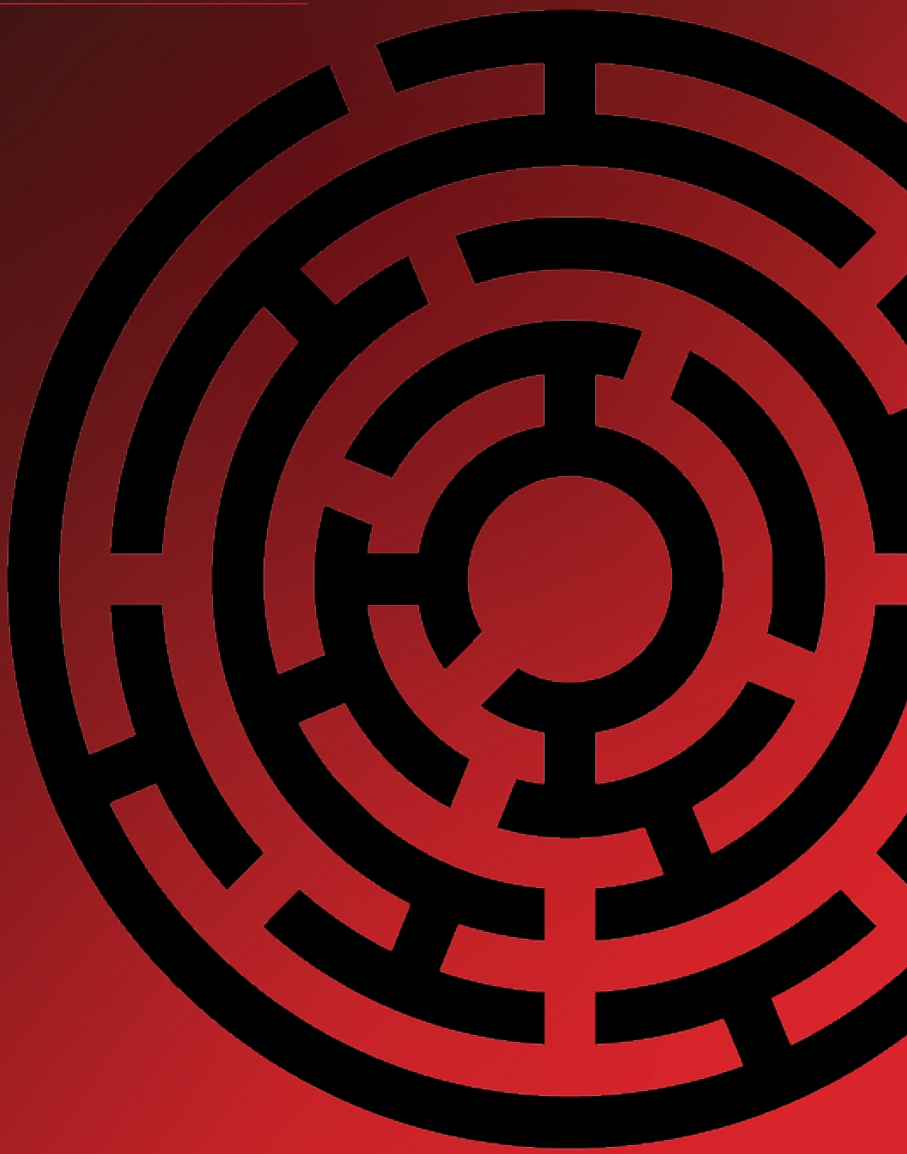
Aligning with the Cyber Assessment Framework

Hard for Hackers.
Simpler for you.



November 2024
Trend Micro

Contents

Published by
Trend Micro

Contributors
Jon Askew
Simon Walsh

Executive Summary

The public sector faces a continuously evolving threat landscape. Already one of the most targeted industries, the challenge is managing this risk with ever-reducing resources.

The National Cyber Security Centre (NCSC) has developed the Cyber Assessment Framework (CAF) to address this risk and help build cyber resilience. The CAF supports both the *U.K. Government Cyber Security Strategy 2022-2030*, and the *Cyber Strategy to 2030 for Health and Adult Social Care*. The CAF covers four objectives and 14 underpinning principles. They highlight: the proactive strategy required for effective cybersecurity; the need to manage security risk across an organisation; the importance of detection in order to reduce time to respond; and how to minimise the impact of cybersecurity incidents.

The NCSC has developed the CAF with a focus on securing network and information systems critical to society's fundamental functions. The reliability and security of these systems are crucial for activities ranging from healthcare provision to transportation safety. Given the escalating frequency and impact of cybersecurity incidents targeting essential functions, the CAF underscores the need to enhance the security of UK network and information systems. Referenced by the NCSC are the WannaCry ransomware attack and attacks on critical infrastructure in Ukraine and the United States; examples highlighting the potential severe consequences of compromised systems.

How can Trend Micro support alignment to the CAF?

Trend Micro is a global cybersecurity provider with over 35 years of experience. We serve more than 500,000 customers worldwide and are trusted by nine of the top 10 Fortune 500, 6 of the top 10 healthcare providers, and all of the top 10 global financial institutions. Trend Micro has a proven history of working with the UK public sector and is experienced in helping to manage the unique challenges the industry faces.

Our solutions cover all layers of the IT environment, from email and endpoint to networks, servers and hybrid cloud environments. We focus on streamlining capabilities by offering as many as possible from a single platform. And our optional SaaS delivery mechanism helps to further simplify security for customers.

Our Trend Vision One™ platform delivers a comprehensive and proactive approach cybersecurity. It equips customer IT teams with intuitive applications that detect, hunt, investigate, analyse and respond to risks and threats at every stage of the lifecycle. The platform automatically identifies and prioritises risks and vulnerabilities, which helps reduce the volume of daily security alerts and simplifies security operations.

Summary of the NCSC CAF Objectives

The CAF features four objectives, with 14 underpinning principles and multiple indicators of good practice. It has an outcome-based approach to improving cybersecurity and resilience. The intent is not to produce a cybersecurity "to-do" list but to influence top-level outcomes that indicate good cybersecurity:

Objective A – Managing Security Risk

Emphasises the need to establish robust policies and processes to improve cybersecurity and cyber resilience. Security measures should be driven by organisational management, with clear governance structures. Central to this is the requirement to identify, assess and understand cybersecurity risk; with a view of the threat landscape and vulnerabilities across the infrastructure. Implementing systematic processes ensures that risks are identified and managed, with the organisation having confidence in the effectiveness of mitigations.

Objective B – Protecting Against Cyber-attack

The organization establishes, communicates and enforces policies and processes to secure systems and data supporting essential functions. It manages access, ensuring users are properly verified, authenticated and authorised. Electronic data is safeguarded against unauthorised access, modification or deletion. The organisation shields network and information systems critical for essential functions from cyber-attacks, informed by a robust understanding of associated risks. Resilience against cyber-attacks is integrated into system design, implementation, operation and management. Staff are equipped with awareness, knowledge and skills to effectively contribute to the security of network and information systems supporting essential functions.

Objective C – Detecting Cybersecurity Events

The focus is on the ability to identify, recognise and respond to cybersecurity incidents. Emphasis is on detection capabilities for rapid response to threats, and having the ability to detect and respond to threats which evade standard signature-based security solutions. This objective covers the requirement for a proactive cybersecurity strategy, constantly monitoring the environment for signs of malicious activity and taking measures to respond. The integrity and availability of essential functions is assured through taking a proactive approach to security.

Objective D – Minimising the Impact of Security Incidents

Cyber resilience is a recurring theme across the CAF, and this objective highlights the requirement to be able to continue operations and recover quickly in the event of a successful cyber-attack. Highlighted is the need for an incident response plan, the ability for security tools to highlight high-fidelity alerts, and sufficient resilience in the event of a physical failure in network and information systems.

How can Trend Micro support your CAF compliance journey?

Objective A: Managing Security Risk

Appropriate organisational structures, policies and processes in place to understand, assess and systematically manage security risks to network and information systems supporting essential functions.	
CAF PRINCIPLE	**HOW TREND WILL SUPPORT YOUR ADHERENCE TO THE PRINCIPLE**
A1: Governance Putting in place the policies and processes which govern your organisation's approach to the security of network and information systems. Trend Vision One Trend Service One	The Trend Vision One cybersecurity platform synthesises attack surface management telemetry to intuitively surface an at-a-glance understanding of your company-wide security posture, benchmarks and trends over time. In addition, your team is given the opportunity to examine and filter assets, vulnerabilities and key metrics in more detail. The platform's Risk Insight capability offers central visibility into the attack surface inventory, cyber risk score, vulnerable assets, predicted impact, operations efficiency and recommended remediation tactics. This delivers a single source of truth for security leaders, security operations and IT operations across your organisation, allowing you to observe and evaluate your entire IT environment at varying and appropriate levels of detail. Trend Service One™ augments your existing team with 24/7/365 managed detection, response and support. Featuring on-demand training, best practices guides and access to cybersecurity and CISO experts, Trend Service One enables you to go further even with limited in-house resources. The service bolsters your existing policies and processes via a dedicated Service Manager. Trend threat analysts notify you of high-risk alerts and guide you through the appropriate response actions, and monthly security reports prevent future attacks. And if needed, Trend's Incident Response Team will investigate breaches guide and support you through the recovery process. Service One is designed to be a part of your vendor management process and has predefined check points, such as a status meeting, security meeting, vendor relationship check-in, and structured reporting and service reviews. It provides an opportunity for a formal service performance review at least once per quarter. This review examines service performance, significant events such as incidents, faults, submitted cases, change requests, executions, and recommendations.
A2: Risk Management Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management. Trend Vision One – Attack Surface Risk Management	Proactive risk management stops breaches before they happen. Featuring the most robust attack surface management capabilities encompassing cloud, hybrid, and on-premises environments, the Trend Vision One Attack Surface Risk Management capability combines continuous attack surface discovery, real-time risk assessments and prioritisation, and automated mitigation actions to dramatically reduce your risk exposure. The platform eliminates blind spots and reduces the attack surface with cutting-edge internal and external continuous asset discovery. It pinpoints users, internet-facing domains, IPs, cloud apps, cloud storage, containers and workloads across internet-facing and internal corporate networks. Post-asset discovery, the platform leverages continuous real-time risk assessments to focus your team's efforts, allowing you to prioritise remediation actions with automatically generated custom recommendations to help address identified risks. **Trend's single platform approach allows already-stretched resources to do more with less.** Reduce your tool sprawl and improve efficiencies by bringing multiple capabilities like External Attack Surface Management (EASM), Cyber Asset Attack Surface Management (CAASM), Vulnerability Prioritisation, and Cloud Security Posture Management (CSPM) together in a single, easy-to-use solution. Trend's approach is comprehensive, combining accurate and comprehensive views of your risk exposure from the combined power of native sensors, third-party sources, industry-leading threat research, and intelligence analysed against the most extensive set of risk factors across cloud, hybrid, and on-premises environments.

A3: Asset Management Determining and understanding all systems and/or services required to maintain or support essential functions. Trend Vision One – Attack Surface Risk Management Trend Vision One - XDR	Featuring the most robust attack surface management capabilities encompassing cloud, hybrid, and on-premise environments, Trend Vision One Attack Surface Risk Management (ASRM) delivers continuous asset discovery of endpoints and servers, internet-facing domains, IPs, cloud apps, cloud storage, containers, and workloads across internet-facing and internal corporate networks, detailing which may be exposed to attack. This enables you to focus on mitigating attacks before they happen. Trend's XDR also extends to the network, providing a low cost, lightweight, easily deployed network sensor which further increases asset visibility by correlating network telemetry with other security vectors such as endpoints and workloads. This helps to identify potential threats—exposing the unmanaged parts of the attack surface by seeing into all network assets, including devices not protected by an agent. XDR for Networks collects and correlates deep activity data for single and multiple vectors including email, endpoints, servers, cloud workloads and networks. That enables a level of threat hunting and investigation analysis that is difficult or impossible to achieve otherwise, all presented via a single console.
A4: Supply Chain Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers. Trend Vision One – Threat Intelligence Trend Vision One – Attack Surface Risk Management	Trend Vision One Threat Intelligence app provides detailed information about global threat actors, events and campaigns, providing insight into threat activity relevant to the external suppliers you work with. Both Trend-curated and custom threat intelligence reports are supported. Either way, your data will be automatically swept for Indicators of Compromise (IoCs) matching those reports, providing you with alerts where matches are found—an early indicator of possible supply chain compromise. Top targeted countries, regions, and industries are detailed, alongside detailed intelligence data including: ▪ Threat actor pseudonyms ▪ Industry-standard MITRE Tactics, Techniques, and Procedures ▪ Tools exploited by the selected threat actor ▪ Malware used by the selected threat actor ▪ CVEs associated with the selected threat including the CVE number, CVE description and affected operating systems ▪ IoCs including URLs and file hashes **Trend Vision One External Attack Surface Risk Management app can look beyond your environment to those of the external suppliers you work with,** identifying exploitable weaknesses and vulnerabilities found in internet- and other external-facing assets, including cloud. The app will also provide recommendations on how to address those weaknesses and vulnerabilities; information which can be shared with trusted third parties. Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers requires an understanding of not just the third-party vendors you work with, but also the third-party code you integrate into your applications. Most application code is third-party open source and widely reused, which can pose significant risk when found to contain vulnerabilities. Trend can address this risk by increasing visibility into security risks hidden in open-source code and strengthening the security procedures that affect application development and productivity. Trend identifies vulnerabilities in dependencies and sub-dependencies, monitors continuously for zero-day vulnerabilities in cloud-native projects and legacy applications, improves application development, enhances security governance, and provides continuous visibility and recommendations to security teams.

Objective B: Protecting Against Cyber-attack

Proportionate security measures are in place to protect the network and information systems supporting essential functions from cyber-attack.	
CAF PRINCIPLE	**HOW TREND WILL SUPPORT YOUR ADHERENCE TO THE PRINCIPLE**
B1: Service Protection Policies and Processes Defining and communicating appropriate organisational policies and processes to secure systems and data that support the operation of essential functions. Trend Service One Trend Incident Response	Trend Service One augments your existing people, processes, and technology with 24/7/365 managed detection, response and support. Service One includes: **Designated Service Manager:** With Trend Micro Service One Complete, your designated Service Manager is committed to providing the most optimised experience of your Trend Micro solutions. Your Service Manager answers all inquiries, enabling you to get the most out of your Trend Micro solutions, and facilitates access to cybersecurity, solution and subject matter experts. **Incident Response Team:** The Trend Micro Incident Response Team is a specialised service that combines cyber crisis management, state-of-the-art threat hunting expertise, digital forensics, and sound professional advice. This specialised team is critical for enterprises managing troves of valuable data, as well as those required to meet several local and global compliance requirements. Specially trained to prioritise, investigate, and fulfil compliance obligations, the Incident Response Team can help organisations avoid legal, financial and customer-relationship issues. Customers also gain access to cybersecurity and CISO advisory experts.
B2: Identity and Access Control Understanding, documenting and controlling access to networks and information systems supporting essential functions. Trend Vision One	Identity and access control are crucial components of cybersecurity, playing a pivotal role in safeguarding an organisation's digital assets, sensitive information, and overall system integrity. They form a critical layer of defence against unauthorised access, insider threat, and data breaches. Implementing effective identity and access management (IAM) practices is essential for maintaining the confidentiality, integrity and availability of an organisation's data and systems. Identity and access controls are a core capability within the Trend Vision One platform. Alongside Trend's native capabilities, the platform also integrates into third-party identity management ecosystems including Active Directory, Microsoft Entra ID, Google Cloud Identity, Okta, and OpenLDAP. This combination of native and third-party capabilities enables the platform to highlight, report and alert on identity-related risks including: ▪ Accounts with weak authentication ▪ Accounts that increase attack surface risk ▪ Accounts with excessive privilege ▪ Accounts using legacy authentication protocols ▪ Account activity by location Trend Vision One also includes a dedicated Identity Posture app, **enabling you to quickly review your organisation's identity-related assets that might be exposed to attack,** and identify risk events that weaken your security posture. Key app capabilities include: ▪ Identity infrastructure discovery (how many privileged users, shadow admins, regular users) ▪ Identity threats (AD / Entra attacks, compromised accounts, infrastructure exploitation) ▪ Identity hygiene (stale accounts, shared accounts, weak authentication, using unmanaged devices) ▪ Identity behaviour monitoring (abnormal sign-ins, unusual login location / IP / time, account login to unusual apps) **Information highlighted in the app includes:** **Identity Posture Overview:** Displays your organisation's overall identity posture risk level, the number of risk

	events that potentially impact your identity posture, and a historical chart of identity-related risk events. **Priority Risk Events**: Displays a list of identity-related risk events prioritised by real-time impact on the Risk Index. **Identity Summary:** Displays how many of each common identity-related asset types have been detected in your organisation's environment. **Highlighted Exposure Risk Events:** Displays risk events identified by Attack Surface Risk Management over the last seven days that have the biggest impact on your exposure. **Identity Behaviour Summary:** Displays the number of identity behaviour-related risk events and a historical chart of risk events. **Identity Behaviour Events:** Displays a list of identity behaviour-related risk events prioritised by real-time impact on your organization's Risk Index.
B3: Data Security Protecting stored or electronically transmitted data from actions that may cause an adverse impact on essential functions. Trend Vision One – Cloud Workload Security	In addition to the system security capabilities detailed below, Trend delivers data-specific security using a combination of Data Loss Protection (DLP), Integrity Monitoring, and Zero Trust. 1. **DLP** safeguards an organisation's confidential and sensitive data—referred to as digital assets—against accidental disclosure and intentional theft. DLP enables you to: ▪ Identify the digital assets to protect ▪ Create policies that limit or prevent the transmission of digital assets through common channels, such as email and external devices ▪ Enforce compliance to established privacy standards 2. **Integrity monitoring scans** for unexpected changes to files, registry values, registry keys, services, processes, installed software and ports. Using a baseline secure state as a reference, the Integrity Monitoring module performs scans on the above and logs an event (and an optional alert) if it detects any unexpected changes to your data or any other monitored objects. 3. To adopt a **Zero Trust strategy**, it is critical to continually assess the risk of identities, devices, applications, and data. This is achieved using telemetry from endpoints, email, directory services, XDR and other sources. Within Trend Vision One, the Zero Trust Risk Insights app helps decide how close the risk is to zero and prioritises issues as well as tracking the organisation's overall posture over time. The security posture of devices and users will be continually checked and monitored and where pre-defined thresholds are met, device and user access to your on-premises and cloud data will be blocked, ensuring your data remains secure at all times.
B4: System Security Protecting critical network and information systems and technology from cyber-attack. Trend Vision One – Attack Surface Risk Management Trend Vision One - XDR	**Trend has been securing network and information systems for 35+ years and remains a market leader**. While preventative controls such as anti-malware, phishing detection, and IPS form the bedrock of any security posture, Trend Vision One bolsters such capabilities with native XDR and Attack Surface Risk Management (ASRM). ASRM, as a proactive measure, is key to getting and staying one step ahead of any would-be attackers, enabling organisations to stop breaches before they happen. Featuring the most robust attack surface management capabilities encompassing cloud, hybrid, and on-prem environments, Trend's ASRM combines continuous attack surface discovery, real-time risk assessments and prioritisation, and automated mitigation actions to dramatically reduce your risk exposure. ASRM eliminates blind spots and reduces your attack surface with cutting-edge internal and external continuous asset discovery, pinpointing users, internet-facing domains, IPs, cloud apps, cloud storage, containers and workloads across internet-facing and internal corporate networks. It brings multiple capabilities together in a single easy-to-use solution including external attack surface management (EASM), cyber asset attack surface management (CAASM), vulnerability prioritisation, and cloud security posture management (CSPM). Trend Vision One provides XDR capabilities, stopping adversaries faster with a broader perspective and better context to hunt, detect, investigate, and respond to threats from a single platform. XDR provides early and precise detection, correlating low-confidence events across security vectors to quickly detect complex, multi-

	layer attacks. Activity telemetry is enriched with full context and understanding across security layers. Multiple rules, filters, and analysis techniques—including data stacking and machine learning—enable early, precise threat detection. Trend's native XDR includes: ▪ XDR for cloud extends detection and response to cloud accounts by examining user, service, and resource log activity for suspicious behaviour and providing remediation and response actions ▪ XDR for email extends detection and response to email accounts by examining user email, threat logs, and user behaviour to cross-correlate suspicious activity with additional intelligence to provide remediation and response actions ▪ XDR for endpoints and server provides deep visibility and threat prevention for endpoints and servers by automatically correlating data across multiple security layers, for faster detection, improved investigation and shorter response times ▪ XDR for networks empowers security teams with advanced AI/ML techniques, data correlation and workflows to address blind spots within your network's unmanaged attack surface ▪ XDR for OT extends detection and response to OT devices, and provides a holistic overview of OT and IT environments in a single platform—allowing organisations to obtain complete visibility of cyber threats, consolidated alerts, and incident view at both device and network levels. Trend's preventative controls are multi-layered and cover cloud, endpoints, servers, mobiles, email, network and OT. Threat detection capabilities include: High-fidelity machine learning detection of unknown malware, Behavioural analysis (against scripts, injection, ransomware, memory, and browser attacks), In-memory analysis for identification of fileless malware, Malicious URL blocking, Exploit prevention, Command and control (C&C) blocking, Data Loss Prevention, Device and application control, Malware and URL sandboxing, Network and host-based IPS, Breach detection. Trend's proactive and preventative technology is further enhanced by Trend Service One, augmenting your existing team with 24/7/365 managed detection, response, and support. **Combined, the above delivers:** ▪ Earlier detection: XDR improves your team's visibility and reduces silos to unearth threats evading detection by hiding in between security silos amid disconnected solution alerts ▪ Advanced correlation: By leveraging native and third-party data, your security team is enabled to deliver deep activity data—not just XDR detections—across endpoint, email, server, cloud workloads, and networks ▪ Optimised detection modelling: Threat intelligence incorporates more sources and research insight to enrich detection and investigation to deliver greater context to your team ▪ Faster investigation: By quickly visualising the full attack story, XDR automatically pieces together fragments of malicious activity across your security layers ▪ Complete response: Enacting embedded response options across multiple security layers enables your security team to prioritise, automate and accelerate response actions from one location
B5: Resilient Networks and Systems Building resilience against cyber-attack. Trend Vision One Zero Day Initiative	Trend Micro believes that managing your cyber risk is an integral part of your business strategy and ultimate success. Leveraging over 35 years of security expertise and technology foresight, Trend Micro is transforming the world of cybersecurity. Be your most resilient with: **A Platform Technology Strategy:** Rated a leader by Gartner, Forrester and IDC, our unified cybersecurity platform is continually evolving to address attack surface risk across the enterprise. Continuously discover your ever-changing attack surface, understand and prioritise vulnerabilities, rapidly detect and respond to threats, and apply the right security at the right time to mitigate risk. Built-in security capabilities like extended detection and response (XDR), risk insights, threat assessment and expert services help your security operations team to be more effective with fewer resources. Understanding the threat landscape is crucial, but effective risk prioritisation is paramount for true cyber resilience. Risk prioritisation allows optimal resource allocation,

	damage mitigation and business continuity. Trend Micro plays a pivotal role in enhancing cybersecurity resilience through a streamlined roadmap that includes establishing visibility across the digital estate, adopting a proactive attack surface management strategy, combining XDR with attack surface management, and securing the cloud transformation journey at every stage. **Global Threat Research:** Across our 16 global threat research centres, hundreds of security experts and data scientists are constantly gathering intelligence to better protect our customers. The Trend Micro Research team delivers 24/7 threat research from around the globe, vulnerability intelligence from our Zero Day Initiative (ZDI) program, and the latest insights on the cybersecurity landscape. The team also works closely with government and law enforcement agencies, including Interpol, the United Nations, the FBI and the US Department of Homeland Security. **People Driven by Passion:** ▪ Security experts with unique core values: With a non-stop focus on protecting customers through world-class security technologies and support, Trenders embody our core principles of customer value, collaboration, change, innovation and trustworthiness. ▪ People focused on making the world better: We educate thousands of small businesses and universities, as well as millions of kids and families around the world, on how to be safe in our connected world. And our Global Citizenship and Give & Match programs help communities in need around the world.
B6: Staff Awareness and Training Appropriately supporting staff to ensure they make a positive contribution to the cybersecurity of essential functions. Trend Micro – Phish Insight	Trend Micro's phishing awareness tool – Phish Insight – enhances information security awareness for your organisation by empowering people to recognise and protect themselves against the latest email threats, effectively reducing the risk of human error. Phish Insight provides: ▪ **Automated and Realistic Simulations:** With just a few clicks, set up your campaign to run monthly or quarterly. Choose from Phish Insight's exclusive templates extracted from real phishing scams and make your campaign more authentic by randomising the delivery pattern. ▪ **Customisable Training Programs:** Phish Insight hosts a wide variety of high-quality training modules. Educate your employees on the most prevalent cyber threats. ▪ **Smart User Management:** With one simple setting, Phish Insight can now sync data from your active directory and keep all employee data up to date. ▪ **Effective Business Intelligence:** Phish Insight features highly visualised data and reports for you to keep track of the results of phishing simulations and security awareness training. ▪ **Multiple Languages for a Global Programme:** Localised content for employees is critical for adoption of your security awareness program. Phish Insight provides both our phishing simulations and training content in Arabic, English, French, German, Hindi, Italian, Portuguese (Latin), Spanish and Traditional Chinese. Cybersecurity education is a key focus area for Trend's Corporate Social Responsibility program. The Trend Micro Initiative for Education includes outreach programs designed to empower communities on their path to a safer digital world. To date, we have reached over 2.9 million kids and parents through the Internet Safety for Kids and Families initiative and offered workshops, webinars, and conferences for over 30,000 businesses and university students, thanks in large part to our network of over 1,200 volunteers around the world. We also provided various sponsorships and resources to assist major non-profit and educational organisations, including groups like PTO Today, National Cybersecurity Alliances, Cybercrime Support Network, SCORE.org, and NIST NICE Conferences.

Objective C: Detecting Cybersecurity Events

Capabilities exist to ensure security defences remain effective and to detect cybersecurity events affecting, or with the potential to affect, essential functions.	
CAF PRINCIPLE	**HOW TREND WILL SUPPORT YOUR ADHERENCE TO THE PRINCIPLE**
C1: Security Monitoring Monitoring to detect potential security problems and track the effectiveness of existing security measures. Trend Managed XDR	Trend Micro Managed Extended Detection and Response (Managed XDR) service augments in-house capabilities with expertly managed security monitoring by a global team of Trend experts 24/7/365—for endpoints, servers, email, cloud and networks. Detection and response capabilities are maximised by correlating detection, activity and telemetry data from these sources, to provide greater insight into targeted attack source and spread. Detection, investigation and threat hunting is optimised by the latest security analytics and enriched by Trend's threat research. The service reduces the burden and time to identify, investigate and respond to threats, helping organisations supplement in-house activities to augment detection levels and improve time-to-detect and time-to-respond. Trend's threat experts create a full picture of the attack, including a root-cause analysis, attack vector, dwell time, spread and impact summary. Analysts turn that data into actionable insights which are shared with customers in detailed incident reports. Security effectiveness is trackable via reports and service reviews. Reports will be sent monthly and quarterly, summarising investigated customer threat alerts, incident cases which contain details of the threat, IoCs, and recommended mitigation options. The Managed XDR team also provides monthly reports summarising case activity from the preceding month. Trend provides an opportunity for a formal service performance review at least once per quarter. This review examines service effectiveness and performance, detailing significant events such as incidents and faults—as well as submitted cases, change requests, executions and recommendations.
C2: Proactive Security Event Discovery Detecting anomalous events in relevant network and information systems. Trend Vision One - XDR	Prevention alone is no longer enough when it comes to the latest cyber-attacks. Detection and Response capabilities are key as they provide visibility of the typically lower volume signals associated with attack activity. This is where EDR – or preferably XDR as it includes multiple sources beyond just the endpoint – delivers value. The Trend Vision One platform is built on XDR, designed to stop adversaries faster with a broader perspective and better context to hunt, detect, investigate and respond to threats from a single platform. ▪ The platform's XDR capabilities deliver native detection capabilities across your security layers including endpoint, server, email, network and cloud. This provides greater visibility, breaking down silos and achieving faster and more precise detection and response by natively integrating views, analysis and workflows across multiple operations ▪ XDR for endpoints and servers provides deep visibility and threat prevention for endpoints and servers by automatically correlating data across multiple security layers, for faster detection, improved investigation, and shorter response times ▪ XDR for email extends detection and response to customer email accounts by examining user email, threat logs, and user behaviour. This helps to cross-correlate suspicious activity with additional intelligence in order to provide remediation and response actions. ▪ XDR for networks empowers security teams with advanced AI/ML techniques, data correlation and workflows to address blind spots within your network's unmanaged attack surface. ▪ XDR for cloud extends detection and response to customer cloud accounts by examining user, service and resource log activity for suspicious behaviour, and providing remediation and response actions.

Objective D: Minimizing the Impact of Incidents

Capabilities exist to minimise the adverse impact of a cybersecurity incident on the operation of essential functions, including the restoration of those functions where necessary.	
CAF PRINCIPLE	**HOW TREND WILL SUPPORT YOUR ADHERENCE TO THE PRINCIPLE**
D1: Response and Recovery Planning Putting suitable incident management and mitigation processes in place. Trend Service One	Trend Service One is designed to help you discover, consolidate and identify critical alerts and warnings and quickly act on threats. It combines Targeted Attack Detection for qualified high risks with predictions of the attacker's next move, premium support-case handling and resolution, and access to Trend's Incident Response team—to give you outsourced cybersecurity monitoring 24/7/365. This frees your team to focus on driving innovation and meeting business objectives. Trend Targeted Attack Detection scans for early IoCs using our industry-leading threat research and the Trend Smart Protection Network. This 24/7/365 service alerts you to high-risk threats and attacks targeting your organisation. It will specify if any indicators of the specific attack were found and which endpoints were affected. In addition, you'll receive recommended actions based on the threat actor's predicted next moves. A designated Service Manager is committed to providing you with the most optimised experience with your Trend solutions. They will answer all inquiries and facilitate access to cybersecurity, solution and subject matter experts. The Trend Micro Incident Response Team is a specialized service that combines cyber crisis management, state-of-the-art threat hunting expertise, digital forensics, and sound professional advice. This specialised team is critical for enterprises managing troves of valuable data as well as those required to meet several local and global compliance requirements. Specially trained to prioritise, investigate, and fulfil compliance obligations, the Incident Response Team can help organisations avoid legal, financial and customer-relationship issues.
D2: Lessons Learned Learning from incidents and implementing these lessons to improve the resilience of essential functions. Trend Vision One – Targeted Attack Detection Trend Service One	Our Targeted Attack Detection provides you with a timeline uncovering predictions of high-risk attacks. In addition, you'll receive a detailed action plan to help you react quickly and limit the scope of an attack and minimise business interruptions. View all notifications on our Targeted Attack Detection app, so you can stay on top of any threats discovered in your environment. Service One provides extended coverage from our global Managed XDR team. Our expert team continually monitors suspicious, malicious and unwanted activity to generate high-fidelity alerts. These alerts are based on intelligence-driven (threat intelligence reports, threat intelligence feeds, and/or malware analysis) or situational awareness driven (suspicious events or IoC within the network) methods, processes and analytics across all your Trend Micro solutions. Within hours of contacting us, our Incident Response experts will have established a customised plan of action with your IT department. Our workforce, tools and processes will be set up instantly to monitor your network traffic, while logs and disk images are already being analysed for IoCs or indicators of attack. In the background, our incident coordinators will organise the flow of information, making sure all defined stakeholders are being kept in the loop about findings, developments and key decisions. Concise daily briefings and reports will provide you with all information and insight required to: ▪ Stop the ongoing attack in its tracks ▪ Start rebuilding your production environment by localizing unaffected assets and backups ▪ Harden your network, servers and endpoint defences to prevent future attacks

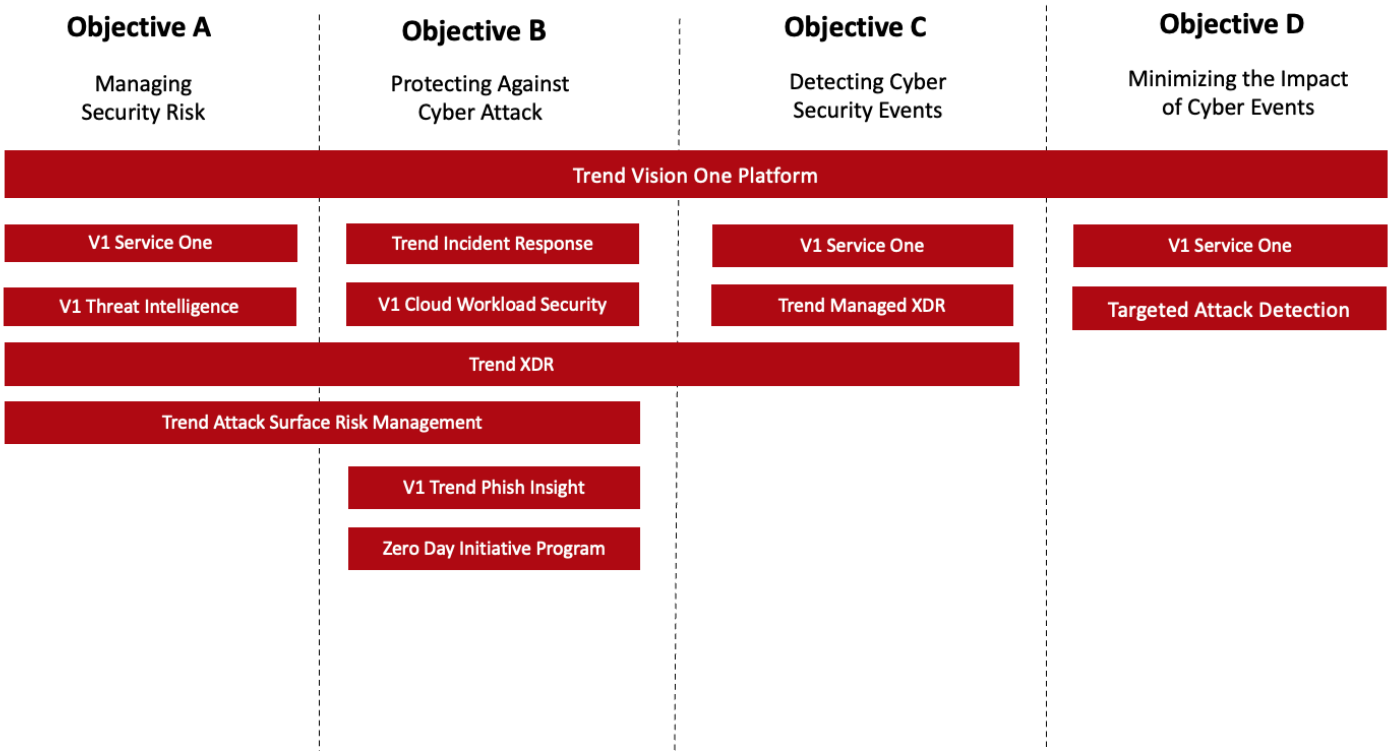
Conclusion

The public sector faces an ongoing and ever-increasing cybersecurity threat, with 40% of all cybersecurity attacks targeted at the sector. The NCSC's CAF offers a comprehensive guide to help enhance both cybersecurity and cyber resilience.

This document has explored how Trend Micro aligns our solutions to the objectives and principles of the CAF. Trend Micro's approach is centred on a comprehensive cybersecurity platform; reducing both the number of security tools required and cybersecurity spend. This is demonstrated by the capability of the platform to cover the broad objectives and principles of the CAF.

Trend Micro's approach ensures proactive cybersecurity with attack surface threat management, while extended detection and response (XDR) capabilities result in threats being identified, investigated and contained in sufficient time. This is supplemented by Trend Micro's market leading threat intelligence program which discovered 64% of all vulnerabilities identified globally in 2022. The outcome is increased cyber resilience and a reduced risk of a cyber-attack impacting the vital services the public sector provides.

Trend Micro Product Alignment to CAF Objectives



Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information.

Fueled by decades of security expertise, global threat research, and continuous innovation, Trend's AI-powered cybersecurity platform protects over 500,000 organizations and millions of individuals across clouds, networks, devices, and endpoints.

Trend's platform delivers advanced threat defense techniques, extended detection and response (XDR), attack surface management (ASM), and integration across the IT ecosystem, including AWS, Microsoft, and Google. This enables organizations to better understand, communicate, and mitigate cyber risk.

Trend's global threat research team delivers unparalleled intelligence and insights that power the platform and help protect organizations around the world from hundreds of millions of threats daily.

With 7,000 employees across 70 countries, Trend is singularly focused on cybersecurity by enabling organizations to simplify their connected world. **TrendMicro.com.**