29 APR 2016 OPINION

2016: Time for Security to Take its Head out of the "Sand" (box)

Israel Levy CEO of BUFFERZONE

As malware has become increasingly sophisticated, conventional protection solutions have proven insufficient for companies' IT security needs.

While "sandboxing" is still a popular, and frequently deployed solution, over the last several years new technologies and approaches have been introduced to the market. Let's take a look at one of those approaches, called "containers", and see how it measures up vs. the current industry standard set by sandboxes.

Common Problems

Containment is a fairly new concept, deviating from the widely known and popular "sandboxing" method. Sandboxing is a detection method which scans potentially malicious files in a confined area/an isolated environment, otherwise known as the "sandbox", to determine if it is indeed malware. Sandboxing arose as a response to the realization that signature-based technology had grown increasingly ineffective in protecting endpoints from

go-to" solution for thwarting unknown threats, is also
today's increasingly sophisticated malware climate, echoing
aced with the inadequacy of signatures.

al containers. Virtual containers reside on the endpoint and
s like web browsers, email and removable storage that come
ces. Unlike sandboxes, containers are not a time-limited
e is malicious. Instead, they provide an ongoing buffer
the internet and the "secure" realm of the corporate network.

Why Not Watch?

29 JAN 2015

Sony Pictures Entertainment: The Fallout from 2014's Biggest Breach

20 OCT 2016

Can Good Security Help Drive Greater Business Agility?

The Benefits and Drawbacks of Sandboxes

Several years ago, sandboxing became the popular approach to detecting advanced threats, causing several big-name security companies to advocate this as the preferred method. Sandboxes do not continuously run on endpoints, rather they generally run on a server and are used to detonate a suspicious file. Files are opened there first, and if they don't trigger any alarms after a short time, they are sent onward.

The sandbox is in action for a short period of time, scanning any unknown content and detecting malware. However, once this process is completed, the approved content is free to transfer over into the trusted network. Malicious content, unfortunately, is "smart" and is known to disguise itself as benign until the testing period is over. Following the testing period, the malware is released and a phenomenon known as "sandbox evasion" occurs.

Evolution of the container

Sandboxing and containers have their similarities - they both use virtualization to create a "safe space" for potentially malicious content. But, as hackers focus on devising attack methods that we haven't thought of, making them impossible to detect, containers take the approach that everyone is suspect.

The security architecture of containers, as opposed to sandboxes, is designed to outsmart malware evasion. With containers, detection is not essential. Instead, both non-malicious and malicious content remain in the container forever.

Containers have evolved out of the need for a more comprehensive solution, one that will create a sort of perimeter around any application that can be used as an attack vector, constantly running, isolating all unknown content, and maintaining constant segregation from trusted networks. A container runs continuously on the endpoint and rather than isolating a file for a short time, it isolates the risky application, like the web browser or email or Skype continuously. Container technology can be implemented in software, on top of the operating system, or as part of the microprocessor's firmware.

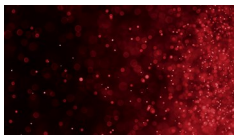
Containers assume anything unknown is untrusted and, therefore, keeps it in a secure and isolated environment, known as the "container". Anything unknown is eternally deemed untrusted and can only leave the container through a secure bridge that disarms threats and gives security teams control over what enters the corporate network.

Looking Ahead

With 44% of respondents in a recent SANS endpoint security survey admitting that one or more of their endpoints had been compromised in the past 24 months, 2016 will see more money invested in endpoint security—a market growing at a CAGR of 8.4% from 2015 to 2020.

While server-based file sandboxing has been successful in stopping many threats, today's sophisticated malware attacks demand a more comprehensive solution. Just as malware has evolved and taken on different forms, sandboxing, as well, is assuming different forms, including virtual containers, and micro-virtualization solutions that provide continuous protection. This more comprehensive approach ensures that any threat that gets in – whether through a web browser, email, document, phone etc. will be locked in a container indefinitely.

If we want to prevent the next data breach from happening, we must offer solutions that provide a solid defense, along with seamless deployment and management. Conventional sandboxing has an important role to play in terms of testing suspicious executables in a safe environment. But it is no longer effective in preventing unknown threats as containers continuously isolate risky applications, do not rely on detection and provide a more effective long-term solution for user endpoints from whatever hackers come up with next.



26 MAR 2015

Insights into Incident Response – A View from the Front Lines

17 NOV 2016

Network Encryption made EASY: Utilizing Network Virtualization to Simplify Network Encryption & Enhance your Network Security

Related to This Story

The Security Challenges of Enterprise Container Adoption

A Data-Driven Approach to Security Decision Making

Web Isolation: The Evolution of Enterprise-Ready Isolation

Ten Compelling Reasons to Improve Security when Harnessing the Power of Desktop Virtualization

Attacks on Virtual Infrastructure Cause Double the Pain

What's Hot on Infosecurity Magazine?

Read Shared Watched Editor's Choice

1 28 JUL 2017 NEWS
German Police to Bypass Encryption by Hacking Devices

2 25 JUL 2017 NEWS
Widespread, Brute-Force, Cloud-to-Cloud Attacks Hit Office 365 Users

3 28 JUL 2017 NEWS
Emotet Crimeware Adds Self-Propagation to the Mix

27 JUL 2017 NEWS

4 #BHUSA: You're Dealing with Supply Chain Security Whether You Like it or Not 28 JUL 2017 NEWS

5 North Korea Turns Cyber-Attention to Hacking for Profit

27 JUL 2017 NEWS

6 Google Uncovers Highly Targeted Spyware "Lipizzan"