Forrester Thought Leadership
Executive Summary
Commissioned By Fortinet

November 2015

Sandbox Technology: Building An Effective Breach Detection And Response Strategy

Much of today's competitive differentiation is based on the depth of your customer data and how efficiently you capture, store, and apply that information. A database teeming with consumer and client data is a powerful asset for your company — and a treasure trove for motivated attackers. The challenge of securing your data, network, and infrastructure is further complicated by the rise of advanced threats. Malicious adversaries have multiple modes of attack at their disposal and often string together different types to get past your defenses.

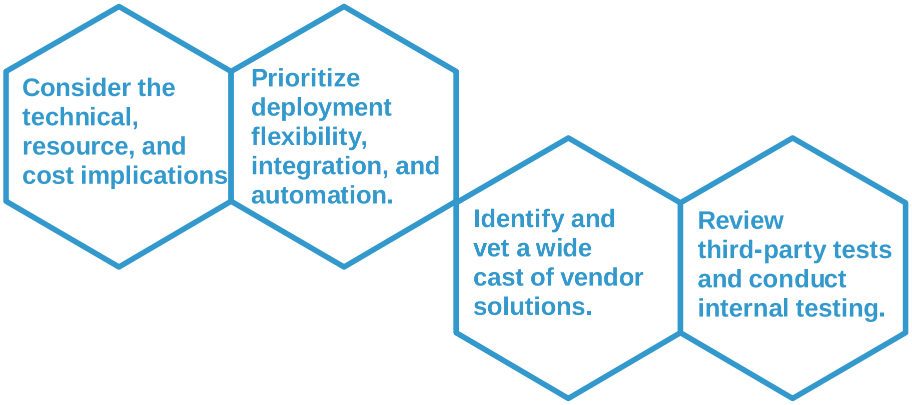
Security professionals need to arm their organizations with the right security solutions to detect threats and manage risks to avoid data breaches. Unfortunately, a determined and well-resourced adversary will find a way to penetrate protections, regardless of whether an organization has the most-advanced preventive controls. And while the hope is that preventive measures are effective, it's imperative to plan for detection and response.

Sandboxes — solutions that virtually replicate operating environments; execute suspicious code such as executables and application data; and observe, rate, and report the behavior — play a key role in this breach detection strategy. And while not a silver bullet, they are an important tool that often enables security pros to block or contain malware in the environment.

Fifty-five percent of surveyed IT security professionals reported their organizations have experienced six or more security incidents within the past 12 months.

Key Findings

Forrester's study yielded the following best practices for sandbox evaluation:



Consider the technical, resource, and cost implications

Prioritize deployment flexibility, integration, and automation.

Identify and vet a wide cast of vendor solutions.

Review third-party tests and conduct internal testing.

This is a summary of results from the Fortinet-commissioned Thought Leadership Study, "Sandbox Technology: Building An Effective Breach Detection And Response Strategy."

METHODOLOGY

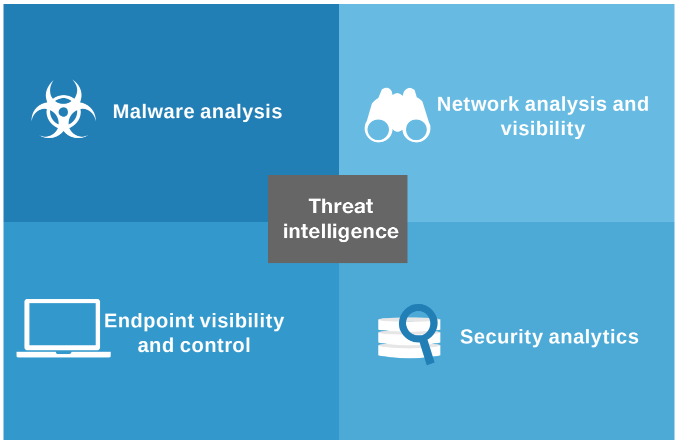
Fortinet commissioned this study to examine the purchase and implementation considerations, as well as the challenges faced, for sandbox solutions.

To explore this topic, Forrester conducted a quantitative survey of 150 IT security professionals at enterprises that had evaluated or implemented sandbox technology.

Advanced Attacks Are The New Normal

Malicious attackers are more advanced, leveraging known and unknown techniques in new ways to penetrate enterprise defenses. Surveyed security pros cited malware, phishing, denial of service (DoS) attacks, and attacks on OS vulnerabilities and web application vulnerabilities as the most-common methods of attack. Attackers often couple two or more of these tactics to exploit outdated patches and vulnerabilities or the human element.

Pillars of detection


Malware analysis
Network analysis and visibility
Threat intelligence
Endpoint visibility and control
Security analytics

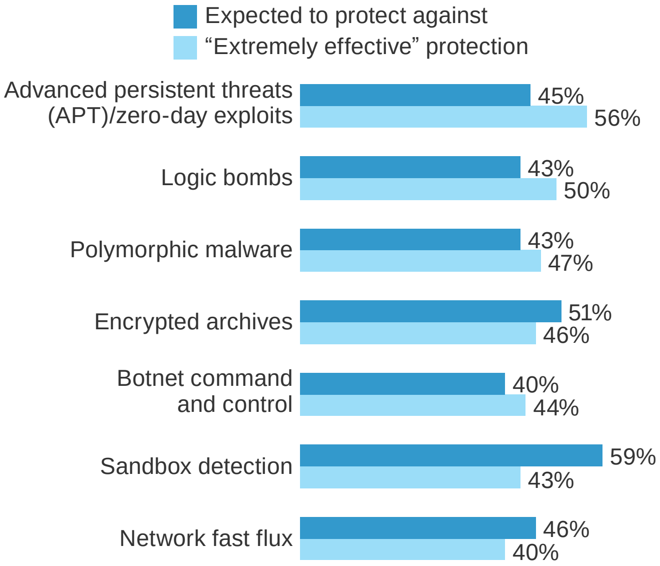
Source: Forrester Research, Inc.

With adversary capabilities at an all-time high, where should security and risk professionals turn? Your company needs a security strategy that employs robust prevention tactics but also accounts for determined, well-armed adversaries that can neutralize even the latest and greatest preventative controls. For this, you need a breach detection and response strategy built upon what Forrester calls the four pillars of breach detection: malware analysis (sandbox), network analysis and visibility (NAV), endpoint visibility and control (EVC), and security analytics (SA).

Sandboxes Play A Key Role In Breach Protection And Detection

Sandboxes are an essential component of a comprehensive prevention, detection, and response strategy. They allow security pros to block or contain sophisticated attacks in their environment, as well as mitigate and prevent damaging attacks in the future:

"When evaluating or implementing a sandboxing solution, what security threats did you expect it to protect against?"
(Select all that apply)
"How effective is/was your sandboxing solution in helping you protect against the following threats?"



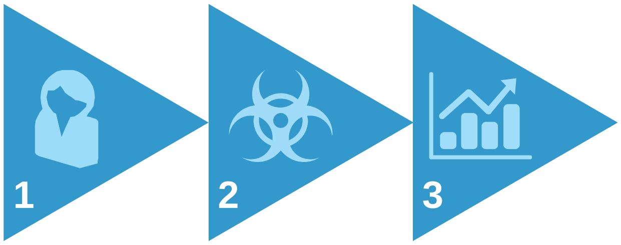
- Fifty-five percent of organizations experienced six or more attacks or breaches within the past 12 months, experiencing an average of four different modes of attacks.
- Fortunately, sandboxes provide effective protection against advanced threats, such as encrypted archives, network fast flux, polymorphic malware, logic bombs, and APTs, among other types of attacks threatening their organizations. Our survey respondents consistently reported sandboxes outperformed their pre-purchase expectations in these areas.
- Organizations need to know what's happening on their network in order to effectively respond to threats. Eighty-seven percent of the security pros surveyed reported that sandboxes arm them with various types of information vital to identifying potential threats, including malicious IPs and file hashes, behavioral results, indicators of compromise, a top-level view into threat activity, and detailed logs and analyses.

Best Practices For Evaluating A Sandbox Solution

The journey toward building an effective breach detection strategy begins with implementing the malware analysis capabilities of a sandbox. But before you take that step, it's important to take the time to select the right sandbox for you. Some lessons learned from study participants include:

- **Consider the technical, resource, and cost implications.** Technical considerations, such as the ability to identify and integrate new threat vectors or analyze a broad range of suspicious objects, were a high priority for our survey respondents when evaluating sandboxes. But they also considered resource implications, such as ongoing cost, implementation time, and the staff resources needed to manage the sandbox.
- **Prioritize deployment flexibility, integration, and automation.** Ninety percent of security professionals surveyed prioritized deployment flexibility when evaluating sandbox solutions. Integration is also highly desirable: The majority of security professionals surveyed (55%) reported they would like their sandbox to integrate with a least six existing security components. Fifty-five percent also reported they'd like a high level of automation.
- **Identify and vet a wide cast of vendor solutions.** While it may be tempting to limit your list of contenders to an incumbent vendor or a marquee brand, don't make this mistake. A top lesson learned, cited by 38% of the security professionals surveyed, is to consider a broader selection of vendors.
- **Review third-party tests and conduct internal testing.** Internal testing, single-vendor proof of concept (PoC), and vendor-provided references were among the top methods used by survey respondents for evaluating sandbox solutions. But don't rely on third-party tests or vendor PoC alone; be sure to thoroughly test multiple sandbox solutions in your own environment. The No. 1 thing security pros would do differently is conduct more thorough testing.

As you continue on your journey to beef up your breach detection, keep in mind that it will require more than just technology. Breach detection will fail unless you have the proper people, process, and oversight. While evaluating technology options:



1. Hire and train the right staff.
2. Assess your malware analysis process.
3. Measure your malware analysis program.

To read the full results of this study, please refer to the Thought Leadership Paper commissioned by Fortinet titled, "Sandbox Technology: Building An Effective Breach Detection And Response Strategy."

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.