FORESCOUT

Automated cybersecurity across your digital terrain

Essential Eight Compliance with Forescout

Achieve Maturity Level 3 with all Essential Eight controls

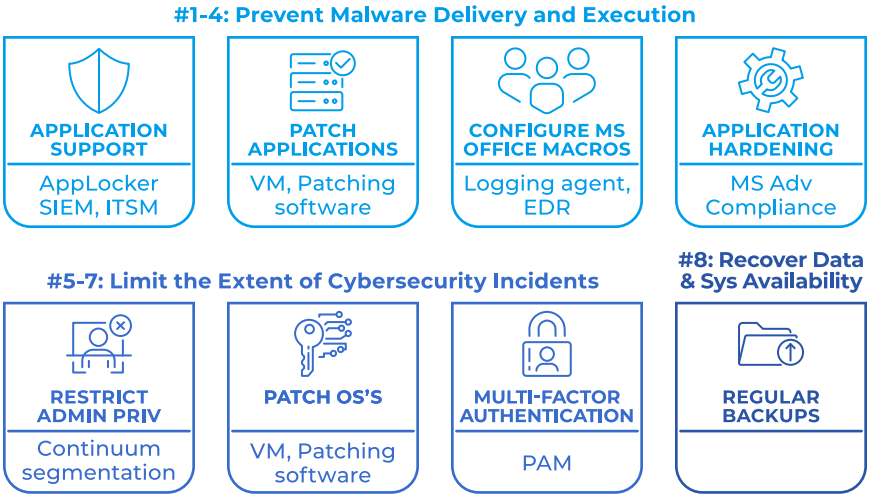
The Australian Cyber Security Centre's Essential Eight Maturity Model is a set of mitigation strategies designed to improve cybersecurity posture by making it hard for adversaries to compromise networks. With three maturity levels, even organisations with scarce IT resources can achieve baseline compliance and protection from increasing cyber threats. And with continuous visibility, compliance assessment and automated workflows using the equipment and security tools you already have, your network can adapt to your ever-changing digital terrain.

How Forescout helps

The Essential Eight is a set of mitigation strategies, not a single solution or technology that can be bought through a single vendor. They address three areas that require not only different security tools but tight communication and coordinated actions.

Either natively or by coordinating automated actions among security tools, Forescout enables you to achieve Maturity Level Three for all eight controls, with continuous visibility into granular compliance status.

By continuously monitoring every asset on your network and sharing collective insights among security products, Forescout enforces policies to drive the right automated actions and ensure compliance.



Automate cybersecurity across your digital terrain

The Essential Eight are designed to protect Microsoft Windows-based, internet-connected networks. For many organisations, that represents a fraction of their environment. Digital transformation has led to explosive growth in IT, IoT, IoMT and OT/ICS assets connecting to your network and expanding the attack surface. To manage this, you don't need more point products. You need a force multiplier – a platform that makes your security team more effective and enabled to focus on what really matters.

The Forescout Continuum Platform automates the near real-time and continuous discovery, assessment, and governance of all cyber assets across your environment, with special consideration for IoMT and OT/ICS assets that require different approaches. When you need to enforce continuous compliance across a mix of network and security infrastructure technologies, Forescout is here.

ESSENTIAL 8 CONTROL	HOW FORESCOUT HELPS
Mitigation strategies to prevent malware delivery and execution	
Application Control	▸ Continuously monitor the Application Control compliance status on every managed endpoint, ensuring each one is using the expected application control policies ▸ Check Enforcement Agents are installed and running ▸ Ensure central logging is functioning
Patch Applications	▸ Continuously monitor the last vulnerability scan date for all endpoints based on events instead of schedules; ensuring scans are being performed and looking for missing patches/updates for security vulnerabilities as required ▸ Ensure the vulnerability manager has not detected any No Longer Supported results and that all patches are applied within required timeframes
Configure MS Office Macros	▸ Continuously assess Microsoft Office macro settings by monitoring the windows registry and sending evidence of macro execution data to the central logging system ▸ Verify endpoint security agents are installed and running ▸ Check that devices have applied Group Policies (RSoP) to detect GPO deployment issues
Application Hardening	▸ Continuously monitor installed applications to ensure no high-risk applications or frameworks are installed ▸ Verify via Policy that applications are installed, updated and licensed for use as required ▸ Monitor endpoints with SCAP policies to ensure application hardening settings have applied
Mitigation strategies to limit the extent of cybersecurity incidents	
Restrict Admin Priv	▸ Audit network traffic to ensure admin connections come only from defined area, such as the Privileged Access system ▸ Continuously monitor group membership and attributes on privileged accounts, e.g., to ensure training and certification are current ▸ Ensure devices with privileged account users logged in are not accessing the internet, using email or web services
Patch OS's	▸ Continuously monitor operating system versions to detect old or unpatched operating systems on all types of devices: Windows, Linux, MacOS and firmware on IoT, OT/ICS and IoMT devices ▸ Monitor vulnerability scan results and audit Microsoft SCCM client registration, collection membership and detect pending updates ▸ Continuously monitor and automatically remediate Windows Update patch status via WSUS or Microsoft Update ▸ Integrate with third-party endpoint management solutions like Ivanti and ManageEngine
Multi-Factor Authentication	▸ Support MFA login to our platform ▸ Ensure MFA agents are installed and running on endpoints ▸ Ensure central logging agents are installed and running on critical MFA servers ▸ Audit network traffic is seen to/from the MFA servers
Mitigation strategies to recover data and system availability	
Regular Backups	▸ Enforce stricter policies for device compliance when used by privileged accounts ▸ Detect network access to the backup system and enforce user and device policies in near real-time ▸ Ensure Microsoft's Shadow Volume Service is running on Windows devices ▸ Support local and remote backup of the Forescout solution itself

FORESCOUT®

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