FORESCOUT

Locate and Remove Prohibited Devices

An unparalleled ability to detect, classify and take action on rogue devices and software

> We're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications.
>
> **FBI Director Christopher Wray**

Governments are taking decisive steps to prohibit the use of certain devices on their networks. Forescout's agentless technology enables you to see, control and remediate banned hardware and software

Why are Kaspersky and other products being banned?

Governments are increasingly enacting laws and regulations to ban software and specific devices such as those manufactured by Kaspersky, Huawei and ZTE because of the security risks these products pose to the security and integrity of data and business functions. Despite the presence of procurement policies and processes to counter this risk, prohibited hardware and software continue to find their way onto enterprise networks. This is especially true for Internet of Things (IOT) and Operational Technology (OT) devices. It is essential that organizations continuously monitor and assess their networks to detect prohibited items. Forescout provides the visibility needed to detect and take action on banned products.

- For organizations to remain secure and compliant in the face of high-risk and banned hardware (HW) and software (SW) products, they must have a way to accurately detect, classify and control assets that are not controlled through procurement. This is even more critical for mission-critical networked equipment (such as scanners, handhelds, and scientific equipment).

- Supply chain security is not just about processes that occur during the product design and manufacturing stages. It must be maintained during the whole lifecycle of the product. HW and SW must be continuously monitored while connected to an organization's network.
- Organizations must have a continuous way to detect and automatically remediate (remove or quarantine) banned HW and SW, as well as to detect and remediate products with known vulnerabilities.
- Rather than a collection of non-integrated tools, IT and security personnel need a visibility and control solution that provides a single-pane-of-glass view across the extended, heterogeneous enterprise.

Hardware and software must be continuously monitored while connected to an organization's network.

Remove banned products – it's the law!

- U.S. Department of Homeland Security Binding Operational Directive (BOD) 17-01 directs federal departments and agencies (D/As) to identify any use or presence of Kaspersky products on their information systems and to develop detailed plans to remove and discontinue present and future use of Kaspersky products. The BOD applies to all "federal information systems" which includes information systems used or operated by a contractor of an agency or by another organization on behalf of an agency.[1]
- Section 1634 of Public Law No. 115-91 (the Fiscal 2018 National Defense Authorization Act) prohibits all federal departments and agencies from using any hardware, software or services developed or provided by Kaspersky Labs.[2]
- Section 889 of Public Law 115-232 (the Fiscal 2019 National Defense Authorization Act) prohibits all federal agencies from procuring equipment produced by Huawei Technologies Company or ZTE Corporation or any of their subsidiaries or affiliates.[3] The U.S. Federal Communications Commission has issued a Notice of Proposed Rulemaking (NPRM) that would ban Huawei and ZTE technology from being procured using Universal Service Funds (USF). Several programs designed to bring greater broadband connectivity in underserved areas and populations which are supported by the USF would be affected by this prohibition, including the Schools and Libraries (E-rate) Program.[4, 5]

U.S. State and Local Governments: At least one state has introduced legislation that would ban Kaspersky products from use on any state agency network.[6]

International: Australia has issued a Huawei and ZTE ban for telecommunications providers and New Zealand issued a Huawei ban for telecommunications providers.[7,8]

How the Forescout Platform Conquers Banned Products

Forescout customers discover up to

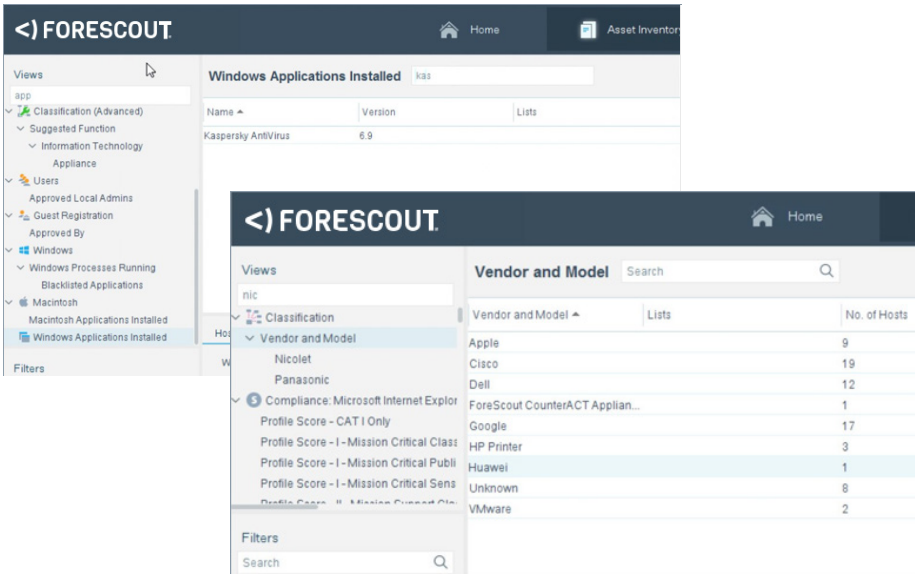
60%

more devices than they knew they had

The Forescout device visibility and control platform occupies a unique space among network security solutions because of its agentless approach to device visibility. Using Forescout companies have reported discovering up to 60 percent more devices than previously known.* A physical or virtual solution, it lets you instantly identify devices with IP addresses, including network infrastructure, BYOD systems, non-traditional IoT devices (handhelds, sensors and machines) and rogue endpoints from Kaspersky, Huawei and others—without requiring management agents or previous device knowledge.

Forescout provides insight into virtually any connected device across your enterprise, known or unknown. The platform deploys quickly into your existing environment and rarely requires infrastructure changes, upgrades or endpoint reconfiguration. Forescout's agentless approach to security lets you discover devices in real time, then classify, assess and monitor these devices. Visibility extends to virtual devices such as virtual machines (VMs) in private and public clouds. In addition, the platform provides agentless control and continuous monitoring across your heterogeneous environment. You can automatically trigger actions to notify, control and remediate.

By providing secure network access for a wide range of devices and user populations, the Forescout platform helps government and private-sector entities protect their confidential data and support their efforts to comply with federal or other mandates for identifying and disposing of banned hardware and software.



* Based on actual ForeScout customer experience.

1 https://cyber.dhs.gov/bod/17-01/
2 https://www.congress.gov/congressional-report/115th-congress/house-report/404/1?overview=closed
3 https://www.congress.gov/bill/115th-congress/house-bill/5515/text
4 https://www.fcc.gov/document/fcc-proposes-protect-national-security-through-fcc-programs-0
5 https://www.usac.org/about/default.aspx
6 https://custom.statenet.com/public/resources.cgi?id=ID:bill:NH2017000H1335&ciq=ncsl&client_md=c53ddbc4d6e319083218cbae6dc05c24&mode=current_text
7 https://www.bbc.com/news/technology-45281495
8 https://www.bbc.com/news/business-46368001

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com