Why Applying Zero Trust Within Endpoints Means Greater Security with Less Effort

by Eirik Iverson

Everybody seems to be buying into the concept of doing more with less, but how can we apply that to endpoint security? Apply zero trust principles WITHIN endpoints.

Zero Trust Doesn't Always Mean Greater Security

Zero trust is centered on the belief that undetected malicious activity will inevitably be present at some point or another, and therefore organizations should not automatically trust anything inside or outside its perimeters. Instead, organizations must apply security practices that assume anything could be malicious. The model presents an approach where the default posture is to deny access.

The concept of zero trust is not new. For well over a decade, we've been hearing about the need for a "zero trust" based cybersecurity infrastructure, to the point where the term is now overused and generically applied across the industry. Yet, despite all the tools claiming to operate on, and enforce, zero trust, more and more breaches are occurring. It is becoming increasingly difficult to manage the numerous zero trust security technologies deployed.

Zero Trust WITHIN Endpoints: True Endpoint Protection

Claiming to offer a zero trust security solution is not enough. It is how you apply zero trust that determines the effectiveness and ease of management. Applying zero trust WITHIN endpoints, meaning endpoints are segmented with policy provisions, ensures endpoints don't even trust other parts of itself. Applying zero trust WITHIN endpoints not only provides you greater security, but it also allows you to do more with less.

However, a zero trust approach WITHIN endpoints is at odds with the "detect and react" paradigm at the core of so many of today's leading endpoint protection solutions. Detect and react tools have common functionality: collect lots of data, monitor and investigate lots of alerts, and do all of this with more sensors, more tools, more integration, and more people. In a world striving to do more with less, the traditional detect and react approach doesn't make sense. In reality, the detect and react approach results in having to "do more, with more." By applying zero trust WITHIN endpoints, you ensure that applications and utilities conform to trustworthy behaviors. By doing so, zero trust WITHIN endpoints actually alleviates some of the burden of detect and react tools.

Improving Cyber Security Efficiency with Zero Trust

Consider the fact that zero trust WITHIN endpoints means malware attempting to exploit applications or utilities to cause harm will be blocked from executing processes on other parts of the endpoint. This not only prevents malware from compromising endpoints, but it also means detect and react tools downstream in the cyber stack will detect fewer incidents and will fire off fewer alerts, thereby reducing the number of alerts needing investigating and remediation. Fewer alerts mean cybersecurity analysts have more time to focus on more strategic issues, and more time to dedicate to improving overall security hygiene. These are just a few examples of the value of zero trust WITHIN endpoints.

Defenders struggle to keep up with the speed of the adversaries. Zero trust enforces its "deny actions" in real time, thereby reducing what the detection teams must consume. This means zero trust helps defenders keep up with the speed of the adversary. Most "suspicious" activities monitored by detect and react tools (IDS, UEBA, XDR, SIEM, etc.) ultimately originated from one or more compromised endpoints. These compromises result from applications and utilities on these endpoints letting malware in or doing harm afterward. By blocking these actions within the endpoint, the rest of the cyber stack need not be burdened.

Zero trust WITHIN endpoints assumes applications and utilities will, at some point, go rogue: downloading/executing malware, stealing credentials from the memory of other applications, conducting remote execution attacks on other endpoints, etc. By blocking these actions from happening, the attack is neutralized. Zero trust WITHIN endpoint restricts what executables, scripts, or DLLs may run/load. It contains high-risk applications so they cannot harm the rest of the host. And it isolates high-value parts or the endpoints so the rest of the host cannot harm or steal from them. Zero trust enforces its "deny actions" in real-time, thereby reducing what the detection teams must consume.

Zero Trust WITHIN Endpoints: More Secure with Less Effort

Now, imagine the implications that neutralizing an attack has on the many different layers and workflows of your cybersecurity operations. How many cleanup processes could be avoided? How much labor could be freed up? What might freed up personnel achieve when not distracted by attacks snuffed out at endpoints? How much could you improve your cybersecurity with the time you gained back? Zero trust WITHIN endpoints truly allows you to do more with less. By making business secure by default, zero trust WITHIN endpoints provides greater security, greater efficiency, and peace of mind.

About the Author

Eirik is a Principal Product Engineer at AppGuard, a pre-detection endpoint protection software company. He has been in the cybersecurity industry for over 20 years in product management, marketing, and product engineering roles across many different domains. His previous decade was in military technologies providing program management, performance measurement, and process improvement. Eirik has a BS in Aerospace Engineering from University of Maryland and MBA from Carnegie Mellon University.