Federal Bans of Specific Products Should Have You Wondering: Can You Remove What You Can't See?

Katherine Gronberg, Vice President, Government Affairs | March 21, 2019

The federal government has banned hardware and software made by Huawei, ZTE, Kaspersky and others from its networks. It could soon ban them from yours.

U.S. federal agencies are not allowed to have certain types of hardware or software on their information technology (IT) networks. In 2017, the U.S. Department of Homeland Security (DHS) issued a directive [1] requiring all federal departments and agencies to identify and remove Kaspersky products. Section 1634 [2] of the Fiscal 2018 National Defense Authorization Act (NDAA) prohibits all federal departments and agencies from using any hardware, software or services developed or provided by Kaspersky Lab. Section 889 [3] of the Fiscal 2019 NDAA prohibits all federal agencies from procuring equipment produced by Huawei Technologies Company and ZTE Corporation, as well as several others, and their subsidiaries or affiliates.

Some agencies may respond to these prohibitions by contracting with large integrators who will send fleets of consultants around with a pen and clipboard to manually count all instances of banned products. This may cost millions of dollars, the numbers might not be right, and their data may be outdated each time they advance to the next computer enclave. Without an automated, real time tool that can detect all of the IT devices — computer or "other" — on your networks, there is simply no way to be 100 percent certain that you are compliant with these product bans.

In our experience, manual enforcement of such product bans is tantamount to no enforcement at all. The proof is that, in new deployments of Forescout, we find a fair number of banned devices. Examples include Xboxes, Raspberry Pis, external hard drives and more. Sometimes there are good reasons for these policy violations: Xboxes are a common occurrence in pediatric waiting rooms, for example. Sometimes there are bad reasons: Someone couldn't be bothered to reach under their desk to plug in his iPhone or Fitbit to charge and instead decided to connect it to his desktop, conveniently forgetting the regulation that prohibits this activity. People violate policies, period. To have real security, your system must tell you when your policies are being violated and automatically secure and correct these violations.

Federal agencies that have implemented Phase I of the Continuous Diagnostics and Mitigation (CDM) program, with Forescout as their detection tool, have the capabilities that allow them to efficiently address these product bans. They have tools in place that allow them to discover, automatically and in real time, and remove any prohibited hardware or software product the instant a non-compliant device tries to connect to their networks. U.S. Department of Defense agencies that have implemented the Comply to Connect (C2C) program utilizing Forescout have the same capabilities. Both programs are based on the National Institute of Standards and Technology (NIST) concept of "continuous monitoring." [4] Both programs feature Forescout as one of their foundational capabilities for device visibility, classification, and control. Forescout

enables its federal customers to identify banned products, block them from connecting to the network so they don't pose a risk to more important systems or devices and can initiate mitigating actions in accordance with agencies' policies to address both the device and the policy violator.

If you're a CEO of a private company, why would you care about this? Federal policymakers have given every indication that they intend to leverage federal authorities to ban untrusted hardware and software from use by private U.S. companies. The Fiscal 2019 NDAA contained a further provision that prohibits recipients of federal loans, grants and subsidies from utilizing the funds from procuring the same product banned in the federal agencies. And it has been widely rumored that the current Administration is considering an executive order [5] to declare a national emergency that would prohibit U.S. companies from using telecommunications equipment made by Huawei and ZTE, and perhaps others. Note that the prohibition may be on "using" equipment, not just on "buying." This would potentially eliminate amnesty for previously purchased or deployed assets.

Until there are better ways to secure the supply chain for information and communications technology, enterprises will need to mitigate the risk posed by untrusted products. The federal government is wasting no time making this point clear, using its grant-making power to effectively disallow groups of private entities from purchasing certain products. Private companies in the U.S. should pay attention to this and ask themselves how they would comply with such prohibitions and perhaps more importantly, how they would demonstrate compliance to federal regulators. "Guys with clipboards" is probably not going to be a sufficient answer, nor should it be. U.S. companies should ask themselves if there is a better way to prepare for this coming paradigm, particularly because what used to be a matter of a mere "finding" could soon be a matter of "breaking federal law."

Read more about specific ways in which Forescout can help your organization protect against cyber-attacks by discovering, classifying and managing all the devices on your network.

Forescout Solution Brief: Locate and Remove Prohibited Devices

[1] Directive: https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01

[2] Section 1634: https://www.congress.gov/congressional-report/115th-congress/house-report/404/1?overview=closed [3] Section 889: https://www.congress.gov/congressional-report/115th-congress/house-report/863/1?overview=closed [4] Continuous Monitoring: https://csrc.nist.gov/publications/detail/sp/800-137/final

[5] Executive order: https://www.politico.com/story/2019/02/07/trump-ban-chinese-telecom-1157090