FORESCOUT

Use the Forescout Platform for Security and IT Operations During COVID-19

The COVID-19 pandemic has created serious, wide-ranging IT and security challenges for organizations worldwide that must balance continuing to function as normal while reducing their on-premise workforce to limit health risk. However, the situation has also created an opportunity to adapt existing and new cyber defense technology investments. As increasing numbers of employees work from home, new obstacles arise, such as scaling and securing Virtual Private Networks (VPNs) and remote access. Most organizations had not previously established or required mature security practices for their VPN networks or their remote workers at the scale they now face. Finding solutions today will help organizations that embrace this turn of events, even after our current situation has passed.

Meeting the Challenge with Forescout

As a first step toward tackling these challenges, organizations can leverage their investment in the Forescout platform to extend security policies within their corporate network to their suddenly increased remote workforce. Organizations' security and network teams need to extend the same level of insight and control to remote users and devices when they connect to corporate networks by VPN as they would for those on campus. This can be achieved by compliance assessment and policy-based endpoint and network controls, which can help secure devices while remotely connecting corporate or Bring Your Own Device (BYOD) systems to corporate networks. Additional methods include security and policy compliance monitoring and the ability to act upon threats quickly.

Security and Network teams must see and identify all remote devices the moment they connect to the corporate network—just like on-campus devices. This extended visibility helps to minimize risk in the new work-from-home environment. Next, they need to ensure those devices are compliant, and remain that way, regardless of the specific location from which they connect.

Armed with that visibility, Security and Network teams can further understand the security posture of their remote devices and manage them accordingly based on a risk assessment for each scenario. To obtain these assessments, Forescout customers can install SecureConnector,™ a dissolvable or persistent client on personal Windows/Mac/Linux PCs or laptops. Using this technology, Forescout customers can ensure both company-owned devices and personally-owned unmanaged devices connecting through VPNs are secure before accessing organizational resources and continuously remain compliant while connected to the corporate network.

The Forescout platform allows customers to identify VPN clients and enforce policies on:

- Managed Windows devices
- Managed Mac devices
- Managed Linux devices
- BYOD/unmanaged devices

Managed devices connecting via VPNs should be subject to the same pre-connect and post-connect security policies that are applied to on-premises devices. The Forescout platform can help address BYOD/unmanaged devices connecting through the VPN. Such devices are immediately flagged by the Forescout platform as non-corporate and logically grouped. This grouping of BYOD/unmanaged connected devices allows system administrators to easily monitor them for user-defined undesirable characteristics or behaviors. Security and Network teams can then rapidly make informed decisions about denying or limiting access to network resources. In this scenario, Forescout customers can deploy the optional lightweight SecureConnector client on to BYOD/unmanaged devices. Combining the Forescout VPN Concentrator Plugin with the SecureConnector client allows administrators to enforce stricter host and network controls over unknown VPN-connected devices, thereby ensuring they meet policy-defined security requirements before authorizing access to corporate network resources. For example, the VPN Concentrator Plugin can disconnect users and prevent them from reconnecting through the network's RADIUS or Active Directory authentication server.

To expedite the grouping of devices into appropriate categories for access control determination, Forescout offers a standard policy template that identifies the VPN segment first to determine which endpoints are managed (or unmanaged) by the organization. The screenshot in Figure 1 shows how Forescout can quickly identify your assets in logical groups, as well as organized by compliance and risk status.

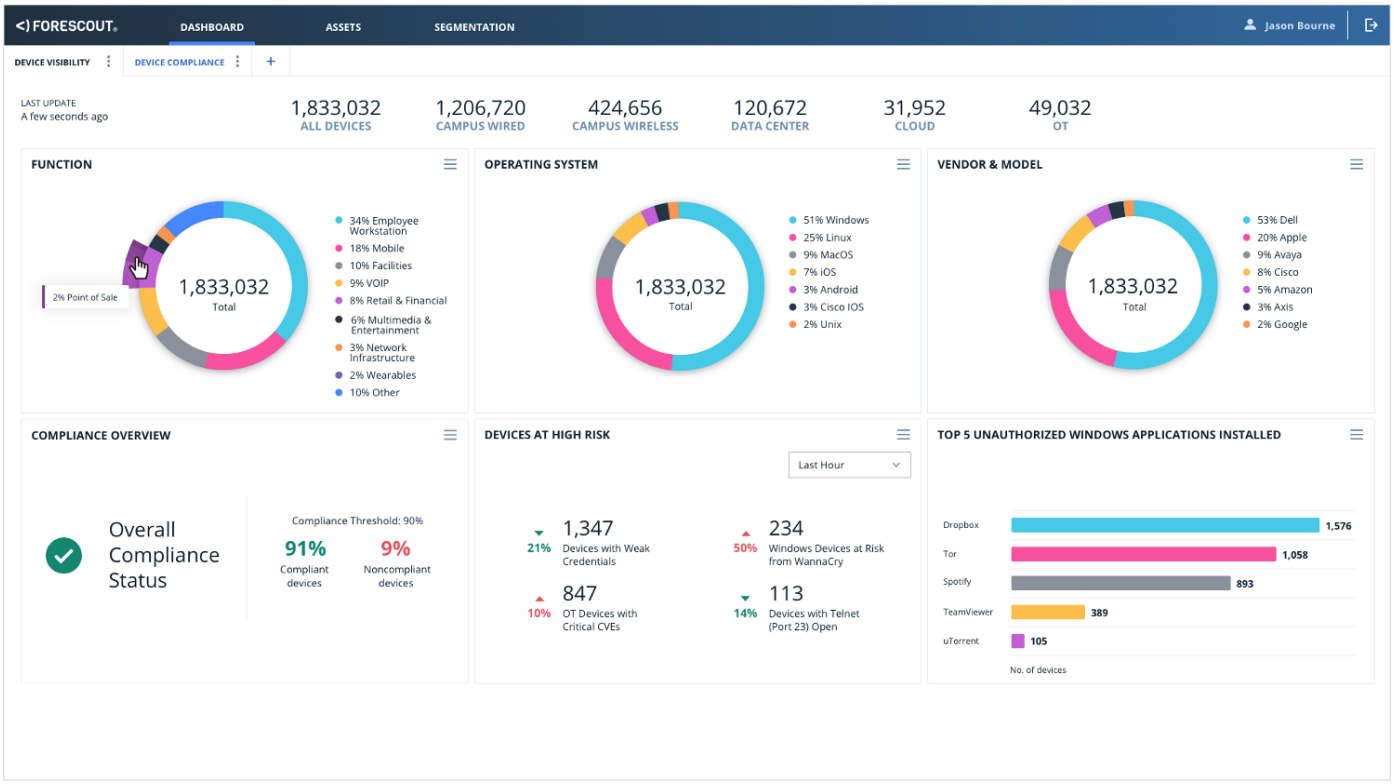

Figure 1 – Forescout dashboard identifying enterprise assets, risks and compliance state.

The Forescout platform identifies and secures devices connecting by VPN, with or without agents, thereby helping to ensure security hygiene, device compliance and a reduced attack surface.

To learn more about improving cyber hygiene or remote and on-site systems, read the Forescout Device Compliance Solution Brief.

<) 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