FORESCOUT

Canadian Centre for Cyber Security Top 10 IT Security Actions

Compliance with Forescout

Automated cybersecurity across your digital terrain

For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide automated cybersecurity at scale.

The Canadian Centre for Cyber Security maintains a list of the Top 10 IT security actions it recommends organizations take to protect connected networks and information[1]. These baseline controls and mitigation strategies are listed sequentially and are designed to add defensive layers. However, the Centre acknowledges that organizations may need to modify the order to best suit their specific requirements and priorities, based on an initial risk assessment.

Forescout supports all 10 of the Top 10 IT Security Actions:

- Defend Internet Gateways #1
- Patch Apps & OSs #2
- Enforce Admin Privileges #3
- Harden OSs & Apps #4
- Segment & Separate Info #5
- Tailored Training #6
- Protect Info - Enterprise #7
- Protect Info - Host #8
- Isolate Web-Facing Apps #9
- App Allow Lists #10

How Forescout helps (click here to see how)

The Forescout Continuum Platform extends scarce resources with continuous, automated asset management, risk compliance, network segmentation, network access control and security orchestration across all assets – cloud, IT, IoT, IoMT and OT/ICS – going above and beyond baseline security recommendations to provide a strong foundation for zero trust.

[1] https://cyber.gc.ca/en/guidance/top-10-it-security-actions

How Forescout Helps

SECURITY ACTION	FORESCOUT CONTINUUM PLATFORM CAPABILITIES
1. Defend internet gateway	▸ Monitor communications, including DNS traffic outbound to the internet, and alert when anomalous or errant DNS requests are generated
2. Patch operating systems & apps	▸ Continuously monitor last vulnerability scan date for all endpoints based on events instead of schedule, ensuring scans are being performed and looking for missing patches/updates for vulnerabilities as required ▸ Ensure vulnerability manager has not detected any No Longer Supported results and all patches are applied within required timeframes ▸ Continuously monitor OS versions to detect old or unpatched OSs on all types of devices: Windows, Linux, MacOS and firmware on IoT, OT/ICS and IoMT ▸ Monitor vulnerability scan results, audit Microsoft SCCM client registration and collection membership, and detect pending updates ▸ Continuously monitor and automatically remediate Windows Update patch status via WSUS or Microsoft Update ▸ Integrate with endpoint management solutions like Ivanti and ManageEngine
3. Enforce management of admin privileges	▸ Audit network traffic to ensure admin connections come only from defined area, such as Privileged Access system ▸ Continuously monitor group membership and attributes on privileged accounts, e.g., to ensure training and certifications are current ▸ Ensure devices with privileged account users logged in are not accessing the internet or using email or web services
4. Harden operating systems & apps	▸ Continuously monitor installed applications to ensure no high-risk applications or frameworks are installed ▸ Verify via automated policy controls that applications are installed, updated and licensed as required ▸ Monitor endpoints with SCAP policies to ensure application hardening settings have been applied
5. Segment & separate information	▸ Automatically map assets and traffic flows to logical taxonomy of users, applications, services and assets, leveraging a traffic matrix to facilitate policy design and visualize violations ▸ Simulate planned segmentation policies to assess impact before deployment ▸ Enforce policies that restrict access to sensitive resources when violations are detected but allow critical operations to function
6. Provide tailored training	▸ Train users on our platform to optimize performance and outcomes ▸ Identify non-Forescout training gaps based on observed network behavior that our platform monitors
7. Protect info at enterprise level	▸ Automate policy-based control actions (network access, device compliance, segmentation, remediation, incident response) to ensure only authorized systems and users are accessing systems and data ▸ Use a single policy decision point/engine aligned with your security framework to orchestrate controls across multivendor enforcement technologies (firewalls, ACLs, SDN controllers, VLANs, etc. ▸ Continuously monitor networks to ensure only authorized communications occur between systems and users despite dynamic changes to enforcement points
8. Host-level protection	▸ Ensure only authenticated, compliant, verified hosts are on the network ▸ Ensure hosts remain compliant throughout duration of connection
9. Isolate web-facing apps	▸ Use automated, policy-based segmentation controls (#5, 7) to ensure web-facing systems are only communicating with the appropriate systems
10. App allow lists	▸ Ensure managed hosts are properly configured for application whitelisting so authenticated, compliant systems can only run authorized software applications

Forescout Technologies, Inc.

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

Learn more at Forescout.com