

DATA SHEET

Forensic Investigation

Hunting down the source of your data leak

The Trellix Guardians Forensic Investigation framework is based on an eight-step process:

1. Determination of investigation scope and authority.
2. Creation of investigative plan.
3. Deliver Attorney-Client/Counsel services
4. Interview of staff.
5. Forensic acquisition of electronic data.
6. Strict chain-of-custody management
7. Forensic analysis of acquired data.
8. Forensic reporting and recommendation.
9. Testimony, if required.

Scope

A typical engagement ranges from one to four weeks, depending on the scope of the investigation. Investigations with a large number of devices may require more time. During the investigation, we collaborate closely with your security team, IT, human resources, and legal and compliance teams. A comprehensive report of our findings will be provided to you at the end of the engagement.

Your security team has the discipline to ensure your Incident Response (IR) plan is current. Twice each year you create security breach test scenarios to keep the team focused and sharp. You are confident you can handle nearly any situation. Then it happens. Information from a strictly confidential internal document shows up on a web blog. Your initial investigation reveals there were only six members of the senior leadership team that had access to the document. Now you must determine how the information in the document leaked out of your organization.

The Trellix Guardians Forensic Investigation Team—part of product and services offering—is ready to provide you the special investigative skills needed to hunt down electronic data. Staffed with some of the best and most experienced forensic talent in the business, we respond immediately and help you through your crisis. Our consultants provide the investigative expertise and tools to answer your data-breach questions.

Methodology

Guardians proven forensic methodology is compliant, consistent, focused, and confidential. We stay informed of the latest legal rulings, rules of evidence handling, and industry best practices. We use proven tools and test them often. Our forensic methodology is highly refined and constantly improving, providing you consistent results in every engagement. By keeping investigations focused and specific, we also save you time and money. And above all, we maintain strict confidentiality in our forensic engagements.

Contact us at Guardians@Trellix.com. For more information