Trustwave®
SpiderLabs®

Proactive Breach Detection Services

DISCOVER DATA COMPROMISE AND MITIGATE QUICKLY

Most Victims Don't Detect a Breach

Even the most sophisticated enterprises can and do fall victim to determined attackers – often without them even realizing it.

Trustwave SpiderLabs' investigations of more than 2,000 data breaches show that the majority of businesses are unable to identify a breach. In only 29 percent of the compromises we investigated in 2013 did the victim themselves identify the break-in. Seventy-one percent of the time, a third-party – such as law enforcement, a regulatory body or even a member of the public – made the initial discovery.

Given these statistics, you already should be asking yourself whether your organization has been breached. Your CEO or executive board certainly wants to know the answer.

Remember, the amount of time that elapses between an intrusion and its discovery correlates directly with the impact of that breach. The longer an attacker resides undetected on your systems, the longer they have to take-over additional systems and siphon sensitive data. The sooner you can identify a potential breach, the sooner you can act to limit its repercussions, which include potentially serious financial losses and reputational harm.

Get Proactive and Limit Damage

Fortunately, you can take action to get ahead of a breach. If you need to know whether attackers already have invaded your systems, Trustwave SpiderLabs' Proactive Breach Detection service can help. The service can quickly determine whether your systems are clean – or potentially compromised.

If evidence of a compromise is identified, Trustwave SpiderLabs can quickly take action to identify the full breadth and depth of the attack, contain the problem and help mitigate any exploited vulnerabilities. If the investigation does not uncover conclusive evidence of a compromise, the resulting report will include recommendations for improving your overall security posture and detection capabilities. You can then share the report internally to demonstrate actions being taken to identify and defend against any threats.

Unmatched Expertise

Nearly every day, Trustwave SpiderLabs responds to another data security incident, and overall we've investigated almost 2,000 compromises in the past seven years. This means we understand data compromises like no one else.

We are intimately familiar with the techniques and tactics that hackers use to infiltrate a system, how they locate and collect the target data and how they get that data out of a business' network. As a result, we also understand the traces attackers leave behind during each aspect of an attack – called indicators of compromise (IoCs). We apply our knowledge of attackers' latest methods to survey your network and identify IoCs or other signifiers of a possible breach.

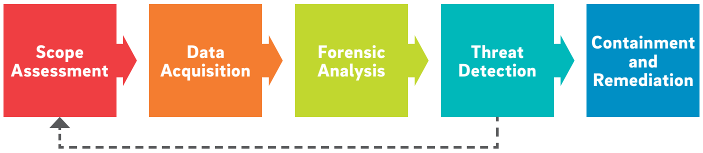
As a part of our Proactive Breach Detection service, we survey your environment for IoCs such as:

Indicator of Compromise	Evidence
External system access	Foreign IPs found in log files
Malware presence	File birth in forensic timelines
Malware execution	Prefetch, timeline, registry, memory
Malware output file	Timeline, malware reversing, registry
Data exfiltration	Application logs, system logs, network logs
Website code modification	Unauthorized code changes
SQL injection	Log files
Webshell presence	Log files, timeline

The 5 Phases of Breach Detection

Trustwave SpiderLabs delivers its Proactive Breach Detection service in five phases:

1. **Scope:** Identify systems, network segments, data and other resources within the environment that intruders would logically target.
2. **Gather Data:** Collect relevant system data to build a profile of relevant systems in their live state.
3. **Analyze:** Evaluate systems, network segments, data and other resources for evidence of indicators of compromise (IoCs).
4. **Detect Threats:** Identify the presence of a compromise and identify any additional systems that may have been impacted – based on information gathered in prior phases.
5. **Contain and Remediate:** Contain and remove the threat and return systems to a secure, normal operating state.



1. Scope Assessment

During this phase, Trustwave SpiderLabs will gather data to understand the logical targets within an environment that may be valuable to attackers. We will inventory assets, review network diagrams and evaluate controls that are in place that could detect malicious activity.

2. Data Acquisition

Trustwave SpiderLabs will gather data to develop a thorough understanding of the traffic that traverses your network and any events that occur in the system's current state. Data is gathered via live, dead and logical data acquisition; log collection; application-specific data collection; network packet capture and live analysis.

3. Forensic Analysis

The third phase will result in a comprehensive view of potentially compromised systems and relevant attack vectors. Trustwave SpiderLabs will consolidate information, gathered in prior phases, for forensic analysis, correlation and event reconstruction. Analysis may include the inspection of:

- **Volatile Data –** Analyzing memory that may contain evidence of malicious applications and network connections.
- **Disk(s) –** Evaluating hard drives for evidence of files created, modified, deleted or accessed by an intruder.
- **Logs –** Correlating events among disparate systems, such as network devices, operating systems and applications that may reveal malicious activity.
- **Networks –** Capturing, dissecting and examining data packets for evidence of rogue network connections, data exfiltration and more
- **Malware –** Reverse engineering of any discovered malware to determine its functionality, artifacts it may create as a result of execution and any unique identifying information

4. Threat Detection

As a part of the threat detection phase, information gathered may point to signs of a potential compromise spreading to additional systems and networks. Trustwave SpiderLabs will employ host-based network detection techniques to audit additional systems. This may include disk sweeps to identify known malicious files, folders and registry keys, or the presence of log entries associated with malicious activity. Network detection may include, for example, the review of log records to identify additional systems communicating with a known rogue IP address. Any systems identified in this phase will be fed back into the scope assessment phase to ensure the breadth of a potential security breach is understood prior to containment and remediation.

5. Containment and Remediation

If at any point during the investigation Trustwave SpiderLabs discovers an indication of a potential breach, staff will immediately inform the client and provide recommendations to contain the data compromise. Once the full impact of the security breach is understood, Trustwave SpiderLabs can develop a complete containment and remediation strategy. That strategy will rapidly contain the current threat by neutralizing the intruder and return the environment to normal operation in a more trusted state. In the event that Trustwave SpiderLabs identifies a breach, a full forensic investigation can be launched at additional cost.

For more information: www.trustwave.com