Risk-Based Approach to the Australian Signals Directorate Essential Eight.

Mapping Essential Eight to the Forcepoint Security Platform

Forcepoint

Whitepaper

forcepoint.com

Table of Contents

03 Introduction

03 What is the Essential Eight?

06 What is Forcepoint ONE Security Service Edge (SSE) Platform?

06 Forcepoint alignment with the ASD Mitigation Strategies and Essential Eight

06 How does Forcepoint's Risk-Based approach help organisations improve security maturity?

Introduction

This document is developed to help customers understand Forcepoint's Security Platform capabilities and how they map to the Australian Cyber Security Centre's (ACSC) Australian Signals Directorate (ASD) Essential Eight Mitigation Strategies.

The ACSC is based within the ASD and is responsible for providing advice and information about foreign signals intelligence, cyber security excellence and how to protect your business online.

Forcepoint has a comprehensive portfolio of integrated security technologies aligned with the Secure Access Service Edge (SASE), Security Service Edge (SSE) and Zero Trust architectures.

What is the Essential Eight?

Essential Eight are baseline mitigation strategies from the ACSC's Strategies to Mitigate Cybersecurity Incidents. This baseline makes it much harder for adversaries to compromise systems.

Essential Eight constitute the following mitigation strategies:

1. Control use of application (application control)
2. Manage application vulnerability (patch application)
3. Removing or disabling active content from Microsoft documents and PDF (configure Microsoft Office macro settings)
4. User application hardening for attack surface reduction
5. Control privileged access (restrict administrative privileges)
6. Manage OS vulnerability (patch operating systems)
7. Use of SSO and Identity Management (Mutifactor authentication)
8. Perform regular backups

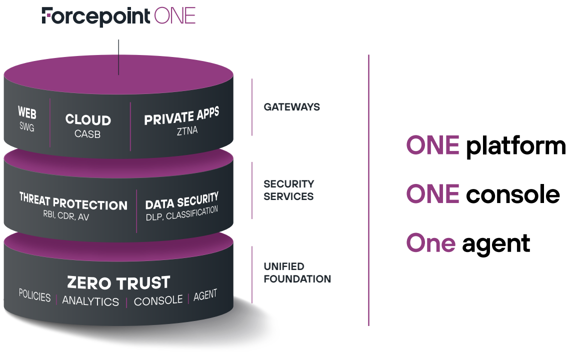
What is Forcepoint ONE Security Service Edge (SSE) Platform?

The Forcepoint ONE SSE Platform delivers comprehensive coverage in the cloud. It is SaaS protection that keeps users and data safe across your entire enterprise.

Forcepoint ONE brings all-in-one cloud security together in the fight against complexity, eliminating the need for patchwork solutions and simplifying security for the hybrid workplace.

It is one platform that unites Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) and Zero Trust Network Access (ZTNA) services alongside additional advanced capabilities such as Remote Browser Isolation (RBI), Content Disarm & Reconstruction (CDR) and Data Loss Prevention (DLP).

Welcome to the power of one



Forcepoint ONE

WEB SWG | CLOUD CASB | PRIVATE APPS ZTNA — GATEWAYS

THREAT PROTECTION RBI, CDR, AV | DATA SECURITY DLP, CLASSIFICATION — SECURITY SERVICES

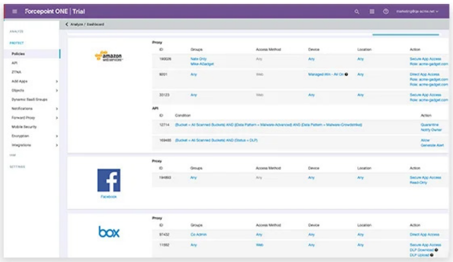
ZERO TRUST POLICIES | ANALYTICS | CONSOLE | AGENT — UNIFIED FOUNDATION

ONE platform

ONE console

One agent

→ **Protect cloud and private apps**
Give users easy access to the apps they need, without exposing the rest of the network. Enforce consistent threat protection and DLP across cloud and private apps to prevent malware and preserve sensitive data.



Forcepoint ONE | Trial

Analyze / Dashboard

amazon web services — Proxy

ID	Groups	Access Method	Device	Location	Action
190026	Nate Only Mike-AGadget	Any	Any	Any	Secure App Access Role: acme-gadget.com
8001	Any	Web	Managed Win - AV On	Any	Direct App Access Role: acme-gadget.com Role: acme-gadget.com
30123	Any	Web	Any	Any	Secure App Access Role: acme-gadget.com

API

ID	Condition	Action
12714	(Bucket = All Scanned Buckets) AND (Data Pattern = Malware-Advanced) AND (Data Pattern = Malware-Crowdstrike)	Quarantine Notify Owner
169485	(Bucket = All Scanned Buckets) AND (Status = DLP)	Allow Generate Alert

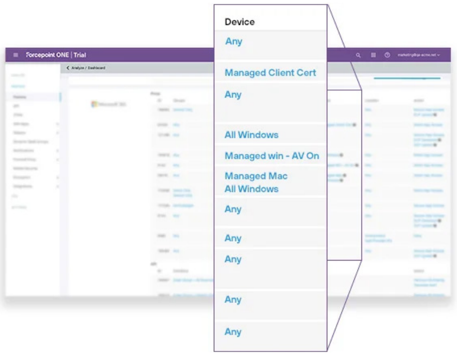
Facebook — Proxy

ID	Groups	Access Method	Device	Location	Action
194893	Any	Any	Any	Any	Secure App Access Read-Only

box — Proxy

ID	Groups	Access Method	Device	Location	Action
97432	Co Admin	Any	Any	Any	Direct App Access
11592	Any	Web	Any	Any	Secure App Access DLP Download DLP Upload

→ **Security for any device**
Consistently protect sensitive data in use across managed and unmanaged devices with agentless or agent-based security, all from one console.



Forcepoint ONE | Trial

Device

Any

Managed Client Cert

Any

All Windows

Managed win - AV On

Managed Mac
All Windows

Any

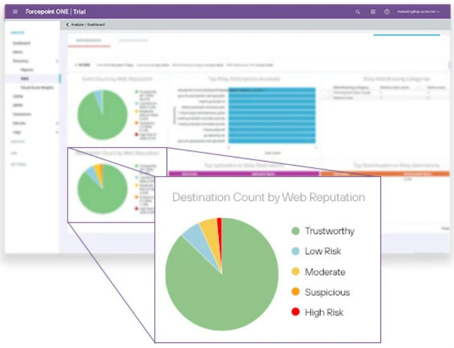
Any

Any

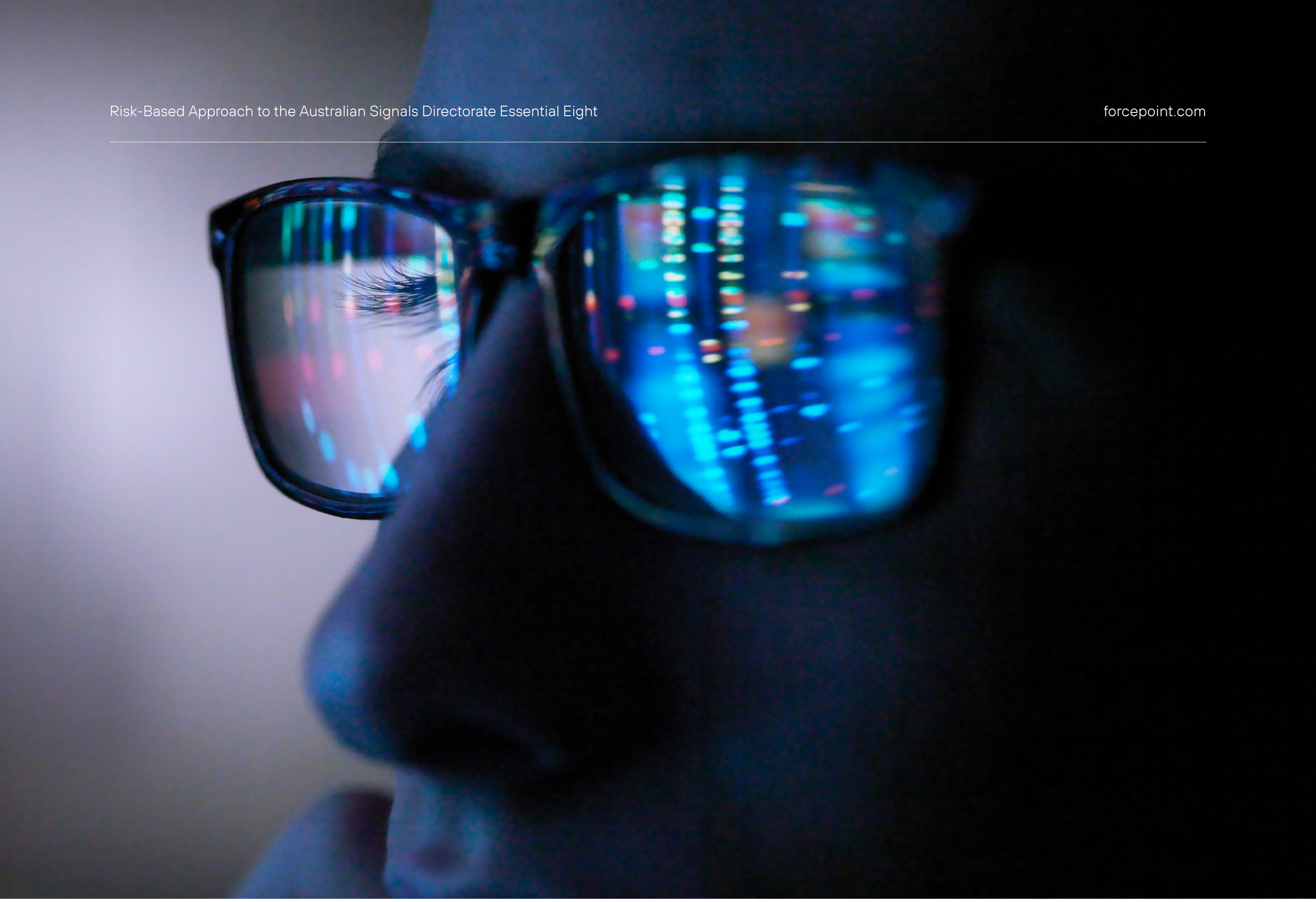
Any

Any

→ **Focus on risky traffic**
Intelligently enforce security as close to the resource and user as possible based on the level of risk. Decryption, inspection, and enforcement all work to provide protection without impacting the user's experience.



Forcepoint ONE | Trial



Forcepoint alignment with the ASD Mitigation Strategies and Essential Eight

Forcepoint has included responses to each of the ASD Mitigation Strategies describing how the Forcepoint ONE security platform maps to each one.

Reference is made to the Mitigation Strategy Maturity Level achieved or supported by Forcepoint ONE, as referenced in the ASD Essential eight maturity model publication.

Reference is also made to the “Essential Eight to ISM Mapping” document available here.

While this document provides a high-level response, Forcepoint ONE provides a comprehensive integrated cyber security capability that can assist organisations in mitigating a broad range of cyber security incidents.

Organisations that are reviewing their cyber security mitigation strategies should refer to the additional information provided by the ASD here. This provides organisations with detailed strategies to mitigate high impact cyber security incidents.

RELATIVE SECURITY EFFECTIVENESS RATING	MITIGATION STRATEGY	FORCEPOINT RESPONSE
Essential	**Application allow listing** of approved/trusted programs to prevent execution of unapproved/ malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	**Forcepoint ONE** With more and more organisation moving towards cloud adoption and adopting SaaS based applications it is becoming difficult for organisation to get visibility and control on which applications are using. This problem is elevated as BYOD is becoming more common. Protecting organisations data and application is top concerns. Forcepoint ONE give users easy access to the apps they need, without exposing the rest of the network. Enforce consistent threat protection and DLP across cloud and private apps to prevent malware and preserve sensitive data. Consistently protect sensitive data in use across managed and unmanaged devices with agentless or agent-based security, all from one console. Intelligently enforce security as close to the resource and user as possible based on the level of risk. Decryption, inspection, and enforcement all work to provide protection without impacting the user's experience. → Gain visibility and control of hybrid workers' interactions with data in web, cloud, and private apps. → Prevent misuse of sensitive data accessed from managed or unmanaged devices. → Control access to high-risk web content. → Provide remote, fast secure access to business resources and private apps without the complexity of VPNs.
		Forcepoint Next Generation Firewall (NGFW) Forcepoint Endpoint Context collects crucial endpoint metadata such as user, application and network information and sends it to NGFW. Forcepoint endpoint security solution gives administrators granular control over which users and applications access what data, making access policies smatter and human centric. Endpoint Applications can be blocked from accessing the network based on the trusted signing authority. eg. Application Control: NGFW blocks access to browsers such as portable Google Chrome and Firefox and allows only Microsoft Internet Explorer to connect to internet. eg. Putty.exe can be blocked from establishing connection by Endpoint Application control policy.
		Forcepoint Remote Browser Isolation (RBI) Forcepoint RBI can provide users with a safe "Zero-Trust" browsing experience by "air-gapping" user devices from websites by removing direct interaction with malware present on webpages and web-based applications. Malware is often delivered through compromised files that are supported by "approved/trusted" applications. For example, a Microsoft Office document containing a malicious macro. Forcepoint's RBI solution also provides Content Disarm & Reconstruction (CDR) capability to sanitise files as they are downloaded from the web. When configured to allow downloads, only the clean file is delivered, with any potentially malicious code removed. In conjunction with Forcepoint RBI, CDR provides comprehensive malware protection for both web browsing activities and file downloads. Users' data sharing activities can be limited, such as embedded email URLs being rendered in read-only mode to prevent data loss and credential theft from phishing attacks. Additionally, web applications accessed via the solution do not leave sensitive corporate data in the browser caches of endpoints.

RELATIVE SECURITY EFFECTIVENESS RATING	MITIGATION STRATEGY	FORCEPOINT RESPONSE
Essential	**Patch applications** e.g., Flash, web browsers, Microsoft Office, Java, and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.	**Forcepoint Next Generation Firewall (NGFW)** Forcepoint NGFW IPS capability provides robust protection against application vulnerabilities. It uses advanced technologies, such as Deep Packet Inspection, to protect against exploits. This feature of NGFW provides mitigation strategy against unpatched vulnerabilities – or, at the least, provides protection between patch availability and patch deployment.
		Forcepoint Remote Browser Isolation (RBI) Web browsers are a specific target for compromise. Organisations often have multiple browser platforms and versions within their organisation, both sanctioned and unsanctioned. The ISM (Security Control: 1144; Revision: 9) refers to the patching of drivers and applications assessed as an extreme risk and as a "must" to be patched, updated, or mitigated within 48 hours. For example, Chrome Stable version 87.0.4280.141 was rolled out with 16 security fixes of which 15 were rated as high-severity – prompting the US United States Cyber and Infrastructure Security Agency (CISA) to warn organisations. With web browsers installed across a growing number of endpoints – and often removed from the organisation's network – the ability to patch browser applications within 48 hours is a challenging task. Combine this with the introduction of BYOD devices, which can have access to organisations' information assets and networks, and this attack surface becomes even wider and more difficult to secure. RBI provides real-time protection against web browser compromise, as the user does not interact directly with websites and web applications. This removes the risks associated with security vulnerabilities. Users' data sharing activities can be limited, such as embedded email URLs being rendered in read-only mode to prevent data loss and credential theft from phishing attacks. Additionally, web applications accessed via the solution do not leave sensitive corporate data in the browser caches of endpoints.

RELATIVE SECURITY EFFECTIVENESS RATING	MITIGATION STRATEGY	FORCEPOINT RESPONSE
Essential	**Configure Microsoft Office macro settings** to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.	**Forcepoint Zero Trust Content Disarm and Reconstruction (CDR)** We have witnessed again and again that the attackers take advantage of vulnerabilities within the software's i.e. Microsoft Office, Microsoft Windows, Adobe PDF to gain access to data, launch malicious programs including exe, dlls, scripts etc. We know detection-based defences alone simply can't keep up. Content Disarm and Reconstruction stops known and unknown threats, zero-day attacks and malware. Forcepoint's Zero Trust Content Disarm and Reconstruction (CDR) is different. Rather than trying to detect malware, it assumes nothing can be trusted. It works by extracting the valid business information from files (either discarding or storing the originals), verifying the extracted information is well-structured, and then building new, fully functional files to carry the information to its destination. Zero Trust CDR is a game-changer for mitigating against the threat of even the most advanced zero-day attacks and exploits. Forcepoint Zero Trust CDR stops file-based malware from entering the organisation without using detection. Due to the unique way that Zero Trust CDR just extracts and delivers what is good in a file and doesn't try to detect what is bad, it protects users from even zero-day and totally unknown malware. This approach to preventing malware doesn't need constant updating with the signatures of the latest new and zero-day malware as they become available, so the defence is always up to date.
		Forcepoint RBI Forcepoint RBI can provide users with a safe "Zero-Trust" browsing experience by "air-gapping" user devices from websites by removing direct interaction with malware present on webpages and web-based applications. Malware is often delivered through compromised files that are supported by "approved/trusted" applications. For example, a Microsoft Office document containing a malicious macro. The ISM (Security Control: 1488; Revision: 0) requires as a "must" that Microsoft Office macros in documents originating from the internet are blocked. Forcepoint's RBI solution also provides Content Disarm & Reconstruction (CDR) capability to sanitise files as they are downloaded from the web. When configured to allow downloads, only the clean file is delivered, with any potentially malicious code removed. In conjunction with Forcepoint RBI, CDR provides comprehensive malware protection for both web browsing activities and file downloads. Users' data sharing activities can be limited, such as embedded email URLs being rendered in read-only mode to prevent data loss and credential theft from phishing attacks. Additionally, web applications accessed via the solution do not leave sensitive corporate data in the browser caches of endpoints.

RELATIVE SECURITY EFFECTIVENESS RATING	MITIGATION STRATEGY	FORCEPOINT RESPONSE
Essential	**User application hardening.** Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g., OLE), web browsers and PDF viewers.	**Forcepoint Next Generation Firewall (NGFW)** Forcepoint Endpoint Context collects crucial endpoint metadata such as user, application and network information and sends it to NGFW. Forcepoint endpoint security solution gives administrators granular control over which users and applications access what data, making access policies smatter and human centric. Endpoint Applications can be blocked from accessing the network based on the trusted signing authority. eg. Application Control: NGFW blocks access to browsers such as portable Google Chrome and Firefox and allows only Microsoft Internet Explorer to connect to internet. eg. Putty.exe can be blocked from establishing connection by Endpoint Application control policy.
		Forcepoint RBI Organisations often have multiple browser platforms and versions within their organisation, both sanctioned and unsanctioned. The ISM (Security Control: 1144; Revision: 9) refers to the patching of drivers and applications assessed as extreme risk as a "must" to be patched, updated or mitigated within 48 hours. For example, Chrome Stable version 87.0.4280.141 was rolled out with 16 security fixes of which 15 were rated as high-severity – prompting the US United States Cyber and Infrastructure Security Agency (CISA) to warn organisations. With web browsers installed across a growing number of endpoints – and often removed from the organisation's network – the ability to patch browser applications within 48 hours is a challenging task. Combine this with the introduction of BYOD devices, which can have access to organisations' information assets and networks, and this attack surface becomes even wider and more difficult to secure. Forcepoint RBI provides real-time protection against web browser compromise, as the user does not interact directly with websites and web applications. This removes the risks associated with security vulnerabilities. Users' data sharing activities can be limited, such as embedded email URLs being rendered in read-only mode to prevent data loss and credential theft from phishing attacks. Additionally, web applications accessed via the solution do not leave sensitive corporate data in the browser caches of endpoints.

RELATIVE SECURITY EFFECTIVENESS RATING	MITIGATION STRATEGY	FORCEPOINT RESPONSE
Essential	**Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Do not use privileged accounts for reading email and web browsing.	**Forcepoint ONE** can enforce user-based policies for any application on any device (including BYOD). This feature is effective in controlling access to internal or external business applications and to provide high visbility of data movement, as well as visibility of users and devices. Forcepoint ONE's data management pane can enforce restrictions to data-based user, device, location, etc. For example: a Domain Admin outside of approved locations should not have access to critical applications. **Forcepoint RBI** The Essential Eight Maturity Model includes the following requirement for level three maturity - "Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services" Forcepoint RBI can be used to protect privileged users with a safe "Zero- Trust" browsing experience by "air-gapping" users' devices from websites, thereby removing direct interaction with malware present on webpages and web-based applications from a user's device. A privileged user's web browsing can be limited to read-only mode to prevent data loss and credential theft from phishing attacks. Additionally, web applications accessed via the solution do not leave sensitive corporate data in the browser caches of endpoints.
Essential	**Patch operating systems.** Patch/ mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Do not use unsupported versions.	**Forcepoint Next Generation Firewall (NGFW)** Forcepoint NGFW IPS capability provides robust protection against application vulnerabilities. It uses advanced technologies, such as Deep Packet Inspection, to protect against exploits. This feature of NGFW provides mitigation strategy against unpatched vulnerabilities – or, at the least, provides protection between patch availability and patch deployment.
Essential	**Multi-factor authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high- availability) data repository.	**Forcepoint ONE** provides full integration capabilities with MFA providers ie. OKTA, DUO, RSA. However, Forcepoint ONE has internal IDP with full MFA built into the platform with capabilities to send tokens to mobile devices or integrate Google, MS Authenticator. With contextual access, organisations have ability to Grant user access to Forcepoint ONE based on user group, device type, location, or time of day. Optional escalation to Multi-factor Authentication based on "impossible travel," unauthorized location, or unknown device. Additional layer of access control for individual websites or applications based on user group, device type, or location.
Essential	**Daily backups** of important new/ changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.	**Not Applicable**

How does Forcepoint’s Risk-Based approach help organisations improve security maturity?

There will be circumstances (such as legacy systems and technical debt) that may prevent immediate or full implementation of requirements within the Essential Eight Maturity Model. In such cases, risk-based cybersecurity tools such as Forcepoint Dynamic User Protection platform may adequately address this.

Forcepoint’s Risk-Based approach help to deliver real results:

→ Gain better context and understanding of user intent by focusing on user behaviour and their interaction with data

→ Increase employee productivity with individualised data security so low risk users can proceed as usual while limiting high risk user activity

→ Minimize false positives with a graduated approach to policy enforcement based on risk level so practitioners don’t experience alert overload

→ Enable safe collaboration on cloud applications by gaining insights to user engagement with cloud data

→ Investigate risk from insiders with efficiency and ease

Forcepoint ACE inspects traffic content and usage patterns using up to eight different defence assessment areas for identifying malware, phishing, spam, and other risks to the enterprise. The eight defence assessment areas that comprise ACE are:

→ **Real-Time Security Classification:** Inspects all traffic content for malicious or suspicious code such as obfuscated scripts and iframe tags that often hide malware behind dynamic content.

→ **Real-Time Content Classification:** Employs advanced machine learning to quickly and accurately classify web pages into highly granular content categories for effective access filtering.

→ **URL Classification:** Applies current classification information for known web pages, and assesses new pages and links based on associated sites and redirections.

→ **Behavioural Sandboxing:** Allows suspicious files to be executed and evaluated for malicious activities in a secure sandbox which emulates a real machine down to the processor and memory layers.

→ **Anti-Malware Engines:** Applies state-of-the-art antimalware protection capable of proactively blocking the latest in binary and script-based threats.

→ **Anti-Spam/Phishing:** Provides proactive protection against high volume spam and Phishing campaigns, as well as email-borne threats.

→ **Reputation Analysis:** Reputation databases (both third-party and Forcepoint proprietary) are applied to emails and URLs to block web and email traffic from untrustworthy sources.

→ **Real-Time Data Classification:** Classifies structured and unstructured data with parsing and decoding support to address outbound data theft.

Additional References

- → **Website –** Forcepoint Remote Browser Isolation
- → **Solution Brief –** Forcepoint Remote Browser Isolation
- → **Technical Report –** Forcepoint RBI - File Content Sanitisation for Thwarting Malware
- → **Forcepoint Use Case –** Remote Browser Isolation for Government Agencies
- → **Website –** Forcepoint Advanced Malware Detection
- → **Solution Brief –** Forcepoint Advanced Malware Detection (AMD)
- → **Website –** Forcepoint NGFW
- → **CyberRating 2022 Report –** Forcepoint NGFW CyberRating 2022 Report
- → **Website –** Forcepoint Zero Trust Content Disarm and Reconstruction
- → **Solution Brief –** Zero Trust CDR for Email
- → **Solution Brief –** Zero Trust CDR for Web Gateways
- → **Solution Brief –** Zero Trust CDR for Portal Protection

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP-Risk-Based Approach to the ASD Essential Eight-Whitepaper-US-EN] 26Sept2022