Gigamon® datiphy™

Joint Solution Brief

Collect Traffic and Identify the Greatest Threats to Your Databases

The Challenge

Enterprise IT and security professionals strive to protect their business-critical information from threats, but breach detection is often severely delayed due to limited visibility of their network and data activities.

Integrated Solution

Enterprise distributed networks can be enhanced by combining Gigamon's pervasive network visibility and the Datiphy user and data behavior analytics solution to protect business-critical data.

Traditional methods of monitoring north-south network traffic lack insight into lateral (east-west) movement of data causing a significant security gap. Gigamon extends the coverage of your network security monitoring capabilities by enabling greater visibility to sensitive data activities.

Datiphy consumes the targeted data provided by Gigamon and produces risk metrics and threat analysis. It also evaluates the potential of data breaches against the compromised data repositories.

Key Benefits

- Extract traffic of interest in complex data environments and filter down to specific database traffic
- Decrypt SSL/TLS traffic to discover obscured malicious activities
- Audit all data activities for security incidents and regulatory purposes
- Actionable real-time user and data behavorial analysis
- Discover latest threats such as SQL injections, privilege issues, and insider threats
- Correlate sensitive data access to all relevant applications and users

Introduction

Databases are the de-facto data repositories for all transactions within an organization. Data is consumed by end-users, internal and external applications, cloud applications, and even by other databases. The access permissions are given to end-users, application users, and privileged users. Control of data movement and utilization can be highly complex, sensitive and disruptive to management. Hackers take advantage of that lack of oversight in order to perform privilege escalations, data exfiltration, and data manipulation.

The biggest problem enterprises face trying to secure their business critical data is lack of visibility followed by lack of actionable threat intelligence.

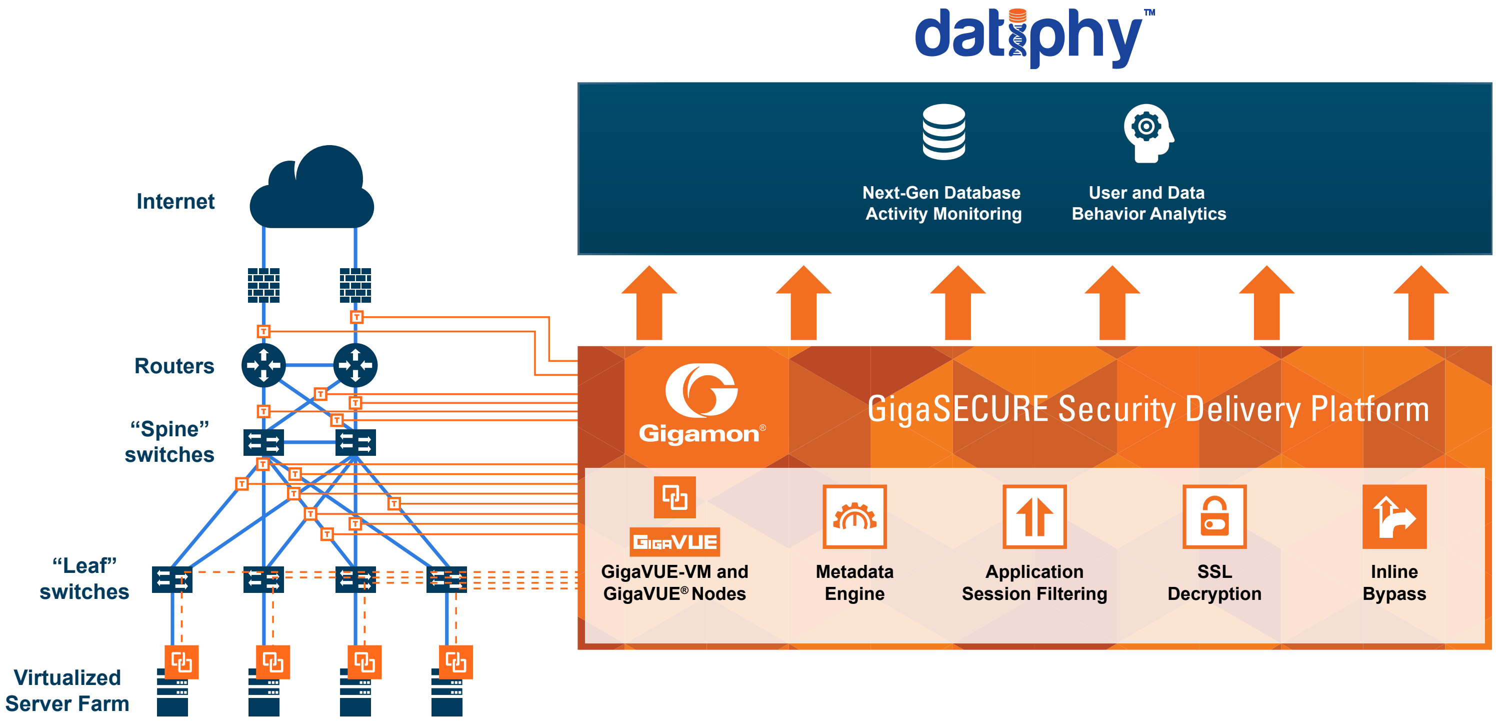
The Gigamon and Datiphy Joint Solution

Gigamon dissects the complex network traffic into comprehensible components for fast consumption by the Datiphy correlation engine. Gigamon's GigaSECURE® Security Delivery Platform provides an efficient and scalable architectural approach to network visibility that can support various deployment options, providing a broad view of physical and virtual networks.

Combining the Datiphy data-centric security and user behavior analytic solution and the GigaSECURE Security Delivery Platform provides a true enterprise-grade data security platform. The combined solution gives deep-dive forensic capabilities for end-to-end protection.

The Datiphy behavior-based data activity monitoring solution allows information security organizations to detect breaches as they unfold. With Gigamon providing the complete visibility to traffic comprised of the front-end HTTP session and back-end data transaction, Datiphy can provide a complete look into the data activities traversing your environment. Changes in behavior, malicious or otherwise, are detectable early with forensics data trails to track down and mitigate data theft.

By deploying Datiphy on an out-of-band port on the GigaSECURE platform, the joint solution is able to process billions of data transactions. Furthermore, the scalable platform covers nearly all relational database protocols and continually adds new unstructured data models. Datiphy provides end-to-end visibility with real time user mapping to reveal true user identities.


datiphy™
Next-Gen Database Activity Monitoring
User and Data Behavior Analytics
Internet
Routers
"Spine" switches
"Leaf" switches
Virtualized Server Farm
Gigamon®
GigaSECURE Security Delivery Platform
GigaVUE
GigaVUE-VM and GigaVUE® Nodes
Metadata Engine
Application Session Filtering
SSL Decryption
Inline Bypass

Two primary network capture points are: (1) in front of the front-end web services and (2) between the application and database servers. Gigamon TAPs are the optimal, least intrusive mechanism to capture the relevant traffic. Through advanced packet filtering, the GigaSECURE Security Delivery Platform can then forward only the HTTP and database (SQL and NoSQL) traffic to Datiphy for deeper analysis. Encrypted HTTPS traffic can be decoded by the GigaSECURE platform and then forwarded to Datiphy for deeper transaction and behavioral analysis. When a suspicious event takes place, Datiphy can notify the end-user to take action by, for example, blocking a live connection.

Learn More

For more information on the Datiphy Enterprise and Gigamon solution, contact:

datiphy™

www.datiphy.com

Gigamon®

www.gigamon.com