In 2016, Resolve to Slim Down "ALL THE ENDPOINTS!"

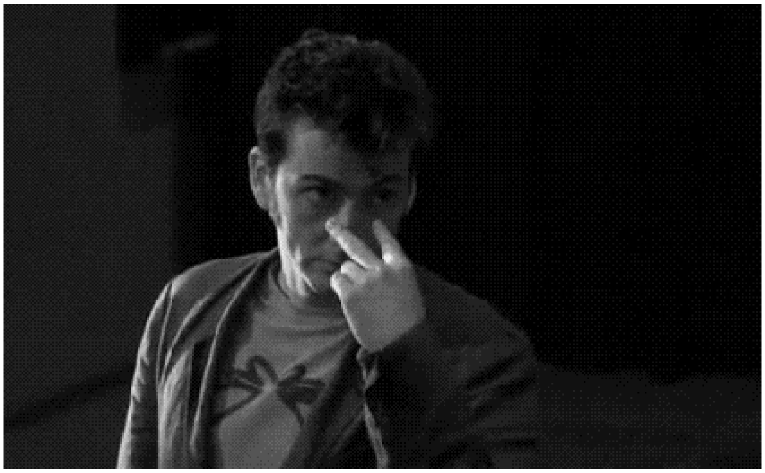
05
JAN

In 2016, Resolve to Slim Down “ALL THE ENDPOINTS!”

January 5, 2016 / Ryan Nolette / Advanced Threat Protection, Community Perspectives, Detection and Response, Endpoint and Server Security, Prevention, Response

Welcome to 2016, where security technologies from the early 90s still reign supreme in some enterprises and corporate data breaches are happening faster than breaking your New Year’s resolution.

I’m looking at you. Put down the pastry.



Now that we’ve had that little heart-to-heart chat, let’s discuss something that acts as a nutrition coach for your endpoints. Trust-based security, a security technology usually grouped under the umbrella term “application whitelisting” will help you slim down those endpoints into the lean, mean, malware-blocking machines you always dreamed of.

Application whitelisting is a very potent tool set that can defend against unknown malware threats, but it has only been during the past few years that it has really started to take off. One of the main reasons for the delay in adoption is that traditional whitelisting solutions are hard to configure and maintain. That is no longer the case.

Yes, there is initial time investment required because every environment is different, however, you can always hit that big red button that locks down everyone at any time if you find a security threat before you finish tuning.

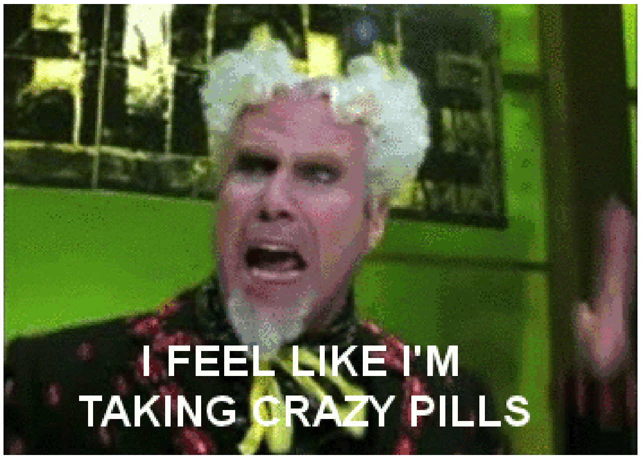
To give you an idea of how mainstream whitelisting has become, NIST (National Institute of Standards and Technology) [PDF] and SANS [PDF] have whitepapers on how to use whitelisting and how important it is to your company's security posture.

So why do I like whitelisting? Well, call me old fashioned, but I prefer to know who I am letting into my house.

For example, almost every technology company has a badging system for their offices. This system works by checking the scanned badge against a predefined list of allowed personnel and only unlocking the door for pre-approved people. This essentially is how whitelisting works. It makes sense. It is a tried and proven technique for physical security for decades.

Admittedly, there are some workarounds though, like tailgating, which is the act of following an approved person through the door without badging in. Sounds an awful lot like an exploit kit doesn't it? Even with this limitation, I still prefer a whitelisting solution to the blacklisting methods used by traditional antivirus solutions because I can create rules to lockdown known vulnerable applications.

Can you imagine trying to secure a building by only denying entry to those people you know shouldn't get in? That is, at a high level, what AV does. It has a list (signatures) of known bad software that it checks every file/application against. If nothing flags, it can run on that system. Does anyone else see the absurdity in trying to make this method effective long term?



New year, new you, new threats…outdated security controls. One of these isn't like the others. Let's change that in 2016

Until next time, remember my motto: "Flag it, Tag it, and Bag it."

Tags: bit9 Carbon Black endpoints New Years resolution security Whitelisting

More Posts

May 27, 2016 / *by Ben Johnson*

#BENVLOG: Crafting a Pattern of Attack "Story" at the Right Level

In today's video blog, Ben Johnson discusses how crafting stories using Patterns of Attack requires hitting the "sweet spot." _____________ What is "Collective Defense?" Click here to learn more.

February 24, 2015 / *by Ben Johnson*

Screenshot Demo: "Rewind the Tape" to Detect Ventir Dropper Malware on Mac OS X

Today's screenshot demo is going to give you a quick glimpse into some of the visibility you get with Carbon Black on Mac OS X. This post touches on some key points to how quickly you can "rewind the tape" to detect Ventir. In this example, the starting point is a typical one—take a strange...

June 3, 2016 / *by Ryan Murphy*

June 3, 2016 – Morning Cyber Coffee Headlines – Casey at the Bat Edition

Good morning! Sit with Carbon Black this morning over a cup of coffee (or tea) and browse a few industry headlines to get the day started. We've got just enough information below to get you through that first cup…enjoy! June 3, 2016 – Headlines Carbon Black in the News: New Windows Zero Day Exploit For Sale…

May 12, 2016 / *by Ryan Murphy*

May 12, 2016 – Morning Cyber Coffee Headlines – Limerick Edition

Good morning! Sit with Carbon Black this morning over a cup of coffee (or tea) and browse a few industry headlines to get the day started. We've got just enough information below to get you through that first cup…enjoy! May 12, 2016 – Headlines Healthcare Suffers Estimated $6.2 Billion In Data Breaches – Dark Reading…

Subscribe

ENTER YOUR EMAIL ADDRESS

PREFERENCES

□ Blog Posts
□ Morning Coffee
□ Community Perspectives
□ Tech Toolbox

SUBSCRIBE

Categories

Advanced Threat Protection (184)

Community Perspectives (125)

Compliance (15)

Detection and Response (161)

Endpoint and Server Security (160)

Featured (1)

Mobile Security (4)

Morning Coffee (113)

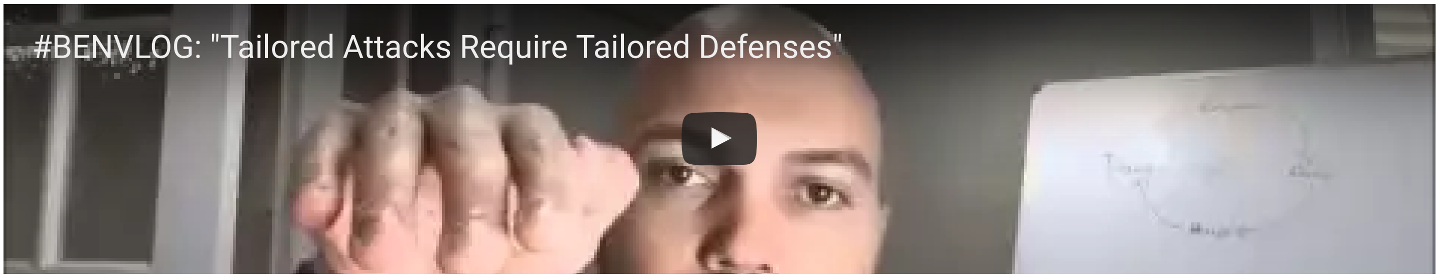
Prevention (91)

Response (115)

Tech Toolbox (82)

Uncategorized (2)

BenVlog: Tailored Attacks Require Tailored Defenses



Authors

- Adam Koblentz
- Alex Baker
- Ben Johnson
- Ben Tedesco
- Berni McCoy
- Threat Intel Team
- Editorial Staff
- Brent Midwood
- Bruce Van Dyke
- Chris Berninger
- Chris Lord
- Christopher Strand
- Dave Brown
- David Dorsey
- Eric O' Neill

Tags

- Ben Johnson
- bit9
- Carbon Black
- detection
- endpoint security
- incident response
- malware
- morning coffee
- security
- security headlines

Carbon Black on Twitter

Shifting The Economic Balance Of #Cyberattacks - @DarkReading https://t.co/qOxUaZqXgA
2 hours ago

Lunchtime Listen: @chicagoben on @FedNewsRadio discussing threat intelligence and securing endpoints https://t.co/NStTgTLAxL #infosec #DFIR
3 hours ago

Had a blast at the @splunk event in Seoul yesterday! #cybersecurity https://t.co/DeRg2BYuYR
4 hours ago

We're hiring a versatile #UX #Designer! Apply here: https://t.co/dz42tR14nB https://t.co/GbnKjI7VjH
4 hours ago

Join fellow #security pros in #London on July 6th! Learn how to transform your #SOC https://t.co/tW1wxOWH2i https://t.co/xT0U8IsiBY
4 hours ago

Archives

2016

2015

2014

2013

Privacy Policy Terms & Conditions
License Agreements