See it. Secure it. Assure it.

Essential Eight Compliance with Forescout

How to overcome common challenges in complying with the Essential Eight and gain confidence in your security strategy.

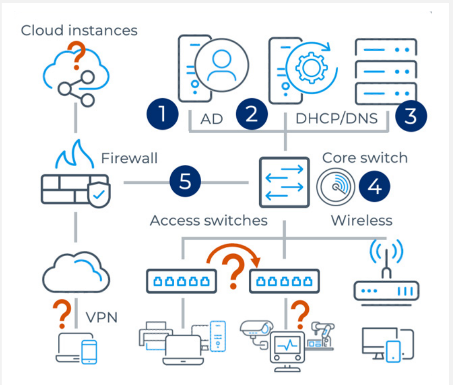
The Australian Cyber Security Centre's Essential Eight Maturity Model lays out a concise list of requirements for organisations looking to comply and bolster their cybersecurity posture. However, many organisations fall into the trap of viewing the Essential Eight as a simple checklist – deploying various tools to tick the boxes without truly addressing the underlying security challenges.

This checklist mentality often leads to the deployment of disjointed solutions that fail to work together effectively, resulting in a fragmented security strategy. Moreover, the shortcomings of each individual service can add up, eroding confidence in the ability to identify, assess, and respond to dangers that put your organisation at risk.

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.

Fully Comprehend Your Network

One such challenge is at the foundation of nearly all eight categories and is explicitly listed as the first item in both Patch Applications and Operating Systems – "*An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities*". This is important because regardless of how thorough your security framework is, you can't apply it to devices you don't see. To better understand where the difficulty lies, let's compare some common methods organisations use in attempting to discover their assets.

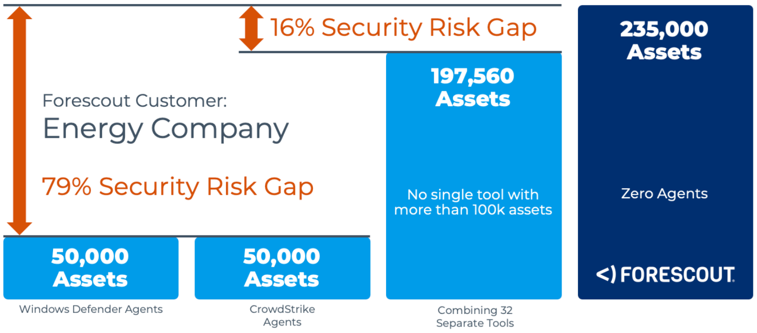


Gaps with Common Discovery Methods

1. **Active Directory:** Provides all domain-joined computers. It offers fair device context but lacks visibility into non-Windows devices.
2. **DHCP/DNS:** These site services can help broaden the scope, however devices with static IPs or without static/self-enrolled DNS names go unseen.
3. **Client Services:** Querying the management systems of tools like Endpoint Protection or Client Management platforms can provide good device context but is limited in scope to traditional IT endpoints with agents deployed.
4. **Recon Traffic:** Pings sweeps or other reconnaissance scanning can help reveal a wider range of devices but only if they respond back - it also generates network noise.
5. **Traffic Logs:** Obtaining traffic logs from core switches or firewalls lets you see more devices communicating on the network but its dependent traffic reaching that collection point. Device context is typically missing - however some vendors offer basic identification.

Confidently detecting and identifying every single device that touches your network is no easy task. While each of the above methods is a good effort to achieve that, not only does each have its individual shortcomings, but even when used together, they fail to detect a significant percentage of devices.

Here, you can see a real-world example of an organisation's attempt to use 32 similar methods for device discovery compared to what the Forescout platform was able to detect.



To achieve this Forescout uses over twenty different methods for discovery. Notably, Forescout has invested in developing integrations with hundreds of network device models spread across common enterprise vendors to get the direct source of truth about what is connected to your network.

But device detection alone is only a small step to fulfilling requirements with the Essential Eight, and that is because if a device is not properly identified then you cannot be sure what security guidelines apply to it. There is no sense in checking your printers for Microsoft Office Macros. Forescout provides accurate device classification for all endpoints so that you only check for policies relevant to its function.

This level of automated detection and identification ensures that not only is every endpoint that touches your network discovered, but they are subjected to the proper inspection and reporting required in your Essential Eight workflow.

Security Assurance

Organisations will likely need to adopt a host of tools in order to fulfill the requirements of the eight categories. Each service offers a specialised solution and most will require the installation of software on the target endpoint. Below is a general list of common solutions:

	CATEGORY	PRIMARY TOOLS USED
1	Patch Applications	Vulnerability Assessment (VA), Configuration Management Tool (CMT)
2	Patch Operating Systems	Vulnerability Assessment (VA), Configuration Management Tool (CMT)
3	Multi-Factor Authentication	Identity Services (MFA)
4	Restrict Administrative Privileges	Privileged Access Management solution (PAM)
5	Application Control	Application Security services
6	Restrict Microsoft Office Macros	Configuration Management Tool (CMT), Microsoft Group Policy, SCAP
7	User Application Hardening	Configuration Management Tool (CMT), Microsoft Group Policy
8	Regular Backups	Backup and Disaster Recovery solution (BDR)

Deploying services such as these will set you on course towards Essential Eight compliance, but it raises the question which leads back to the foundational challenge of device discovery – where are you deploying these agents to? How can you be sure all required devices are within scope of your security framework?

Additionally, all agent solutions have a dependency risk that the agent must be operational to report client status. If that client-server communication is broken, then the backend system is also unable to fix the problem. Just as with physical security, if a CCTV camera goes down or a server room door malfunctions, its common to have a person or system monitoring the status of all the critical pieces and address failures. For information security the same concept should apply.

Forescout acts as the manager of all your important IT security agents by constantly monitoring their status and applying automatic remediation if needed. For example, helping find orphaned client management tools and repoint them to the new server after a migration. This can be accomplished without Forescout itself needing an agent on the device and is controlled via a flexible policy engine which can be tailored for your unique environment and needs.

Extending Your Reach

For traditional IT devices that can be managed by an agent install, getting the required status for Essential Eight items is possible with multiple tools. But vulnerabilities exposed by operating systems and applications are not unique to IT devices alone. How do you extend those same practices to the growing number of IoT and OT devices on the network? Since they cannot be managed, this requires alternative methods to answer for operating system and application patch requirements.

Forescout solves for this problem by using both passive and active measures to determine both the identity of the device as well as the risk it poses by finding out what firmware, open services, and configuration it has. Forescout's uses Deep Packet Inspection of traffic it sees to extract the firmware, services, and protocol versions of IoT and OT devices then associate them to known vulnerabilities. Patch solutions and mitigation suggestions are also provided. Active scanning can also be enabled to provide added device context that might not be obtained from traffic alone.

Connecting the Dots

As there is no single system which will cover all your Essential Eight requirements this will naturally lead to multiple sources of events for security teams to digest and make sense of. This can place a heavy burden on already strained resources tasked with filtering through the stream of alerts to find critical incidents.

Forescout's Threat Detection & Response (TDR) helps focus attention to where it's needed the most by identifying high fidelity threats to your organisation. Forescout TDR is an extended detection and response solution that automatically and intelligently correlates threat signals from across the entire enterprise – campus, remote, data centre, cloud, IT/IoT/OT and medical devices – to quickly generate high-fidelity, high-confidence detections for analyst investigation.

Achieving Compliance

In addition to helping overcome these key challenges, the Forescout platform provides a solution for many individual requirements of the Essential Eight.

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

CATEGORY	HOW FORESCOUT HELPS
Patch Applications	*Regularly apply updates to address software vulnerabilities.* ▸ 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.
Patch Operating System	*Keep operating systems up to date with the latest security patches.* ▸ 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. ▸ 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. ▸ Detect the firmware versions of unmanaged IoT devices, as well as list any vulnerabilities and instructions to resolve.
Multi-Factor Authentication	*Requires multiple verification factors for secure system access.* ▸ 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. ▸ Ingest logs from MFA services and correlate with other security events to identify high fidelity threats.
Restrict Administrative Privileges	*Minimizes access to administrative accounts, reducing the impact of compromised credentials or phishing.* ▸ 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. ▸ Restrict devices with privileged account users logged in from accessing the internet, using email or web services. ▸ Audit local privileged account assignments and also detect if logged-in. ▸ Identify privileged operating system use and alert if found in unprivileged environment. ▸ Analyse security logs to uncover significant threats.
Application Control	*Ensures only approved software can run, reducing the risk of malicious code execution.* ▸ Continuously monitor the Application Control compliance status on every managed endpoint, ensuring each one is using the expected policies. ▸ Check Enforcement Agents are installed and running. ▸ Correlate application control alerts with other security events to initiate incident workflows.
Restrict Microsoft Office Macros	*Limits macro functionality to mitigate risks from malicious code.* ▸ 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. ▸ Ensure devices with privileged account users logged in are not accessing the internet, using email or web services.
User Application Hardening	*Disables unnecessary features to reduce exploitable vulnerabilities.* ▸ 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. ▸ Integrate with third-party endpoint management solutions like Ivanti and ManageEngine.
Regular Backups	*Ensures data backups to facilitate recovery in case of a breach or data loss.* ▸ 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 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