CHECKLIST

FCC Cybersecurity Pilot Program Checklist

How eSentire helps schools and libraries build cyber resilience against advanced cyberattacks with services eligible for the FCC Cybersecurity Pilot Program

Introduction

The FCC Schools and Libraries Cybersecurity Pilot Program is a three-year, $200 million initiative designed to help eligible K-12 schools, districts, libraries, and consortia enhance their cybersecurity posture in the face of escalating threats. The FCC Cybersecurity Pilot Program was created to address these vulnerabilities by supporting the adoption of advanced cybersecurity technologies, reducing risk, and ensuring the continuity of critical learning services.

Educational organizations are prime targets for ransomware, phishing, and data breaches, often due to limited resources and an attack surface that has grown exponentially while defenses haven't kept up. By participating in the FCC Cybersecurity Pilot, education sector IT and security leaders can access much-needed resources to better protect their networks, ensure compliance, and build resilience against evolving threats.

Funding through this program will be available for public and private K-12 schools, libraries, and consortia that meet E-Rate eligibility criteria, though E-Rate participation is not required. Moreover, while high-need, low-income, and Tribal applicants may be prioritized, the program will also award funding based on geographic and institutional diversity across large and small, urban and rural environments.

Participation in the FCC Cybersecurity Pilot is a unique opportunity to accelerate your organization's security maturity, demonstrate due diligence, and help shape the future of K-12 cybersecurity policy. With funding available for solutions that many schools and libraries previously could not afford, IT and security leaders can now:

- Deploy enterprise-grade controls and technologies aligned to NIST, CIS, and other security frameworks.
- Integrate identity and access management with cloud and on-premises systems.
- Establish 24/7 threat monitoring and incident response, often for the first time.
- Reduce manual security workloads through automation and managed services.
- Demonstrate clear ROI and ensure educational services are not disrupted by cyber incidents.

Administered through the Universal Service Fund but separate from E-Rate, this program is designed to address the growing cybersecurity risks facing educational institutions by supporting the deployment of a broad range of advanced cybersecurity services and equipment. Specifically, it emphasizes a focus on four primary categories:

- **Advanced and Next-Generation Firewalls:** Capabilities may include deep packet inspection, intrusion prevention, application-layer controls, threat intelligence integration, and support for segmentation/micro-segmentation.
- **Endpoint Protection:** Solutions such as EDR (Endpoint Detection and Response), anti-malware, and managed endpoint security that provide proactive threat detection and automated response for workstations, laptops, tablets, and mobile devices.
- **Identity Protection and Authentication:** Multi-factor authentication (MFA), single sign-on (SSO), privileged access management (PAM), and identity threat detection and response (ITDR) to secure user access across networks and cloud environments.
- **Monitoring, Detection, and Response:** Security Operations Center (SOC)-as-a-service, Security Information and Event Management (SIEM), log monitoring, Managed Detection and Response (MDR), and threat intelligence platforms. These solutions provide continuous visibility and incident response across hybrid and cloud-connected environments.

Process & Compliance Requirements

To participate in the FCC Cybersecurity Pilot Program, schools and libraries must follow defined compliance protocols designed to ensure transparency, accountability, and program integrity. The following requirements are essential for maintaining eligibility and maximizing program benefits:

- **Competitive Bidding:** Participants must conduct open and fair procurement processes, evaluating solutions primarily on cost-effectiveness.
- **Documentation and Audits:** All procurements, configurations, and incident response activities must be fully documented and available for review. This includes maintaining records related to procurement, configuration baselines, change management, and incident response.
- **Data Reporting:** Participants are required to submit detailed initial, annual, and final reports on their cybersecurity posture, incidents, technology deployments, and the effectiveness of funded solutions. This reporting supports ongoing improvement and program evaluation by the FCC.
- **Program Integrity:** Compliance with document retention, audit readiness, and gift restriction requirements is mandatory for both applicants and vendors.

In this checklist, we highlight how eSentire's portfolio of Continuous Threat Exposure Management (CTEM) and Managed Detection and Response (MDR) services can help you align to the FCC Pilot Program's most critical requirements so you can maximize the benefits of the program, strengthen your cybersecurity posture, and build resilience against sophisticated threats.

Advanced / Next-Generation Firewalls	eSentire Services	FCC Notes about Coverage
Advanced Threat Detection and Prevention	**eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	*Equipment and services that implement advanced/ next-generation firewalls, including software-defined firewalls and Firewall as a Service, are eligible.* *Specifically, equipment, services, or a combination of equipment and services that limits access between networks, excluding basic firewalls that are funded through the Commission's E-Rate program, are eligible.* *Eligible equipment and services may include the following features, substantially similar features, or their equivalents.*
AI/ML Threat Detection and Response	**eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	
Application Awareness & Control	**eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	
Cloud-Delivered Threat Intelligence	**eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	

Advanced / Next-Generation Firewalls	eSentire Services	FCC Notes about Coverage
Deep Packet Inspection (DPI)	**eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	
Integrated Intrusion Prevention Systems (IPS)	**eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	
Intrusion Prevention/Detection	**eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	
Malware Detection	**eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	

Endpoint Protection	eSentire Services	FCC Notes about Coverage
Anti-Malware	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting expertise with best-of-breed endpoint threat prevention and endpoint detection and response (EDR) capabilities to eliminate blind spots, detect, and stop threats such as ransomware, APTs, zero-day attacks, and more. Our Threat Response Unit (TRU) investigates and correlates anomalous behavior detected to create advanced machine-learning models and novel detection rules to help you stay ahead of cyber threats. When a threat bypasses your controls, our 24/7 Elite Threat Hunters will take action on your behalf to contain and remediate compromised endpoints, minimizing disruption to your business. **Learn More**	*Equipment and services that implement endpoint protection are eligible.* *Specifically, equipment, services, or a combination of equipment and services that implements safeguards to protect school- and library-owned end-user devices, including desktops, laptops, and mobile devices, against cyber threats and attacks are eligible.* *Eligible equipment and services may include the following features, substantially similar features or their equivalents.*
Anti-Ransomware	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting expertise with best-of-breed endpoint threat prevention and endpoint detection and response (EDR) capabilities to eliminate blind spots, detect, and stop threats such as ransomware, APTs, zero-day attacks, and more. Our Threat Response Unit (TRU) investigates and correlates anomalous behavior detected to create advanced machine-learning models and novel detection rules to help you stay ahead of cyber threats. When a threat bypasses your controls, our 24/7 Elite Threat Hunters will take action on your behalf to contain and remediate compromised endpoints, minimizing disruption to your business. **Learn More**	
Anti-Spam	**eSentire MDR for Microsoft** eSentire MDR for Microsoft helps you identify, contain, respond and remediate threats across Microsoft SIEM, endpoint, identity, email, and cloud security services stopping threats before they disrupt your business operations. Our dedicated Microsoft security experts help you operationalize Microsoft Defender XDR and Microsoft Sentinel to onboard our services. Our MDR for Microsoft offerings include Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps. Our 24/7 SOC Cyber Analysts and Elite Threat Hunters rapidly respond to and investigate threats across your Microsoft environments, with a Mean Time to Contain of less than 15 minutes. **Learn More**	
Anti-Virus	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting expertise with best-of-breed endpoint threat prevention and endpoint detection and response (EDR) capabilities to eliminate blind spots, detect, and stop threats such as ransomware, APTs, zero-day attacks, and more. Our Threat Response Unit (TRU) investigates and correlates anomalous behavior detected to create advanced machine-learning models and novel detection rules to help you stay ahead of cyber threats. When a threat bypasses your controls, our 24/7 Elite Threat Hunters will take action on your behalf to contain and remediate compromised endpoints, minimizing disruption to your business. **Learn More**	

Endpoint Protection	eSentire Services	FCC Notes about Coverage
Endpoint Detection & Response (EDR)	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting expertise with best-of-breed endpoint threat prevention and endpoint detection and response (EDR) capabilities to eliminate blind spots, detect, and stop threats such as ransomware, APTs, zero-day attacks, and more. Our Threat Response Unit (TRU) investigates and correlates anomalous behavior detected to create advanced machine-learning models and novel detection rules to help you stay ahead of cyber threats. When a threat bypasses your controls, our 24/7 Elite Threat Hunters will take action on your behalf to contain and remediate compromised endpoints, minimizing disruption to your business. **Learn More**	
Extended Detection & Response (XDR)	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting expertise with best-of-breed endpoint threat prevention and endpoint detection and response (EDR) capabilities to eliminate blind spots, detect, and stop threats such as ransomware, APTs, zero-day attacks, and more. Our Threat Response Unit (TRU) investigates and correlates anomalous behavior detected to create advanced machine-learning models and novel detection rules to help you stay ahead of cyber threats. When a threat bypasses your controls, our 24/7 Elite Threat Hunters will take action on your behalf to contain and remediate compromised endpoints, minimizing disruption to your business. **Learn More**	
Insider and Privilege Misuse	**eSentire MDR for Identity** eSentire MDR for Identity detects and responds to identity-based attacks using context from our threat intelligence research and integration with our best-of-breed identity solutions. We provide visibility into credential misuse, entitlement exposures, and privilege escalation activities from the endpoint to Active Directory to multi-cloud environments. eSentire Atlas XDR platform leverages identity-based behavioral analytics and machine learning models to monitor and detect anomalies across your entire attack surface, providing our SOC with a comprehensive view of security incidents. Our multi-signal approach ingests & correlates data to investigate & respond to identity-based threats before they disrupt your business. **Learn More** **eSentire MDR for Log** eSentire MDR for Log delivers critical visibility across your multi-cloud and hybrid environments without the day-to-day challenges of log management. We aggregate actionable intelligence from multi-signal ingestion to accelerate our investigations and deliver complete response against threats such as phishing and business email compromises, insider threats, suspicious VPN activity, data exfiltration, and more. Our best-of-breed log monitoring technology ingests and stores logs across AWS, Microsoft 365, Azure, and your existing security controls to provide complete attack surface visibility and help you satisfy insurance, regulatory and compliance requirements. **Learn More**	

Endpoint Protection	eSentire Services	FCC Notes about Coverage
Target Intrusions	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting expertise with best-of-breed endpoint threat prevention and endpoint detection and response (EDR) capabilities to eliminate blind spots, detect, and stop threats such as ransomware, APTs, zero-day attacks, and more. Our Threat Response Unit (TRU) investigates and correlates anomalous behavior detected to create advanced machine-learning models and novel detection rules to help you stay ahead of cyber threats. When a threat bypasses your controls, our 24/7 Elite Threat Hunters will take action on your behalf to contain and remediate compromised endpoints, minimizing disruption to your business. **Learn More**	
Web Application Hacking	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting expertise with best-of-breed endpoint threat prevention and endpoint detection and response (EDR) capabilities to eliminate blind spots, detect, and stop threats such as ransomware, APTs, zero-day attacks, and more. Our Threat Response Unit (TRU) investigates and correlates anomalous behavior detected to create advanced machine-learning models and novel detection rules to help you stay ahead of cyber threats. When a threat bypasses your controls, our 24/7 Elite Threat Hunters will take action on your behalf to contain and remediate compromised endpoints, minimizing disruption to your business. **Learn More**	

Identity Protection and Authentication	eSentire Services	FCC Notes about Coverage
Cloud Application Protection	**eSentire MDR for Identity** eSentire MDR for Identity detects and responds to identity-based attacks using context from our threat intelligence research and integration with our best-of-breed identity solutions. We provide visibility into credential misuse, entitlement exposures, and privilege escalation activities from the endpoint to Active Directory to multi-cloud environments. eSentire Atlas XDR platform leverages identity-based behavioral analytics and machine learning models to monitor and detect anomalies across your entire attack surface, providing our SOC with a comprehensive view of security incidents. Our multi-signal approach ingests & correlates data to investigate & respond to identity-based threats before they disrupt your business. **Learn More** **eSentire MDR for Cloud – Cloud-Native Application Protection Platform (CNAPP)** eSentire MDR for Cloud – CNAPP enables you to gain visibility into all portions of your cloud environment to implement build-to-run-time security. You can leverage configuration hardening, agentless workload protection of virtual machines and containers, and vulnerability assessment functionality. We also curtail user privileges and over-permissive cloud entitlements to keep your identities safe and secure. **Learn More**	*Equipment and services that implement identity protection and authentication are eligible.* *Specifically, equipment, services, or a combination of equipment and services that implements safeguards to protect a user's network identity from theft or misuse and/or provide assurance about the network identity of an entity interacting with a system are eligible.* *Eligible equipment and services may include the following features, substantially similar features, or their equivalents.*
Cloud Services	**eSentire MDR for Identity** eSentire MDR for Identity detects and responds to identity-based attacks using context from our threat intelligence research and integration with our best-of-breed identity solutions. We provide visibility into credential misuse, entitlement exposures, and privilege escalation activities from the endpoint to Active Directory to multi-cloud environments. eSentire Atlas XDR platform leverages identity-based behavioral analytics and machine learning models to monitor and detect anomalies across your entire attack surface, providing our SOC with a comprehensive view of security incidents. Our multi-signal approach ingests & correlates data to investigate & respond to identity-based threats before they disrupt your business. **Learn More** **eSentire MDR for Cloud – Cloud-Native Application Protection Platform (CNAPP)** eSentire MDR for Cloud – CNAPP enables you to gain visibility into all portions of your cloud environment to implement build-to-run-time security. You can leverage configuration hardening, agentless workload protection of virtual machines and containers, and vulnerability assessment functionality. We also curtail user privileges and over-permissive cloud entitlements to keep your identities safe and secure. **Learn More**	

Identity Protection and Authentication	eSentire Services	FCC Notes about Coverage
Credential Stuffing	**eSentire MDR for Identity** eSentire MDR for Identity detects and responds to identity-based attacks using context from our threat intelligence research and integration with our best-of-breed identity solutions. We provide visibility into credential misuse, entitlement exposures, and privilege escalation activities from the endpoint to Active Directory to multi-cloud environments. eSentire Atlas XDR platform leverages identity-based behavioral analytics and machine learning models to monitor and detect anomalies across your entire attack surface, providing our SOC with a comprehensive view of security incidents. Our multi-signal approach ingests & correlates data to investigate & respond to identity-based threats before they disrupt your business. **Learn More**	
Content Blocking and Filtering/URL Filtering	**eSentire MDR with Microsoft Defender for Identity and Cloud Apps** eSentire MDR with Microsoft Defender for Identity and Cloud Apps solution combines elite threat hunting and 24/7 SOC expertise to protect your Microsoft cloud environments by extending visibility into cloud applications, investigating identity-related security events and analyzing user risks using context from your Microsoft Defender XDR products, providing 24/7 response and remediation capabilities, and integrating security capabilities with your existing investment into Microsoft ecosystem. **Learn More**	
Email and Web Security	**eSentire MDR for Microsoft** eSentire MDR for Microsoft helps you identify, contain, respond and remediate threats across Microsoft SIEM, endpoint, identity, email, and cloud security services stopping threats before they disrupt your business operations. Our dedicated Microsoft security experts help you operationalize Microsoft Defender XDR and Microsoft Sentinel to onboard our services. Our MDR for Microsoft offerings include Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps. Our 24/7 SOC Cyber Analysts and Elite Threat Hunters rapidly respond to and investigate threats across your Microsoft environments, with a Mean Time to Contain of less than 15 minutes. **Learn More** **eSentire MDR with Microsoft Defender for Identity and Cloud Apps** eSentire MDR with Microsoft Defender for Identity and Cloud Apps solution combines elite threat hunting and 24/7 SOC expertise to protect your Microsoft cloud environments by extending visibility into cloud applications, investigating identity-related security events and analyzing user risks using context from your Microsoft Defender XDR products, providing 24/7 response and remediation capabilities, and integrating security capabilities with your existing investment into Microsoft ecosystem. **Learn More**	

Identity Protection and Authentication	eSentire Services	FCC Notes about Coverage
Identity Governance & Technologies	**eSentire MDR for Identity** eSentire MDR for Identity detects and responds to identity-based attacks using context from our threat intelligence research and integration with our best-of-breed identity solutions. We provide visibility into credential misuse, entitlement exposures, and privilege escalation activities from the endpoint to Active Directory to multi-cloud environments. eSentire Atlas XDR platform leverages identity-based behavioral analytics and machine learning models to monitor and detect anomalies across your entire attack surface, providing our SOC with a comprehensive view of security incidents. Our multi-signal approach ingests & correlates data to investigate & respond to identity-based threats before they disrupt your business. **Learn More**	
Intrusion Detection Systems (IDS)	**eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting expertise with best-of-breed endpoint threat prevention and endpoint detection and response (EDR) capabilities to eliminate blind spots, detect, and stop threats such as ransomware, APTs, zero-day attacks, and more. Our Threat Response Unit (TRU) investigates and correlates anomalous behavior detected to create advanced machine-learning models and novel detection rules to help you stay ahead of cyber threats. When a threat bypasses your controls, our 24/7 Elite Threat Hunters will take action on your behalf to contain and remediate compromised endpoints, minimizing disruption to your business. **Learn More** **eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	

Identity Protection and Authentication	eSentire Services	FCC Notes about Coverage
Logging Practices / Event Logging	**eSentire MDR for Log** eSentire MDR for Log delivers critical visibility across your multi-cloud and hybrid environments without the day-to-day challenges of log management. We aggregate actionable intelligence from multi-signal ingestion to accelerate our investigations and deliver complete response against threats such as phishing and business email compromises, insider threats, suspicious VPN activity, data exfiltration, and more. Our best-of-breed log monitoring technology ingests and stores logs across AWS, Microsoft 365, Azure, and your existing security controls to provide complete attack surface visibility and help you satisfy insurance, regulatory and compliance requirements. **Learn More**	
MFA/Phishing-Resistant MFA	**eSentire MDR for Identity** eSentire MDR for Identity detects and responds to identity-based attacks using context from our threat intelligence research and integration with our best-of-breed identity solutions. We provide visibility into credential misuse, entitlement exposures, and privilege escalation activities from the endpoint to Active Directory to multi-cloud environments. eSentire Atlas XDR platform leverages identity-based behavioral analytics and machine learning models to monitor and detect anomalies across your entire attack surface, providing our SOC with a comprehensive view of security incidents. Our multi-signal approach ingests & correlates data to investigate & respond to identity-based threats before they disrupt your business. **Learn More**	
Password Spraying	**eSentire MDR for Identity** eSentire MDR for Identity detects and responds to identity-based attacks using context from our threat intelligence research and integration with our best-of-breed identity solutions. We provide visibility into credential misuse, entitlement exposures, and privilege escalation activities from the endpoint to Active Directory to multi-cloud environments. eSentire Atlas XDR platform leverages identity-based behavioral analytics and machine learning models to monitor and detect anomalies across your entire attack surface, providing our SOC with a comprehensive view of security incidents. Our multi-signal approach ingests & correlates data to investigate & respond to identity-based threats before they disrupt your business. **Learn More** **eSentire MDR for Log** eSentire MDR for Log delivers critical visibility across your multi-cloud and hybrid environments without the day-to-day challenges of log management. We aggregate actionable intelligence from multi-signal ingestion to accelerate our investigations and deliver complete response against threats such as phishing and business email compromises, insider threats, suspicious VPN activity, data exfiltration, and more. Our best-of-breed log monitoring technology ingests and stores logs across AWS, Microsoft 365, Azure, and your existing security controls to provide complete attack surface visibility and help you satisfy insurance, regulatory and compliance requirements. **Learn More**	

Identity Protection and Authentication	eSentire Services	FCC Notes about Coverage
Security Information and Event Management (SIEM)	**eSentire MDR for Log** eSentire MDR for Log delivers critical visibility across your multi-cloud and hybrid environments without the day-to-day challenges of log management. We aggregate actionable intelligence from multi-signal ingestion to accelerate our investigations and deliver complete response against threats such as phishing and business email compromises, insider threats, suspicious VPN activity, data exfiltration, and more. Our best-of-breed log monitoring technology ingests and stores logs across AWS, Microsoft 365, Azure, and your existing security controls to provide complete attack surface visibility and help you satisfy insurance, regulatory and compliance requirements. **Learn More**	
Single Sign-On (SSO)	**eSentire MDR for Identity** eSentire MDR for Identity detects and responds to identity-based attacks using context from our threat intelligence research and integration with our best-of-breed identity solutions. We provide visibility into credential misuse, entitlement exposures, and privilege escalation activities from the endpoint to Active Directory to multi-cloud environments. eSentire Atlas XDR platform leverages identity-based behavioral analytics and machine learning models to monitor and detect anomalies across your entire attack surface, providing our SOC with a comprehensive view of security incidents. Our multi-signal approach ingests & correlates data to investigate & respond to identity-based threats before they disrupt your business. **Learn More**	
Web Content Controls	**eSentire MDR with Microsoft Defender for Identity and Cloud Apps** eSentire MDR with Microsoft Defender for Identity and Cloud Apps solution combines elite threat hunting and 24/7 SOC expertise to protect your Microsoft cloud environments by extending visibility into cloud applications, investigating identity-related security events and analyzing user risks using context from your Microsoft Defender XDR products, providing 24/7 response and remediation capabilities, and integrating security capabilities with your existing investment into Microsoft ecosystem. **Learn More** **eSentire MDR for Cloud** eSentire MDR for Cloud detects, investigates, and responds to threats specific to multi-cloud environments leveraging our cloud-native XDR platform, proprietary MITRE ATT&CK mapped detections, and our 24/7 Security Operations Centers (SOCs) staffed with Elite Threat Hunters and experienced Cyber Analysts. We go beyond traditional security measures to safeguard your business from a wide range of threats across various environments, including Virtual Machines (VMs), containers, and Kubernetes in multi-cloud environments across AWS, Microsoft Azure, and Google Cloud. **Learn More**	

Monitoring, Detection, and Response	eSentire Services	FCC Notes about Coverage
Advanced Attack Surface Management and Asset Management Solutions	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. **Learn More** **eSentire MDR for Cloud – Cloud-Native Application Protection Platform (CNAPP)** eSentire MDR for Cloud – CNAPP enables you to gain visibility into all portions of your cloud environment to implement build-to-run-time security. You can leverage configuration hardening, agentless workload protection of virtual machines and containers, and vulnerability assessment functionality. We also curtail user privileges and over-permissive cloud entitlements to keep your identities safe and secure. **Learn More** **eSentire Continuous Threat Exposure Management (CTEM)** eSentire CTEM advisory services help you proactively identify gaps in your cybersecurity program, mitigate identified vulnerabilities, reduce your cyber risk, and build a cybersecurity strategy to improve how you anticipate, withstand, and recover from the most advanced cyberattacks. We continuously test the resilience of your systems and employees so you can enjoy peace of mind. Plus, our Threat Response Unit (TRU) keeps you ahead of emerging cyber threats by leveraging human-driven intelligence, original content on the latest threats, and advanced analytics. **Learn More**	*Equipment and services that implement monitoring, detection and response are eligible.* *Specifically, equipment, services, or a combination of equipment and services that monitor and/or detect threats to a network and that take responsive action to remediate or otherwise address those threats is eligible.* *Eligible equipment and services may include the following features, substantially similar features, or their equivalents.*
Compliance Assessment	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organization's cybersecurity program and initiatives. **Learn More** **eSentire MDR for Cloud – Cloud-Native Application Protection Platform (CNAPP)** eSentire MDR for Cloud – CNAPP enables you to gain visibility into all portions of your cloud environment to implement build-to-run-time security. You can leverage configuration hardening, agentless workload protection of virtual machines and containers, and vulnerability assessment functionality. We also curtail user privileges and over-permissive cloud entitlements to keep your identities safe and secure. **Learn More**	

Monitoring, Detection, and Response	eSentire Services	FCC Notes about Coverage
Dark Web Scanning	**eSentire Dark Web Monitoring** eSentire Dark Web Monitoring provides 24/7 continuous monitoring and broad visibility into the Dark Web to protect your executives, employees, and customers' sensitive data before it's used maliciously by threat actors. We help you identify early IOCs and TTPs that threat actors rely on to conduct sophisticated cyberattacks, and provide additional contextual awareness into known and unknown threat actor groups for deeper threat investigations. Unlike other Dark Web threat intelligence vendors, we leverage threat intelligence gathered from the Dark Web to take actual response actions, disrupt cyberattacks, and put our customers ahead of disruption. **Learn More**	
Internal/External Vulnerability Scanning	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organization's cybersecurity program and initiatives. **Learn More**	
Network/Device Monitoring & Response	**eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	
Network Security Audit	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organization's cybersecurity program and initiatives. **Learn More**	

Monitoring, Detection, and Response	eSentire Services	FCC Notes about Coverage
Network Traffic Analysis	**eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	
Managed Detection & Response (MDR)	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. **Learn More**	
Managed Service Providers	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. **Learn More**	
Maturity Models	**eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organization's cybersecurity program and initiatives. **Learn More**	

Monitoring, Detection, and Response	eSentire Services	FCC Notes about Coverage
Network Detection Response (NDR)	**eSentire MDR for Network** eSentire MDR for Network combines deep packet inspection with proprietary attack pattern analysis and behavioral analytics to rapidly identify and block known threats and malicious activity and notify your security team of policy violations. Our proprietary network software and open XDR platform enable automated disruption, firewall integration and real-time response capabilities, helping you anticipate and outpace adversaries, on-premises, in the cloud, and across your hybrid environment. We disrupt malicious traffic on your behalf with root cause determination and remediation support to reduce your Mean Time to Detect (MTTD) and Mean Time to Response (MTTR). **Learn More**	
Penetration Testing	**eSentire Penetration Testing** eSentire's Penetration Testing helps you understand how effective your privacy and security controls are, before a malicious actor breaks into your environment, causing business disruption. Our penetration testers use the latest tactics, techniques and procedures (TTPs) in an authorised attempt to gain access to your resources without the knowledge of usernames, passwords, and other usual means of access. In the post-penetration testing report, we provide a detailed summary of high-risk systems and recommendations on how you can improve your security posture. **Learn More**	
Security Operations Center (SOC) for Around the Clock (24/7/365) Monitoring, Detection, and Response	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. **Learn More**	
Threat Hunting/Updates and Threat Intelligence	**eSentire Multi-Signal MDR** eSentire Managed Detection and Response combines cutting-edge open XDR technology, multi-signal threat intelligence, and the industry's only 24/7 Elite Threat Hunters to help you build a more resilient security operation. Our multi-signal MDR approach ingests high-fidelity data sources from endpoint, network, log, cloud, identity, assets, and vulnerability data to enable complete attack surface visibility. Our powerful XDR Platform correlates indicators of compromise to detect, respond and automatically disrupt threats in minutes - with a Mean Time to Contain of less than 15 minutes. Through host isolation, malicious network communication disruption, account-based suspensions, and other measures, we can stop the attacker at any level. **Learn More**	

Monitoring, Detection, and Response	eSentire Services	FCC Notes about Coverage
Vulnerability Management	**eSentire Managed Vulnerability Service** eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across your on-premises and cloud environments by scanning for zero-day vulnerabilities and CVEs, providing full visibility and contextual awareness across your attack surface. We partner with leaders in vulnerability management to deliver scanning precision and minimise vulnerability discovery to remediation timeframe. Our best-of-breed technology is supported by the expertise of our 24/7 SOC Analysts and Elite Threat Hunters, who act as an extension of your team to execute scans, provide analysis, and support remediation plans. **Learn More** **eSentire CISO & Advisory Services** eSentire's CISO and Advisory Services is a flexible engagement offering which provides the organisation access to an eSentire Executive Consultant who can assist them with the designing, developing, enhancing, and communicating aspects of the organization's cybersecurity program and initiatives. **Learn More** **eSentire MDR for Cloud – Cloud-Native Application Protection Platform (CNAPP)** eSentire MDR for Cloud – CNAPP enables you to gain visibility into all portions of your cloud environment to implement build-to-run-time security. You can leverage configuration hardening, agentless workload protection of virtual machines and containers, and vulnerability assessment functionality. We also curtail user privileges and over-permissive cloud entitlements to keep your identities safe and secure. **Learn More**	

Training

Training is eligible as a part of installation of the equipment and services only if it is basic instruction on the use of eligible equipment and services, directly associated with equipment and services installation, and is part of the contract or agreement for the equipment and services. Training must occur coincidently or within a reasonable time after installation.

Ready to Get Started?

Reach out to connect with an eSentire security specialist and build a more resilient security operation today.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US 1-866-579-2200

eSentire

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organisations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organisation's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organisations with 65% of its global base recognised as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organisations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.