices and applications, and by whom, DLP can only work blindly to block some data transfers while completely ignoring others that are high risk. By using HoloNet's relation-based visibility and anomaly detection focused on sensitive data, IT teams can dynamically tune DLP policies to protect sensitive business data while minimizing the impact to normal business communications and operations.

- Amplify the value of a **FW** – Most enterprises have already invested in firewall sandbox technology, which can identify various malicious files being transferred through the corporate FW. While a sandbox may be able to identify the current device that sends or receives a malicious file, it won't be able to tell the security team whether the exact same file has been accessed by other devices or servers across the corporate network. HoloNet can instantly bring comprehensive relation-based visibility to the security team to facilitate a complete clean up and eliminate all potential risks from this single file. This extends the capabilities of a FW beyond that of a point solution.

- Complement an **EDR** product to complete the data security solution – While an EDR product provides very detailed visibility for each individual device, it lacks a global view of how sensitive data is flowing across a corporate network, either accessing internal servers or cloud services. EDR also lacks visibility into devices not supported by corporate IT, such as BYO, unmanaged and IoT devices. By feeding EDR logs to HoloNet OnFire, enterprise customers achieve full visibility into how sensitive data is flowing inside the corporate and off-campus network, regardless of where employees are located.

Use Case: Compromise of an End-Point Computer

To better understand how OnFire excels at detecting malicious breaches, and what distinguishes it from existing solutions, let's examine a realistic business scenario: The CFO's laptop has been compromised by a hacker, who then tries to use the computer to steal confidential data files from inside the company network.

In a conventional security environment, the IT team has no good solution for detecting a compromised machine until the damage is done. Network-based anomaly detection solutions may be able to see suspicious activity on the network, but will likely generate too many false positives and impede the IT team's ability to respond.

For an IT team using the HoloNet solution, OnFire will have already profiled the CFO's laptop. Through a built-in content inspection engine, OnFire identifies the types of sensitive files the CFO typically moves, and from where – for example, financial statements from the main finance department server. OnFire links all data movements with the actual user – the CFO – and her device in real-time, and profiles that behavior accordingly. After a brief learning period, OnFire will have built a base pattern for the CFO's movement of data using her laptop device.

When the hacker gets control of her laptop, he attempts to access source code from a completely different server in a different department. This is clearly outside the CFO's normal pattern of behavior. OnFire instantly detects the abnormal behavior and alerts the CFO and the security team, enabling immediate response to the incident.

About HoloNet Security - HoloNet has ingeniously combined the best of UEBA, CASB and DLP technologies to create a revolutionary platform that delivers real-time breach detection and remediation in a single, powerful solution. By connecting every piece of moving data with its user, application, and device in real-time, HoloNet OnFire provides unmatched visibility and protection for sensitive and regulated business data.

.

HoloNet Security - 1294 Kifer Road, Suite 710, Sunnyvale, CA 94086
www.holonetsecurity.com | +1-408-940-0225