CITY OF AMESBURY
IN THE YEAR TWO THOUSAND TWENTY-FIVE

SPONSORED BY: Kassandra Gove **BILL No.** 2025-050
Kassandra Gove, Mayor

An Order to authorize the Mayor to accept and expend a grant in the amount of $40,000.00 from the Executive Office for Administration and Finance FY25 Community Compact Cabinet's (CCC) Information Technology grant program.

Summary: The Grant money will be used to purchase one year of service for Trend Micro's Vision One Managed Detection and Remediation product for both the City and the Schools. This product is a cyber-defense platform that uses real time monitoring of our email systems, cloud-based environments, and physical devices to block malicious attacks like viruses, phishing, malicious links, inappropriate data transmissions (including PII and PHI flagging), and suspicious activity. This product will monitor and block these types of attacks in real time, using AI and heuristics to determine violations and a technique called Sandboxing, to shunt suspicious activity to a private "bubble" allowing analysts (either IT or the Trend Micro support team) to examine the activity to determine if it should be permanently blocked or allowed.

Be it Ordered by the City Council of the City of Amesbury assembled, and by the authority of the same as follows:

That the City of Amesbury authorizes the Mayor to accept and expend a grant in the amount of $40,000.00 from the Executive Office for Administration and Finance FY25 Community Compact Cabinet's (CCC) Information Technology grant program.

EXECUTIVE OFFICE FOR ADMINISTRATION & FINANCE
COMMONWEALTH OF MASSACHUSETTS
STATE HOUSE - BOSTON, MA 02133
(617) 727-2040

MAURA T. HEALEY
GOVERNOR

KIMBERLEY DRISCOLL
LIEUTENANT GOVERNOR

MATTHEW J. GORZKOWICZ
SECRETARY

April 1, 2025

Dear Kassandra Gove,

It is with great pleasure that we inform you that the City of Amesbury has been awarded a $40,000 grant through the Community Compact Cabinet's (CCC) Information Technology grant program. Once again, this year, grant requests exceeded the program's available budget, reiterating the value of this program. Your application was chosen because it met the overarching goal of driving innovation and transformation at the local level via investments in technology.

We want to thank you for your continued efforts to make your community a better place by adopting best practices and striving for innovation. Your participation in the Community Compact program not only provided you with technical assistance, it also places you in a more competitive position for other state grants, including this IT program. The health of the Commonwealth's 351 cities and towns underpins the overall success of Massachusetts and its residents. Without the tireless efforts of folks like you, our communities wouldn't be the vibrant, thriving places they are today.

Attached are the grant documents that need to be completed to get the funds to your community. These should be sent to Jennifer McAllister (communitycompact@dor.state.ma.us) at the Division of Local Services (DLS) as soon as possible, but no later than April 18, 2025.

The receipt of grant funds is contingent upon the grantee being able to certify that it will comply with the Massachusetts General Laws, including G.L. c. 40A, § 3A, the MBTA Communities Act. Compliance with the MBTA Communities Act is determined by the Executive Office of Housing and Livable Communities.

Congratulations and thank you, again, for your tireless work to serve your community.

Sincerely,

Kimberley Driscoll

Kim Driscoll
Lieutenant Governor

Matthew J. Gorzkowicz

Matthew J. Gorzkowicz, Secretary
Executive Office for Administration and Finance

COMMONWEALTH OF MASSACHUSETTS ~ STANDARD CONTRACT FORM

This form is jointly issued and published by the Office of the Comptroller (CTR), the Executive Office for Administration and Finance (ANF), and the Operational Services Division (OSD) as the default contract for all Commonwealth Departments when another form is not prescribed by regulation or policy. The Commonwealth deems void any changes made on or by attachment (in the form of addendum, engagement letters, contract forms or invoice terms) to the terms in this published form or to the Standard Contract Form Instructions and Contractor Certifications, the Commonwealth Terms and Conditions for Human and Social Services or the Commonwealth IT Terms and Conditions which are incorporated by reference herein. Additional non-conflicting terms may be added by Attachment. Contractors are required to access published forms at CTR Forms: https://www.macomptroller.org/forms. Forms are also posted at OSD Forms: https://www.mass.gov/lists/osd-forms.

CONTRACTOR LEGAL NAME: (and d/b/a): City of Amesbury		**COMMONWEALTH DEPARTMENT NAME:** Executive Office of Administration & Finance **MMARS Department Code:** ANF	
Legal Address: (W-9, W-4):62 Friend Street, Amesbury MA 01913		**Business Mailing Address:**	
Contract Manager: Stephen Hare	**Phone:** (978) 393-0762	**Billing Address (if different):**	
E-Mail: hares@amesburyma.gov	**Fax:**	**Contract Manager:** Jennifer McAllister	**Phone:** 617-626-3838
Contractor Vendor Code: VC6000191693		**E-Mail:** mcallisterj@dor.state.ma.us	**Fax:**
Vendor Code Address ID (e.g. "AD001"): AD001 (Note: The Address ID must be set up for EFT payments.)		**MMARS Doc ID(s):** **RFR/Procurement or Other ID Number:**	

_X_ NEW CONTRACT

PROCUREMENT OR EXCEPTION TYPE: (Check one option only)

- __ **Statewide Contract** (OSD or an OSD-designated Department)
- __ **Collective Purchase** (Attach OSD approval, scope, budget)
- X **Department Procurement** (includes all Grants - 815 CMR 2.00) (Solicitation Notice or RFR, and Response or other procurement supporting documentation)
- __ **Emergency Contract** (Attach justification for emergency, scope, budget)
- __ **Contract Employee** (Attach Employment Status Form, scope, budget)
- __ **Other Procurement Exception** (Attach authorizing language, legislation with specific exemption or earmark, and exception justification, scope and budget)

_____ CONTRACT AMENDMENT

Enter **Current Contract End Date *Prior*** to Amendment: _____, 20___.

Enter **Amendment Amount:** $ _____. (or "no change")

AMENDMENT TYPE: (Check one option only. Attach details of amendment changes.)

- __ **Amendment to Date, Scope or Budget** (Attach updated scope and budget)
- __ **Interim Contract** (Attach justification for Interim Contract and updated scope/budget)
- __ **Contract Employee** (Attach any updates to scope or budget)
- __ **Other Procurement Exception** (Attach authorizing language/justification and updated scope and budget)

The Standard Contract Form Instructions and Contractor Certifications and the following Commonwealth Terms and Conditions document are incorporated by reference into this Contract and are legally binding: (Check ONE option): X Commonwealth Terms and Conditions __ Commonwealth Terms and Conditions For Human and Social Services __ Commonwealth IT Terms and Conditions

COMPENSATION: (Check ONE option): The Department certifies that payments for authorized performance accepted in accordance with the terms of this Contract will be supported in the state accounting system by sufficient appropriations or other non-appropriated funds, subject to intercept for Commonwealth owed debts under 815 CMR 9.00.

__ **Rate Contract.** (No Maximum Obligation) Attach details of all rates, units, calculations, conditions or terms and any changes if rates or terms are being amended.)

X **Maximum Obligation Contract.** Enter total maximum obligation for total duration of this contract (or ***new*** total if Contract is being amended). $40,000

PROMPT PAYMENT DISCOUNTS (PPD): Commonwealth payments are issued through EFT 45 days from invoice receipt. Contractors requesting **accelerated** payments must identify a PPD as follows: Payment issued within 10 days __% PPD; Payment issued within 15 days __ % PPD; Payment issued within 20 days __ % PPD; Payment issued within 30 days __% PPD. If PPD percentages are left blank, identify reason: X agree to standard 45 day cycle __ statutory/legal or Ready Payments (M.G.L. c. 29, § 23A); __ only initial payment (subsequent payments scheduled to support standard EFT 45 day payment cycle. See Prompt Pay Discounts Policy.)

BRIEF DESCRIPTION OF CONTRACT PERFORMANCE or REASON FOR AMENDMENT: (Enter the Contract title, purpose, fiscal year(s) and a detailed description of the scope of performance or what is being amended for a Contract Amendment. Attach all supporting documentation and justifications.) Community Compact Grant: This award is being made through the FY25 Community Compact IT Grant Program to the city of Amesbury for the costs associated with: cybersecurity infrastructure enhancement.

ANTICIPATED START DATE: (Complete ONE option only) The Department and Contractor certify for this Contract, or Contract Amendment, that Contract obligations:

X 1. may be incurred as of the Effective Date (latest signature date below) and no obligations have been incurred prior to the Effective Date.

__ 2. may be incurred as of _____, 20___, a date **LATER** than the Effective Date below and no obligations have been incurred **prior** to the Effective Date.

__ 3. were incurred as of _____, 20___, a date **PRIOR** to the Effective Date below, and the parties agree that payments for any obligations incurred prior to the Effective Date are authorized to be made either as settlement payments or as authorized reimbursement payments, and that the details and circumstances of all obligations under this Contract are attached and incorporated into this Contract. Acceptance of payments forever releases the Commonwealth from further claims related to these obligations.

CONTRACT END DATE: Contract performance shall terminate as of October 31, 2026 with no new obligations being incurred after this date unless the Contract is properly amended, provided that the terms of this Contract and performance expectations and obligations shall survive its termination for the purpose of resolving any claim or dispute, for completing any negotiated terms and warranties, to allow any close out or transition performance, reporting, invoicing or final payments, or during any lapse between amendments.

CERTIFICATIONS: Notwithstanding verbal or other representations by the parties, the **"Effective Date"** of this Contract or Amendment shall be the latest date that this Contract or Amendment has been executed by an authorized signatory of the Contractor, the Department, or a later Contract or Amendment Start Date specified above, subject to any required approvals. The Contractor certifies that they have accessed and reviewed all documents incorporated by reference as electronically published and the Contractor makes all certifications required under the Standard Contract Form Instructions and Contractor Certifications under the pains and penalties of perjury, and further agrees to provide any required documentation upon request to support compliance, and agrees that all terms governing performance of this Contract and doing business in Massachusetts are attached or incorporated by reference herein according to the following hierarchy of document precedence, the applicable Commonwealth Terms and Conditions, this Standard Contract Form, the Standard Contract Form Instructions and Contractor Certifications, the Request for Response (RFR) or other solicitation, the Contractor's Response (excluding any language stricken by a Department as unacceptable, and additional negotiated terms, provided that additional negotiated terms will take precedence over the relevant terms in the RFR and the Contractor's Response only if made using the process outlined in 801 CMR 21.07, incorporated herein, provided that any amended RFR or Response terms result in best value, lower costs, or a more cost effective Contract.

AUTHORIZING SIGNATURE FOR THE CONTRACTOR:

X: _____. Date: _____,
(Signature and Date Must Be Captured At Time of Signature)

Print Name: _____.

Print Title: _____.

AUTHORIZING SIGNATURE FOR THE COMMONWEALTH:

X: _____. Date: _____,
(Signature and Date Must Be Captured At Time of Signature)

Print Name: Sean Cronin

Print Title: DOR Sr. Deputy Commissioner for Local Services

STANDARD CONTRACT FORM INSTRUCTIONS
CONTRACTOR CERTIFICATIONS
COMMONWEALTH TERMS AND CONDITIONS

INSTRUCTIONS

The following Instructions, Contractor Certifications and the applicable Commonwealth Terms and Conditions are incorporated by reference into an executed Standard Contract Form. Instructions are provided to assist with completion of the Standard Contract Form. Additional terms are incorporated by reference. Links to legal citations are to unofficial versions and Departments and Contractors should consult with their legal counsel to ensure compliance with all legal requirements. Please note that not all applicable laws have been cited.

Contractor Legal Name (and D/B/A): Enter the **Full Legal Name** of the Contractor's business as it appears on the Contractor's W-9 or W-4 Form (Contract Employees only) and the applicable Commonwealth Terms and Conditions. If Contractor also has a "doing business as" (d/b/a) name, BOTH the legal name and the "d/b/a" name must appear in this section.

Contractor Legal Address: Enter the Legal Address of the Contractor as it appears on the Contractor's W-9 or W-4 Form (Contract Employees only) which must match the legal address on the 1099I table in MMARS (or the Legal Address in HR/CMS for a Contract Employee).

Contractor Contract Manager: Enter the authorized Contract Manager who will be responsible for managing the Contract. The Contract Manager should be an Authorized Signatory or, at a minimum, a person designated by the Contractor to represent the Contractor, receive legal notices and negotiate ongoing Contract issues. The Contract Manager is considered "Key Personnel" and may not be changed without the prior written approval of the Department. If the Contract is posted on COMMBUYS, the name of the Contract Manager must be included in the Contract on COMMBUYS.

Contractor E-Mail Address/Phone/Fax: Enter the electronic mail (e-mail) address, phone and fax number of the Contractor Contract Manager. This information must be kept current by the Contractor to ensure that the Department can contact the Contractor and provide any required legal notices. Notice received by the Contract Manager (with confirmation of actual receipt) through the listed address, fax number(s) or e-mail address will meet any written legal notice requirements.

Contractor Vendor Code: The Department must enter the MMARS Vendor Code assigned by the Commonwealth. If a Vendor Code has not yet been assigned, leave this space blank and the Department will complete this section when a Vendor Code has been assigned. The Department is responsible under the Vendor File and W-9s Policy for verifying with authorized signatories of the Contractor, as part of contract execution, that the legal name, address and Federal Tax Identification Number (TIN) in the Contract documents match the state accounting system.

Vendor Code Address ID: (e.g., "AD001") The Department must enter the MMARS Vendor Code Address ID identifying the payment remittance address for Contract payments, which MUST be set up for EFT payments PRIOR to the first payment under the Contract in accordance with the Bill Paying and Vendor File and W-9 policies.

Commonwealth Department Name: Enter the full Department name with the authority to obligate funds encumbered for the Contract.

Commonwealth MMARS Alpha Department Code: Enter the three (3) letter MMARS Code assigned to this Commonwealth Department in the state accounting system.

Department Business Mailing Address: Enter the address where all formal correspondence to the Department must be sent. Unless otherwise specified in the Contract, legal notice sent or received by the Department's Contract Manager (with confirmation of actual receipt) through the listed address, fax number(s) or e-mail address for the Contract Manager will meet any requirements for legal notice.

Department Billing Address: Enter the Billing Address or e-mail address if invoices must be sent to a different location. Billing, confirmation of delivery or performance issues should be resolved through the listed Contract Managers.

Department Contract Manager: Identify the authorized Contract Manager who will be responsible for managing the Contract, who should be an authorized signatory or an employee designated by the Department to represent the Department to receive legal notices and negotiate ongoing Contract issues.

Department E-Mail Address/Phone/Fax: Enter the e-mail address, phone and fax number of the Department Contract Manager. Unless otherwise specified in the Contract, legal notice sent or received by the Contract Manager (with confirmation of actual receipt) through the listed address, fax number(s) or e-mail address will meet any requirements for written notice under the Contract.

MMARS Document ID(s): Enter the MMARS 20-character encumbrance transaction number associated with this Contract, which must remain the same for the life of the Contract. If multiple numbers exist for this Contract, identify all Document IDs.

RFR/Procurement or Other ID Number or Name: Enter the Request for Response (RFR) or other Procurement Reference number, Contract ID Number or other reference or tracking number for this Contract or Amendment which will be entered into the Board Award Field in the MMARS encumbrance transaction for this Contract.

NEW CONTRACTS (Left Side of Form):

Complete this section ONLY if this Contract is brand new. (Complete the CONTRACT AMENDMENT section for any material changes to an existing or an expired Contract, and for exercising options to renew or annual contracts under a multi-year procurement or grant program.)

Procurement or Exception Type: Check the appropriate type of procurement or exception for this Contract. Only one option can be selected. See the Office of the Comptroller Guidance for Vendors Policies (State Finance Law and General Requirements, Acquisition Policy and Fixed Assets) and the Operational Services Division Conducting Best Value Procurements Handbook for details.

Statewide Contract (OSD or an OSD-designated Department): Check this option for a Statewide Contract under OSD, or by an OSD-designated Department.

Collective Purchase approved by OSD: Check this option for Contracts approved by OSD for collective purchases through federal, state, or local government or other entities.

Department Procurement: Check this option for a Department contract procurement including state grants and federal sub-grants under 815 CMR 2.00 and State Grants and Federal Subgrants Policy, Departmental Master Agreements (MA). If this is a multi-Department user Contract, state that multi-Department use is allowable in the section labeled "Brief Description."

Emergency Contract: Check this option when the Department has determined that an unforeseen crisis or incident has arisen which requires or mandates immediate purchases to avoid substantial harm to the functioning of government, the provision of necessary or mandated services, or where the health, welfare or safety of clients or other persons or serious damage to property is threatened.

Contract Employee: Check this option when the Department requires the performance of an Individual Contractor, and when the planned Contract performance with an Individual has been classified using the Employment Status

Solution Brief

TREND MICRO™

Trend Vision One™

Integrated attack surface management (ASM) and extended detection and response (XDR)

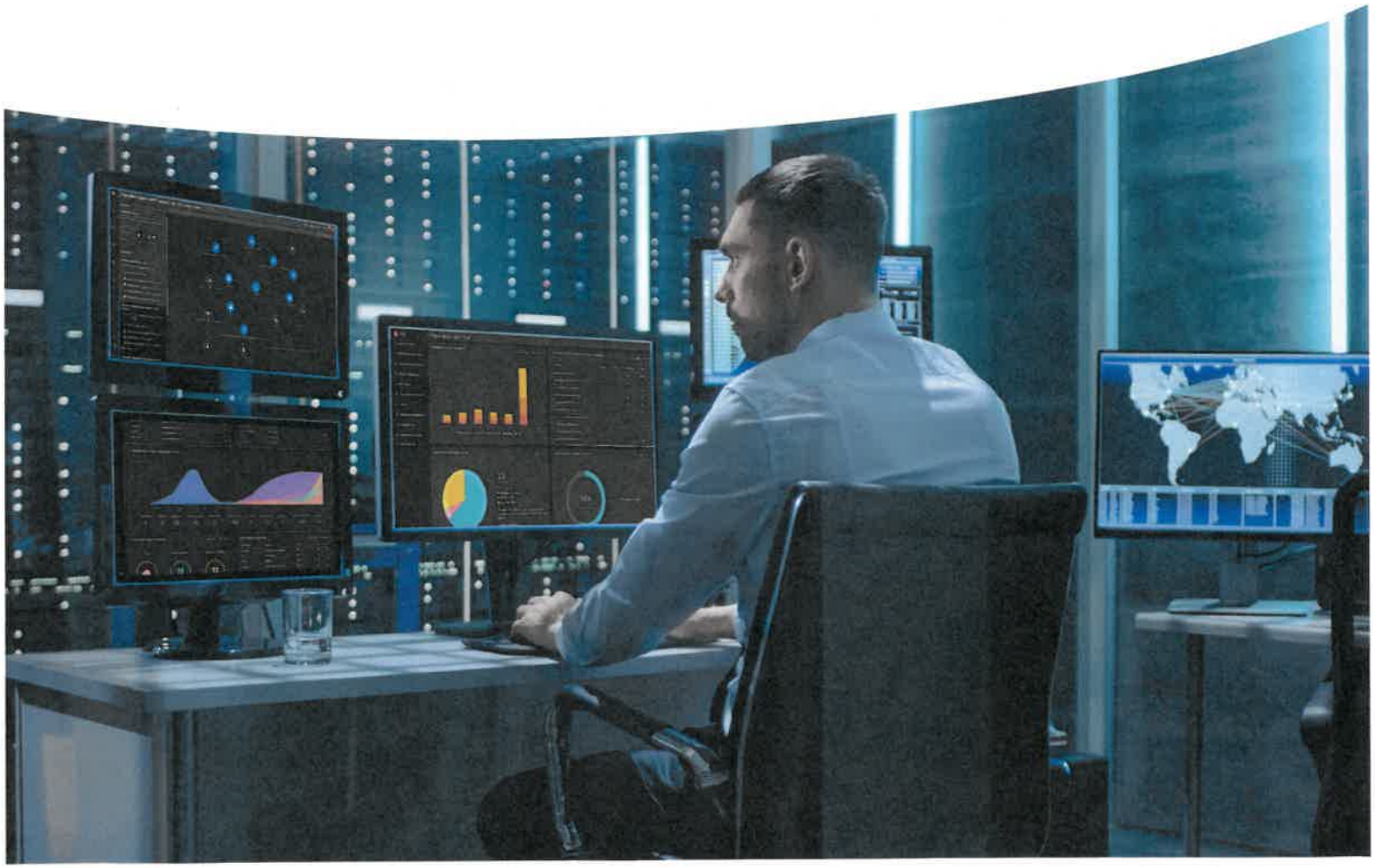
Today, many organizations leverage multiple, disconnected security solutions to identify and assess risk, take inventory of assets, and detect and respond to threats across their email, endpoints, servers, cloud infrastructure, and networks. Unfortunately, this has led to limited visibility across the enterprise and an overload of uncorrelated alerts.

Market trends and security challenges like cloud migration, digital transformation, hybrid work, and shadow IT projects continue to evolve and propagate. Security teams must confront even more risk factors to prevent potential attacks and breaches from materializing.

Attacks or threats represent a critical but singular risk factor within the corporate environment. Proactively addressing additional areas of risk—including unknown and unmanaged assets, weak or misconfigured security controls, vulnerable assets (like unpatched operating systems), and cloud misconfigurations—can significantly influence overall security posture and reduce the likelihood of an attack occurring.

Working across disparate security tools creates challenges like tedious, manual investigation processes and dangerous blind spots, which provide adversaries the opportunity to more easily hide and maneuver within the corporate environment. This limited visibility into the environment and an attacker's tactics, techniques, and procedures (TTP) can result in an inadequate and incomplete response.

As ransomware, fatigue, data breach, destruction, and fileless attacks increase in volume, a risk- centric approach to attack surface management (ASM) and XDR is required to strengthen security resiliency of your organization. Your SOC and security teams need advanced tools to proactively improve security posture, detect and respond faster, track and benchmark risk, and optimize overall security and IT operations. This means leveraging the capabilities of an AI-powered, unified, and all-empowering cybersecurity platform.



Introducing Trend Vision One

Our cloud-native security operations platform—optimized for cloud, hybrid, and on-premises environments—combines ASM and XDR in a single, unified console to effectively manage cyber risk across your organization.

Empower your team with comprehensive risk insights, earlier threat detection, and automated risk and threat response options—all bolstered and made more efficient with the help of AI. Utilize the platform's predictive machine learning and advanced security analytics for a broader perspective and advanced context.

Trend Vision One integrates with its own expansive protection platform portfolio and industry-leading global threat intelligence in addition to a broad ecosystem of purpose-built and API-driven third-party integrations.
This allows you to ingest and normalize activity and detection telemetry across the user environment.

Open or hybrid-first XDR and ASM security providers rely on other vendors. The customer receives inefficiently correlated detection logs from third parties to surface low-fidelity threat events and a more limited asset inventory and incomplete risk assessment. This strategy leads to slower detection, more blind spots, and greater potential for partial remediation.

Trend Vision One delivers the broadest native XDR sensor coverage in the cybersecurity market. The platform's native-first, hybrid approach to XDR and ASM benefits your security teams by delivering richer activity telemetry—not just detection data—across security layers with full context and understanding.
This results in earlier, more precise risk and threat detection and more efficient investigation.

Security and SOC analysts, threat hunters, and senior security leaders across your organization are given the tools to contextualize risk and reduce the likelihood of attacks—all while reducing false positives and noise within the environment continuously and proactively.

Anticipate your adversaries and develop more proactive and resilient programs by providing in-depth coverage across the attack surface risk management lifecycle. Trend Vision One identifies internal and internet-facing assets, assesses individual assets and company-wide risk, and provides custom, intelligent remediation recommendations while addressing your detection and response needs concurrently.

Figure one: overview of Trend Vision One platform capabilities and unified solutions

Trend Micro™ Zero Trust Secure Access (ZTSA)

follows the principles of zero-trust networking. Strengthen your overall security posture by enforcing strong access control permissions from multiple identity services across the organization.

Rather than granting access to the entire network, as a VPN does, ZTSA provides a gateway to specific applications and resources, restricting access to everything within the network that is not being employed. If valid user credentials are stolen, the level of access they will grant to the organization can be contained, effectively reducing the blast area of any attack.

Purpose-built XDR, Attack surface risk management (ASRM), and zero-trust capabilities

The expansive threat landscape, combined with the evolving role of security within the modern enterprise, demands an integrated and proactive approach. Trend Vision One empowers your team at every stage of the risk and threat lifecycle with intuitive applications to detect, hunt, investigate, analyze, and respond–and automatically surface prioritized risks and vulnerabilities.

This approach eases your security operations while providing the right information at the right time. Enable the streamlined development of plans. reduce risk, and improve key performance indicators like mean time to detect, patch, and respond–all while reducing the volume of security alerts your analysts face daily.

Actionable, predictive risk insights

Trend Vision One™ – Attack Surface Risk Management (ASRM) synthesizes 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 analysts are given the opportunity to examine and filter assets, vulnerabilities, and key metrics in more detail. ASRM offers central visibility into your attack surface inventory, cyber risk score, vulnerable assets, predicted impact, operations efficiency, and recommended remediation tactics.

- **Leading ASM:** Leverage first-to-market technology to deliver broad coverage for internal and internet-facing (external) attack surface discovery, risk assessment and vulnerability prioritization, and automated risk and threat remediation
- **Complete coverage**: Risk index, attack index, exposure index, and security misconfiguration trends track the attack pressure, threat and exploit impact, unpatched vulnerabilities, and misconfigurations within your environment

ASRM delivers a single source for security leaders, security operations, and IT operations across your organization, enabling you to observe and evaluate your entire IT environment at varying and appropriate levels of detail.

Trend Vision One automatically measures and weighs different risk factors including vulnerabilities, security controls and misconfigurations, asset criticality, XDR detections, account compromise, anomalies, and cloud activity data. The information it gathers is then used to predict potential gaps for exploitation as well as automate and accelerate mitigation actions across people, processes, and technology.

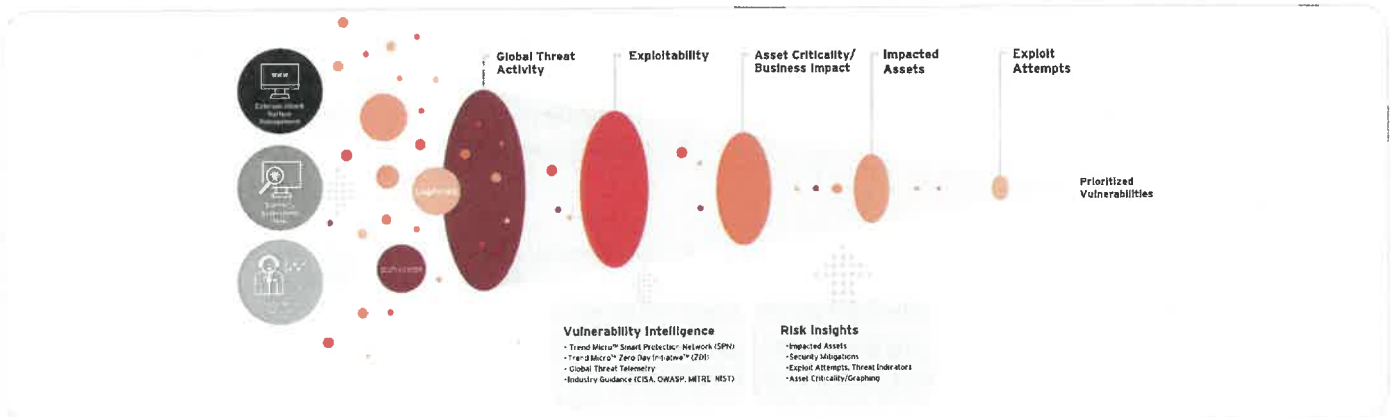
Trend is a Leader in Gartner Magic Quadrant for EPP since 2002, 19 times in a row

A Leader in the Forrester New Wave™: Extended Detection and Response, Q4 2021

A Leader in The Forrester Wave™: Endpoint Security, Q4 2023 - with the highest score in the strategy category

Customers' Choice in 2024 Voice of the Customer for Network Detection and Response, Midsize Enterprise ($50M - $1B)

Figure two: overview of protection layers



Supercharge your XDR capabilities

XDR correlates data across multiple security layers—including endpoint, server, email, identity, mobile, cloud workload, and network—from native sensors, global threat intelligence feeds, and third-party data sources. A single pane of glass allows you to detect, investigate, and respond to suspicious behavior, malware, ransomware, disruption, and other critical attacks. XDR works across different security vectors to reduce silos and detect threats that have evaded your protection technology.

According to ESG, organizations with Trend XDR are 2.2 times more likely to detect an attack, save up to 79% on security costs, and improve response time by 70%.

- **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
- **Optimized detection modeling:** Threat intelligence incorporates more sources and research insight to enrich detection and investigation to deliver greater context to your team
- **Faster investigation:** By quickly visualizing 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 prioritize, automate, and accelerate response actions from one location

Experience Trend Vision One

Platform trial

Explore the entire Trend Vision One platform free for 30 days. Access powerful XDR capabilities, leading attack surface management tools, and award-winning global threat intelligence.

Get started today

Essential access for Trend protection customers

Trend customers are entitled to complimentary Trend Vision One™ Essential Access for the duration of their protection product license.

Activate your account

Essential Access includes a subset of Trend Vision One features including:

Reporting and visibility
- Executive dashboard
- Operations dashboard

Assessment: uncover malicious activity
- At-risk mailbox
- At-risk endpoint
- At-risk users
- At-risk cloud apps
- Trend Phishing Simulation

Threat intelligence
- Intelligence report
- Suspicious object management
- Third-party intelligence (TAXII, MISP)
- Campaign intelligence
- Vulnerability intelligence

Workflow and automation
- Third-party integration
- Service gateway
- Playbooks

Solution connector
- Protection solution connection

Threat identification and hunting
- Targeted attack detection
- Search

Admin
- Audit logs
- Credit usage
- User accounts
- Notifications
- Console and support settings

About Trend Micro

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, our unified cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints.

With 7,000 employees across 65 countries, and the world's most advanced global threat research and intelligence, Trend enables organizations to simplify and secure their connected world.

TrendMicro.com

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy