Cybersecurity Coordinator Forum

October 2025

Daniel Ramirez

Chief Information Security Officer

Texas Education Agency

cybersecurity@tea.texas.gov

Cybersecurity Coordinator Forum

The **TEA Cybersecurity** team hosts a **monthly** meeting for Texas School Systems **Cybersecurity Coordinators**, **Technology Coordinators**, Education Service Center (ESC) **Cybersecurity personnel**, and other members of the community that support K12 Cybersecurity efforts. It provides content designed to assist School Systems and ESCs towards maturity in an information security program.

Register here:
https://t.ly/Hmimy

Please register with your School System email account.

Cybersecurity Nutritional Facts

Serving Size: 1 Cybersecurity Professional

	%Daily Value*
Passion	300%
Determination	500%
Creativity	100%
Critical Thinking	1000%
Innovation	100%
Hard Work	200%
Sleep	0%
Caffeine	110%

*Percent Daily Values Are Based on Your Unique Diet

Daniel Ramirez

Chief Information Security Officer for TEA

- Started August 1, 2025

Working in IT for 28+ years

- Texas A&M Kingsville
- University of Texas Rio Grande Valley (Pan Am)
- Region One Education Service Center
- 13 of the 28+ years have been in Information Security

Security Certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Penetration Tester (SANS GIAC-GPEN) *(*not active)*

OCTOBER IS


01 110 101 011 010110 101 01011
CYBERSECURITY AWARENESS MONTH
2025 THEME: STAY SAFE ONLINE
NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE
CYBERSECURITY AWARENESS MONTH
2025 CHAMPION

Remind staff and students

- Password best practices (the longer the better)
- Multi-Factor Authentication (protect all important accounts)
- Secure email practices (think before you click!)
- Keep your computer and personal device software updated
- Do your part, share your knowledge with family and friends

https://www.cisa.gov/resources-tools/resources/cybersecurity-awareness-month-toolkit

Agenda

- In State News
- Regional Security Operation Centers (RSOCs)
- Texas K12 Cybersecurity Initiative Update
- Survey Updates
- Defining Managed Endpoint Detection & Response (EDR)
- Cybersecurity News & Advisories

Texas Education Agency

In State News

HB 3512 - FYI

- **HB 3512** - establishes requirements for artificial intelligence (AI) training programs for certain employees and officials of state agencies and local governments in Texas. It amends existing statutes to integrate AI training alongside cybersecurity training.
  - School districts must ensure their cybersecurity coordinators complete both cybersecurity and AI training annually.
  - DIR will develop forms for verification and reporting.
- **Required training is still under development and should be announced early next year.**

Texas Cyber Command

- Passed by 89th Texas Legislature as HB 150
- Governor Abbott appointed retired U.S. Navy Vice Admiral Timothy James “TJ” White to lead the command.
- https://www.txcc.texas.gov/

TXCC
TEXAS CYBER COMMAND

Texas Cyber Command Overview

- Largest state-based cybersecurity department in the U.S.
- Shifts from reactive defense to proactive prevention and resilience
- Collaborates with universities, RSOCs, federal agencies, and local/state partners
- Strengthens cybersecurity on strategic fronts and key terrain
- Deploys cutting-edge capabilities to secure Texas infrastructure

TXCC will be advertising and hiring to support:

- Cyber Threat Intelligence Unit
- Cyber Incident Response Unit
- Digital Forensic Laboratory
- Texas Information Sharing & Analysis Organization (ISAO)
- Cybersecurity Architect (IT/OT/IOT)
- Principal Privacy Engineer

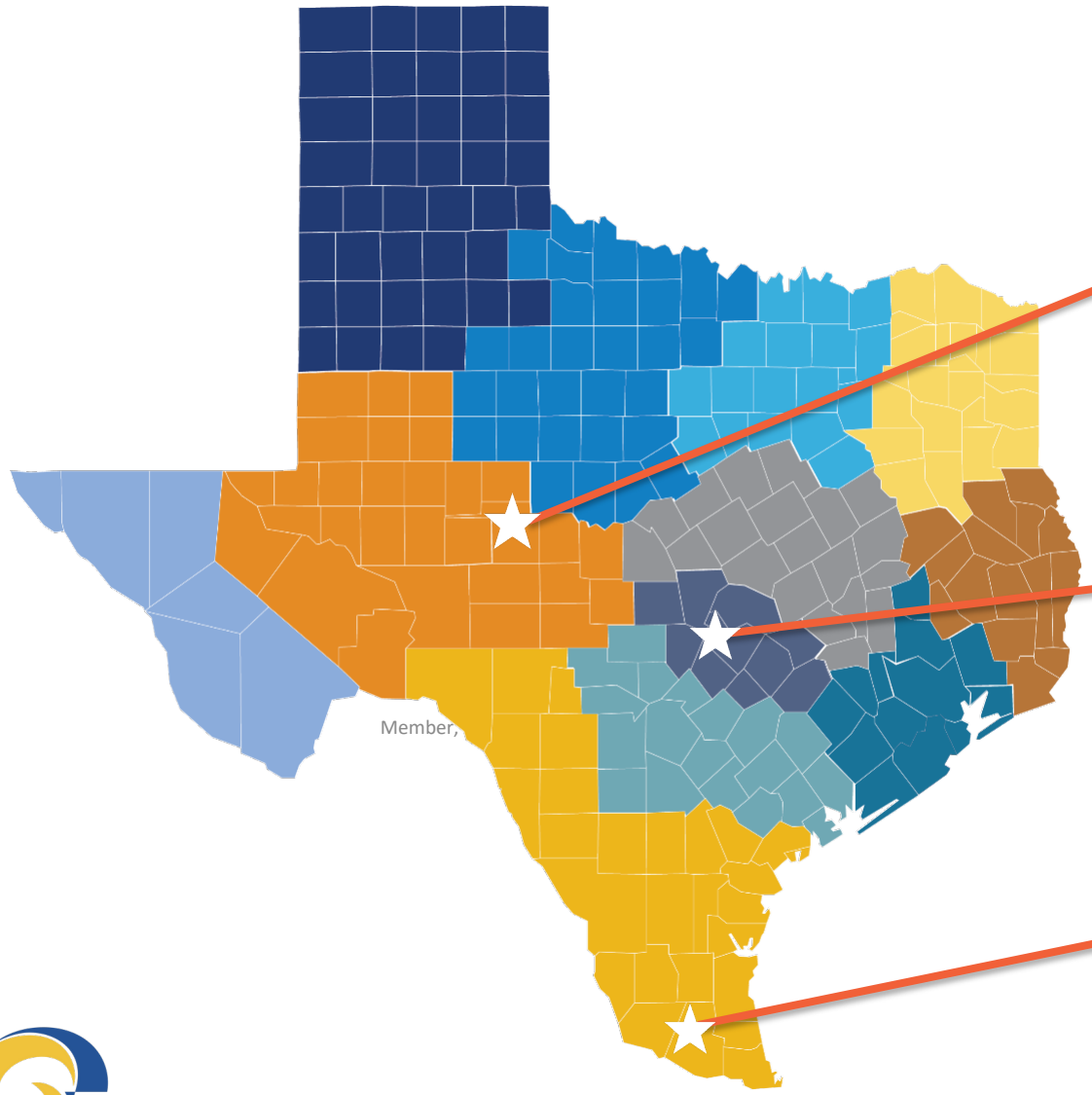
https://www.txcc.texas.gov/careers

"Now and long term. People are why we do it, and people are how we do it." –TJ White

Texas Education Agency

Regional Security Operation Center (RSOC)

Funded Texas RSOCs



Angelo State University
San Angelo
Economic Region: West Texas
(325) 942-2150
rsoc@angelo.edu

University of Texas at Austin
Austin
Economic Region: Capitol
(512) 475-9242
security@ut-rsoc.org

University of Texas Rio Grande Valley
Edinburg and Brownsville
Economic Region: South Texas
(956) 665-7762
RSOC@utrgv.edu

Image courtesy of ASU RSOC

ASU RSOC (rsoc@angelo.edu)

- Managed Endpoint Detection and Response (EDR)
- Real-time network security monitoring
- Alerts and guidance for defeating security threats
- Remote and on-site cyber incident responders
- Guidance on implementing cyber policies and plans
- Educational and awareness services
- Train University students in live Security Operations Center (SOC) environment
- Community outreach and cybersecurity training

https://www.angelo.edu/community/kay-bailey-hutchison-institute/operations/regional-security-operations-center/

UT Austin RSOC (rsoc@utexas.edu)

- Managed Endpoint Detection and Response (EDR)
- Real-Time Network Monitoring
- Automated Darkweb Monitoring
- Automated Web Application Security Assessment
- Threat Alerts and Guidance
- Incident Response
- Cybersecurity Policy Guidance
- Education and Awareness Programs
- Statewide Services
  - Dorkbot, CredMaster, Scavenger

https://rsoc.utexas.edu/

UTRGV RSOC (rsoc@utrgv.edu)

- Managed Endpoint Detection and Response (EDR)
- Incident Response
- Monitoring and Alerting
- Policy and Planning
- Training and Awareness

https://rsoc.utrgv.edu/

Texas Education Agency

Texas K12 Cybersecurity Initiative

Fully Funded Services ($0 Cost to School Systems)

- **Fully funded services currently available for request :**
  - **Managed Endpoint Detection and Response (EDR)**
    - Requirement: student enrollment **50,000** or less, licenses up to **30%** enrollment, 30 license min.
    - Once registered, request service via Managed Security Service (MSS): MSS Portal Log In Process (texas.gov).
    - School Systems may choose between EDR vendors CrowdStrike or SentinelOne.
    - Shared option should be most common for School Systems.
  - **Texas Cybersecurity Framework (TCF) Assessment (*aka School District Cybersecurity Assessment (SDCA)*)**
    - Requirement: First come, first served for **any** School System.
    - Once registered, request service via MSS : TX K-12 Cybersecurity Assessment Quick Start Guide
    - School Systems may choose between Small (~~Basic~~), Medium (~~Intermediate~~), or Large (~~Advanced~~) Cybersecurity Assessments.
    - May be ordered now and scheduled for any time through August 2027.
  - **Network Detection and Response (NDR) – Pilot Program Closed for FY23 - FY25**
    - NDR pilot results are being evaluated to determine inclusion for FY26 – FY27.
    - NDR vendor is Vectra.

https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/sts-new-customer-information-form.docx

ILC & STS Portal Access Process

1. School System Completes **New Customer Form,** send to DIR
   - *No signatures required*
2. DIR Receives New Customer Form and Sends School System the **Interlocal Contract (ILC)**
3. School System reviews, completes, approves, and signs ILC
   - *Requires Superintendent Signature*
4. School System sends signed ILC to DIR for processing
5. DIR reviews and approves ILC, then **STS Portal Access** Granted (to listed technical contacts on New Customer Form)
6. School System requests MSS services via STS Portal
   1. EDR
   2. TCF Assessment

Ongoing Goals – K12 Cybersecurity Initiative

- Current goals are still in effect and will be carried forward in FY26/27
  - Implement fully managed **Endpoint Detection and Response (EDR)** on School System servers and applicable staff devices.
  - Implement **Multi-Factor Authentication (MFA**) for staff email systems**.**
  - Ensure **Domain-based Message Authentication, Reporting, and Conformance (DMARC) Compliance** to enhance protection against phishing and spoofing**.**
  - Restrict **local administrator access** to minimize the risk of unauthorized system changes.
  - Complete a **Texas Cybersecurity Framework (TCF) assessment** to get a baseline of cybersecurity program and action plan for improving maturity.
  - Implement **Network Detection and Response (NDR**).
    - NDR Pilot is paused to new customers as we evaluate a more viable cost option

Program Participation - ILC

- **School Systems that have onboarded with DIR**
  - 480 School Systems have signed the DIR Interlocal Contract (ILC) form. (40%)
  - Two (2) new since our last CCF (28 days ago)

- Goal: 100% of School Systems complete a signed ILC with DIR.
- Why?
  - **Zero** Commitment to request any services
  - **Zero Cost** for any TEA K12 Cybersecurity Initiative services in scope
  - ILC process takes time to complete
    - Superintendent Signoff, Board Approval, etc.
    - Cannot provide EDR or other services until signed ILC is on file

DIR = Texas **D**epartment of **I**nformation **R**esources

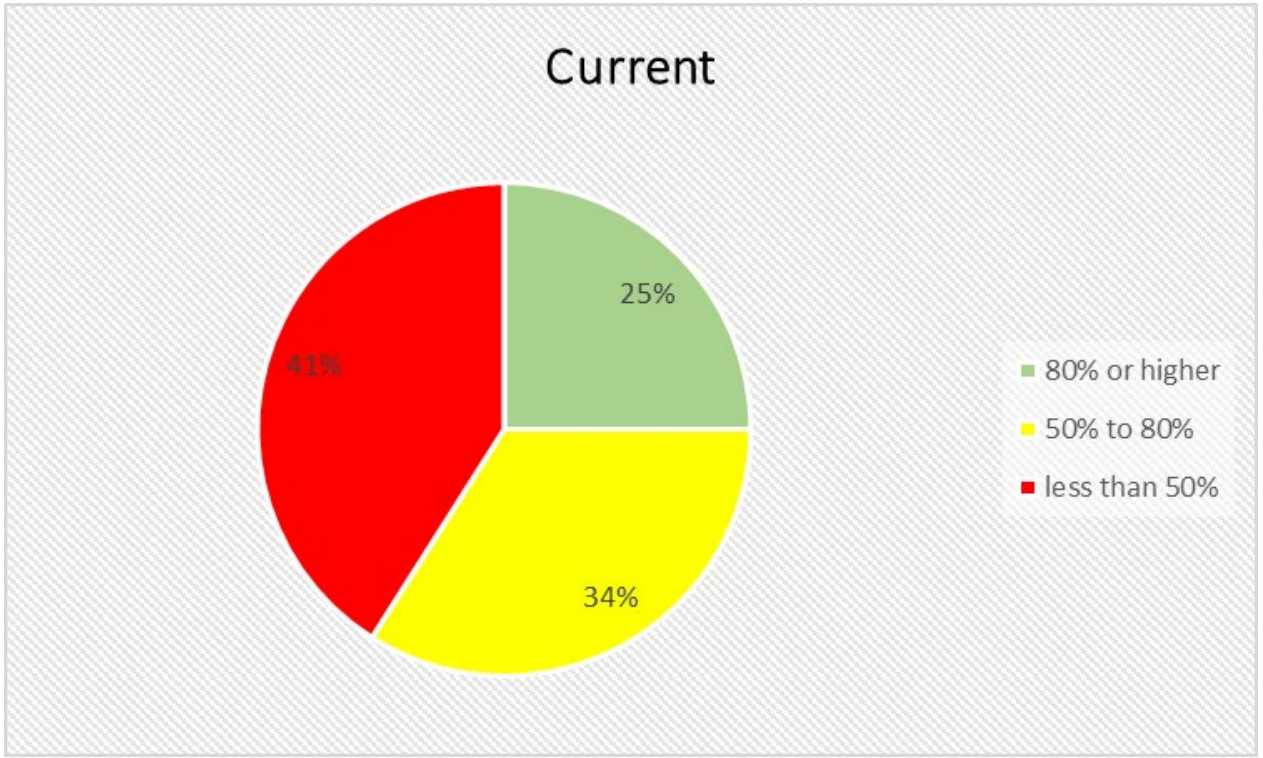
Program Participation - EDR

- **End Point Detection Response (EDR)**
  - 344 School Systems have signed up for EDR
  - Installed on 238,000 endpoints.
  - 40,600+ attacks blocked.
  - 10,500+ ransomware threats neutralized.

- ESCs contracted to assist school systems with deploying EDR at no cost.
- Note: Managed EDR is a budgeted item, this will remain for as long as EDR retains its utility.

Program Participation - EDR Agent Deployment

K12 Cybersecurity Initiative - EDR Deployment Metrics
(Requested vs % Deployed)



EDR In-Scope Computers

- School Systems need comprehensive EDR coverage
  1. On-Prem Servers (100%)
  2. IT Staff & Central Office Staff Computers
  3. Teacher Computers
  4. All remaining staff computers
  5. Student Lab Computers (must remain on campus)

  Start at 1 and move down list until all approved agents are deployed. If additional agents are needed for 1, 2, or 3 then submit and Add-On request when you are at ~90%.

Program Participation – NDR

- **Network Detection Response (NDR) pilot**
  - Nine School Systems have implemented the NDR pilot.
  - Pilot is closed to new customers while pilot benefits & costs are evaluated.

ESC Support

- Email Domain Security (SPF, DKIM, DMARC Conformance)
  - Configuration, No Cost
- Multi-Factor Authentication on ALL employee email accounts. (Microsoft 365 & Google Workspace)
  - Employee Awareness, Configuration, No Cost
- Restrict Local Admin Privileges
  - Employee Awareness, Configuration, No Cost

Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication Reporting & Conformance (DMARC)

K12 Cybersecurity Initiative Website

- https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative
  - Steps to onboarding School Systems to DIR STS portal can be accessed on this page
  - Updates about the program
  - Frequently asked questions about the program
  - Handy link to sign-up for the Cybersecurity Coordinator Forum meetings
  - Previous K12 Cybersecurity Initiative Webinars posted on this page

K12 Cybersecurity Contacts (priority assistance)

- SAIC
  - L_TXDIR_MSS_EDR@saic.com (EDR Support)
  - L_TXDIR_MSS_SOC@saic.com (Security Team) *
  - Toll Free Hotline 1.800.536.9706 (MSS SOC Team) *
- DIR
  - cirt@dir.texas.gov (cybersecurity incident response team) *
  - Toll Free Hotline (877) DIR-CISO (1.800.347.2476) *
- TEA
  - cybersecurity@tea.texas.gov
- ESC
  - Request from your ESC

DIR STS Portal (non-priority requests)

Other Operational Services Requests

- non-incident, operational requests
- quickly receive help for non-incident requests, such as user provisioning and removal, console login issues, agent installations, uninstalling agents, agent upgrades, whitelisting software, etc.
- please begin the **provide brief 40-character summary** field with "MSS -" followed by your summary description. This assures that the request is correctly routed to SAIC.
- https://txdir.servicenowservices.com/sp?id=sc_cat_item&sys_id=9d4bc3961318ab804210f65ed144b062&sysparm_category=9955beb91bfed054a04b74c8dc4bcbd7 *(requires STS Portal Access)*
  - Short link: http://bit.ly/47TmT1L

Update your School System Contacts

- Update AskTED
  - Technology Coordinator & Cybersecurity Coordinator
  - *Request assistance from your TED Administrator to update AskTED.*
- Update contact info with your ESC
  - Provide a primary and a backup contact
- Update contact info for STS Portal Access
  - Email terese.shade@dir.texas.gov if you have lost access
- Update contact info with SAIC SOC Team *
- Update all the above when Technology or Cybersecurity Coordinators change

New Goals – K12 Cybersecurity Initiative

- New goals are being developed and considered for FY26/27
- Survey went out on September 29th to School Systems
  - Please complete the survey once received. Your responses are essential for TEA to accurately assess the current impact and understand the cybersecurity needs of our school systems.

Texas Education Agency

K12 Cybersecurity Initiative Survey

Survey Update

- 764 Total Responses (57% of School Systems)

Participated in FY 24/25 K-12 Cybersecurity Initiative (Sept 2023-Aug 2025)	Participating
Yes	281
No	245
Unsure	179
total responses	705

Participated in FY 26/27 K-12 Cybersecurity Initiative (Sept 2025-Aug 2027)	Response
Unsure	197
Yes	137
No	62
total responses	396

FY 24/25 K-12 Cybersecurity Initiative Value (Sept 2023-Aug 2025)	Response
Extremely valuable	212
Somewhat valuable	45
Neutral	12
Not very valuable	1
Not valuable at all	1
total responses	271

K-12 Cybersecurity Initiative Services	Participating
Endpoint Detection & Response (EDR) - (DIR MSS SentinelOne or CrowdStrike)	209
Texas Cybersecurity Framework Assessment	88
ESC assistance with Email security protocol configuration (SPF DKIM DMARC)	82
ESC assistance with Multi-Factor Authentication implementation	52
ESC assistance with Local admin access restrictions	46
Network Detection & Response (NDR) Pilot	21
total responses	498

{ 344 School Systems using EDR }

Tell us what you need, what you really, really need!

Identified Needs	Count
Advanced phishing simulation & user training	333
Email filtering/gateway protection	311
Cloud security hardening (Microsoft 365 / Google Workspace)	294
Vulnerability management	288
Endpoint Management (patching and software deployment)	234
Cyber incident response planning or tabletop exercises	223
Off-Site Backups	197
Identity and Access Management (IAM)	149
Network segmentation	132
TCF-aligned policy templates	67

Other EDR's

EDR Solution	~Count
Scinary - w/ThreatDown	27
Crowdstrike	22
SentenalOne - (DeepSeas)	19
Microsoft Defender - 365/ADP/Endpoint/A5/EDR/Intune/Security	18
Bit Defender	16
Sophos - Central/Endpoint/X-Intercept	15
RSOC - ASU / Austin / UTRGV	14
Malwarebytes	9
Carbon Black	6
ThirtySeven4	6
FortiEDR	5
Microsoft	5
Scinary Cybersecurity	5
PC Matic - Pro/Endpoint Suite	4
Cortex (Palo Alto)	3
Datto by Kaseya	3
ESET	3
Symantec	3
Threatlocker	3
Trend Micro	3
Coro	2
ESC 17	2
Panda	2
SonicWall and ContentKeeper	2

Wazuh	2
Wolfe	2
Artic Wolf	1
BestLine Solutions	1
BlackSwan, and Crowdstrike	1
Carbon Black, but moving to SOPHOS XDR service due to the price hike announced	1
Check Point & CrowdStrike	1
Cisco	1
Crowdstrike and Palo Alto Cortex	1
Currently Sophos, but migrating to Texas A&M's Cybersecurity Services	1
Cylance	1
DIR	1
ESC 20 Sentinel One for servers and student devices	1
Farley's Tech	1
Heimdal Enterprise	1
Huntress and SentinelOne	1
MS Defender and Crowdstrike	1
MS Defender on client machines, ThreatDown on servers	1
Scinary and Malwarebytes	1
Scinary and Threatdown/Malwarebytes	1
Scinary Solutions	1
ThirtySeven4 Antivirus	1
VIPRE	1
Webroot by OpenText	1

Survey will close on midnight October 24th, 2025

~50 hours left to submit yours!

Email your ESC or our TEA team:

- If you have an error that your link is expired or is not working
- If you have not received/cannot find your unique survey link

K12cyber@tea.texas.gov

Texas Education Agency

Managed Endpoint Detection & Response (EDR)

Defining Managed EDR

- K-12 Cybersecurity Initiative includes Fully-Managed EDR
  - What is Endpoint Protection & Response (EDR)?
  - How does it differ from Antivirus?
  - What is Fully-Managed?

Standard Antivirus vs Endpoint Detection & Response

Texas Education Agency

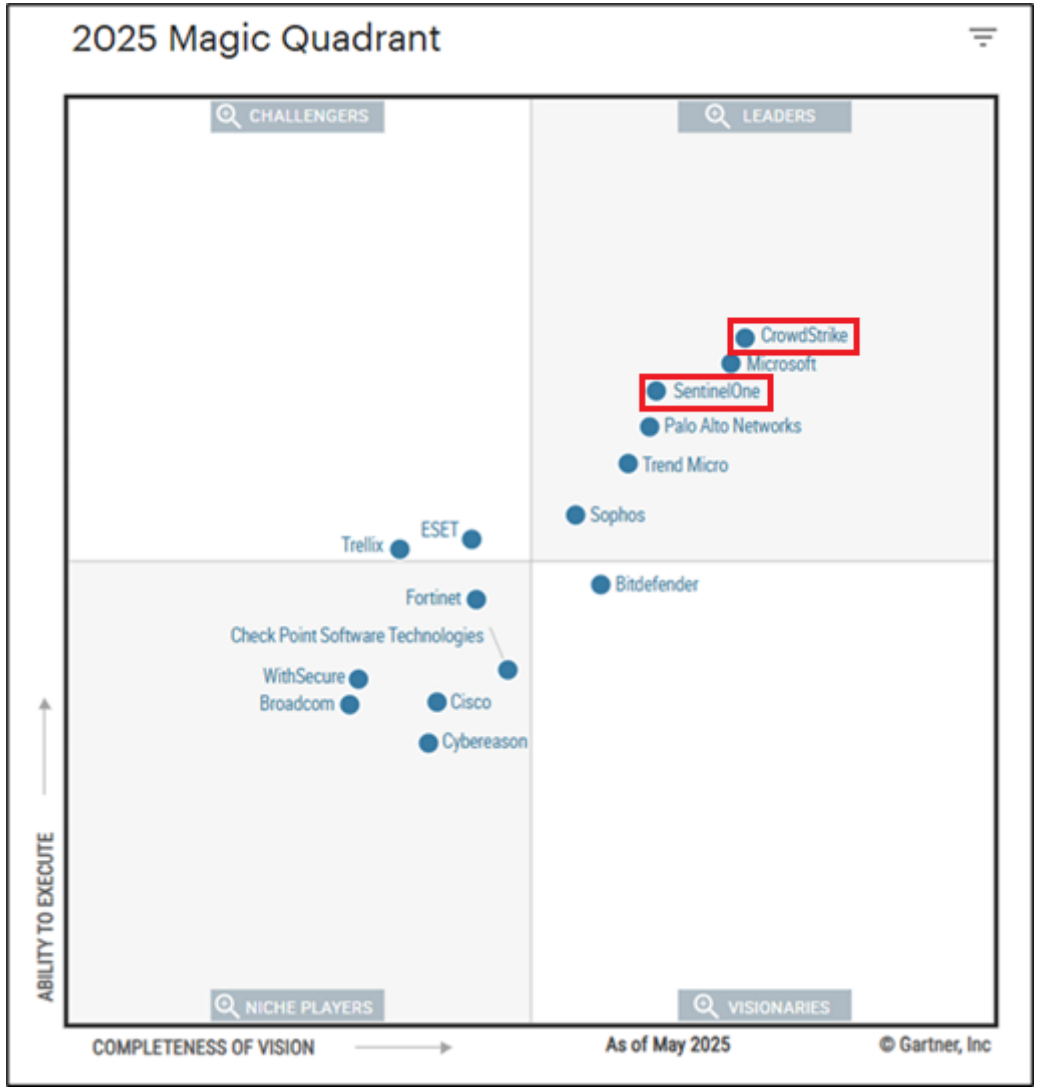
✅ Summary Table

Capability	Traditional AV	Advanced EDR
Signature-based detection	✅	✅
Behavioral / ML detection	⚠️ Limited	✅ Robust
Continuous telemetry	❌	✅
Threat hunting	❌	✅
Incident forensics	❌	✅
Automated response (kill/isolate/rollback)	⚠️ Partial	✅
Threat intelligence integration	❌	✅
MITRE ATT&CK mapping	❌	✅
Endpoint isolation	❌	✅
Rollback capability	❌	✅ (some)

24/7 Managed Endpoint Detection & Response (EDR)

- Includes a security operations center (SOC) team that:
  - Monitors endpoint alerts 24/7 – 365
    - SAIC, RSOC, Vendor
  - Analyzes alerts first and engages you only if a real threat requires attention
  - Can call you at 3am on a Saturday morning or act on a threat for you
  - Provides 100% hands free management or you can engage with SOC
  - Configures and tunes the EDR for you
  - {K-12 Cybersecurity Initiative – SAIC or RSOCs}
    - Threat intel is shared statewide and added to all customers
    - Apart from typical vendor threat feeds

Gartner Magic Quadrant - EDR



- **Leaders** – High completeness of vision and strong ability to execute.
- **Challengers** – Strong ability to execute but may lack a fully developed vision.
- **Visionaries** – Innovative and forward-thinking but may struggle with execution.
- **Niche Players** – Focused on a specific segment or capability, with limited execution or vision.

Source: www.gartner.com

Microsoft Defender vs Defender for Endpoint

🧩 Summary: Key Differentiators

Feature	Microsoft Defender Antivirus	Microsoft Defender for Endpoint
Service Name	`WinDefend`	`Sense`
Executable	`MsMpEng.exe`	`MsSense.exe`
Portal Visibility	None	Visible in Microsoft 365 Defender
Telemetry & Alerts	Local only	Cloud-based, centralized
EDR Capabilities	❌ No	✅ Yes
PowerShell Status	Basic AV status	Includes EDR mode (Active/Passive)

```
C:\>sc query sense

SERVICE_NAME: sense
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
```

Texas Education Agency

Cybersecurity News & Advisories

Breached Password Managers

- Compromised password managers, specifically Google's, continue to be reported by school systems.
- This has resulted in unauthorized access to Ascender (and other student information systems), enabling threat actors to alter employee banking details and redirect payroll deposits to fraudulent accounts.
- Regular training and enforcing vetted password management policies will empower staff to prevent these types of attacks.
- Changes to employee banking details should require manual validation before being committed.

Password Manager Best Practices

- Secure use of any password manager must include MFA.
- Your password manager password should be unique.
  - Not the same as or tied to a Google email account.
- Recovery email accounts for a password manager must require MFA.
- Individual privileged or important (e.g., banking, work) passwords should require MFA.
  - If your password manager is breached, this may be your only saving grace!
- Avoid the use of the built-in browser managers, they often lack more robust security features.

TX-ISAO

The Texas Information Sharing & Analysis Organization (TX-ISAO) is open to all organizations in Texas to include K-12.

- Established by DIR to enable Texas entities to share cybersecurity threat intelligence, best practices and remediation strategies.

ACTION: Please sign up for mailing list at the link below.

https://dir.texas.gov/txisao

- Cybersecurity Coordinator Forum – Save The Dates!
  - ~~November 26, 2025~~
  - ~~December 24, 2025~~
  - January 28, 2026 @ 11:00 AM CST
- We are only accepting registered school system emails to join the CCF, all others are removed. So please continue to use your work school email address when you sign up.
- What would you like included in the next CCF?
  - Email us: cybersecurity@tea.texas.gov

Stay Safe & Secure

Thank you!

Questions?

Email :

cybersecurity@tea.texas.gov