Cy-Napea®

powered by Aurora Consolidated Ltd.

Secure Your Digital Future

Introduction to Aurora Consolidated Ltd.

Founded in 2016, based in Bulgaria.

Specializes in corporate SaaS software and consulting services.

Known for integrating AI into their solutions.

Owns the trademark **Cy-Napea**®, a comprehensive cybersecurity platform.

Overview of Cy-Napea®

Advanced cybersecurity solution.

Features: EDR, XDR, EDRR, MDR.

Intelligent threat recognition and real-time response.

Used in the US, Europe, and Asia.

Key Features of Cy-Napea®

EDR: Monitors and responds to endpoint threats.

XDR: Integrates multiple security products for unified threat detection.

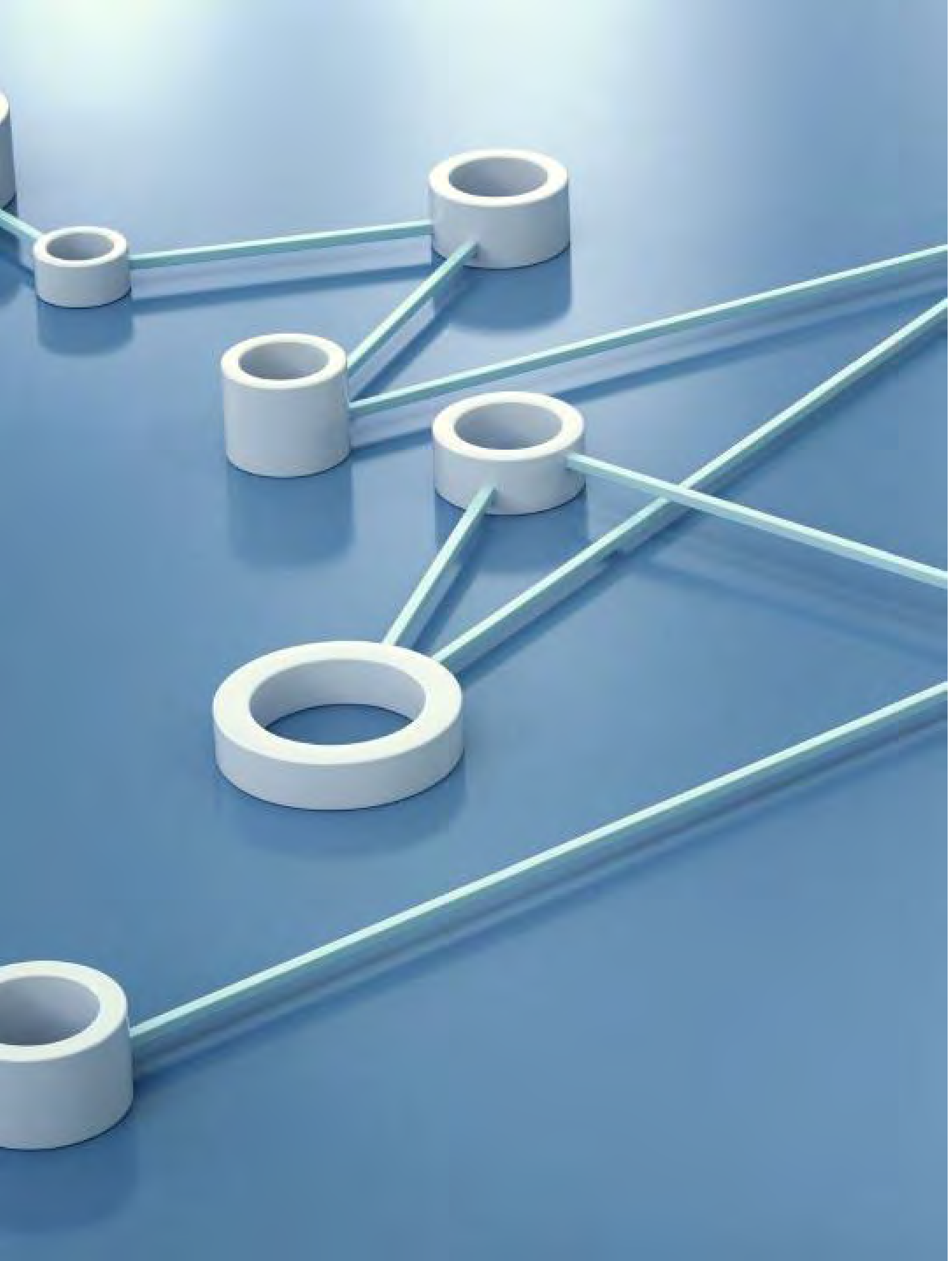
EDRR: Adds automated recovery to EDR.

MDR: Outsourced threat monitoring and management.

DLP: Protects sensitive data.

Anti-Ransomware: Shields systems from ransomware.

Centralized Management: Simplifies security policy management.



What is a Cybersecurity Platform?

- **Definition**: A centralized solution for managing and securing an organization’s data, users, and network.
- **Components**: Integrates various security tools such as threat detection, response, and prevention into a unified system.
- **Benefits**: Simplifies security management, enhances threat detection and response, and reduces the attack surface by consolidating security functions

Difference Between Cybersecurity Platform and Antivirus Program

Scope:

Antivirus Program: Focuses on detecting and removing known malware from individual devices.

Cybersecurity Platform: Provides comprehensive protection across the entire network, including endpoints, cloud environments, and more.

Functionality:

Antivirus Program: Uses signature-based detection to identify threats.

Cybersecurity Platform: Utilizes advanced techniques like behavioral analysis, AI, and machine learning for proactive threat detection and response

Management:

Antivirus Program: Typically managed on a per-device basis.

Cybersecurity Platform: Centralized management for all security functions, providing a unified view and control4

Why Do We Need Cybersecurity Solutions?

- **Threat Landscape**: Increasingly sophisticated cyber threats require advanced security measures beyond traditional antivirus programs.

- **Business Continuity**: Protects against data breaches, ransomware, and other cyber incidents that can disrupt operations and cause financial losses.

- **Data Protection**: Ensures the confidentiality, integrity, and availability of sensitive information, safeguarding against unauthorized access and data breaches.

Compliance with NIS2

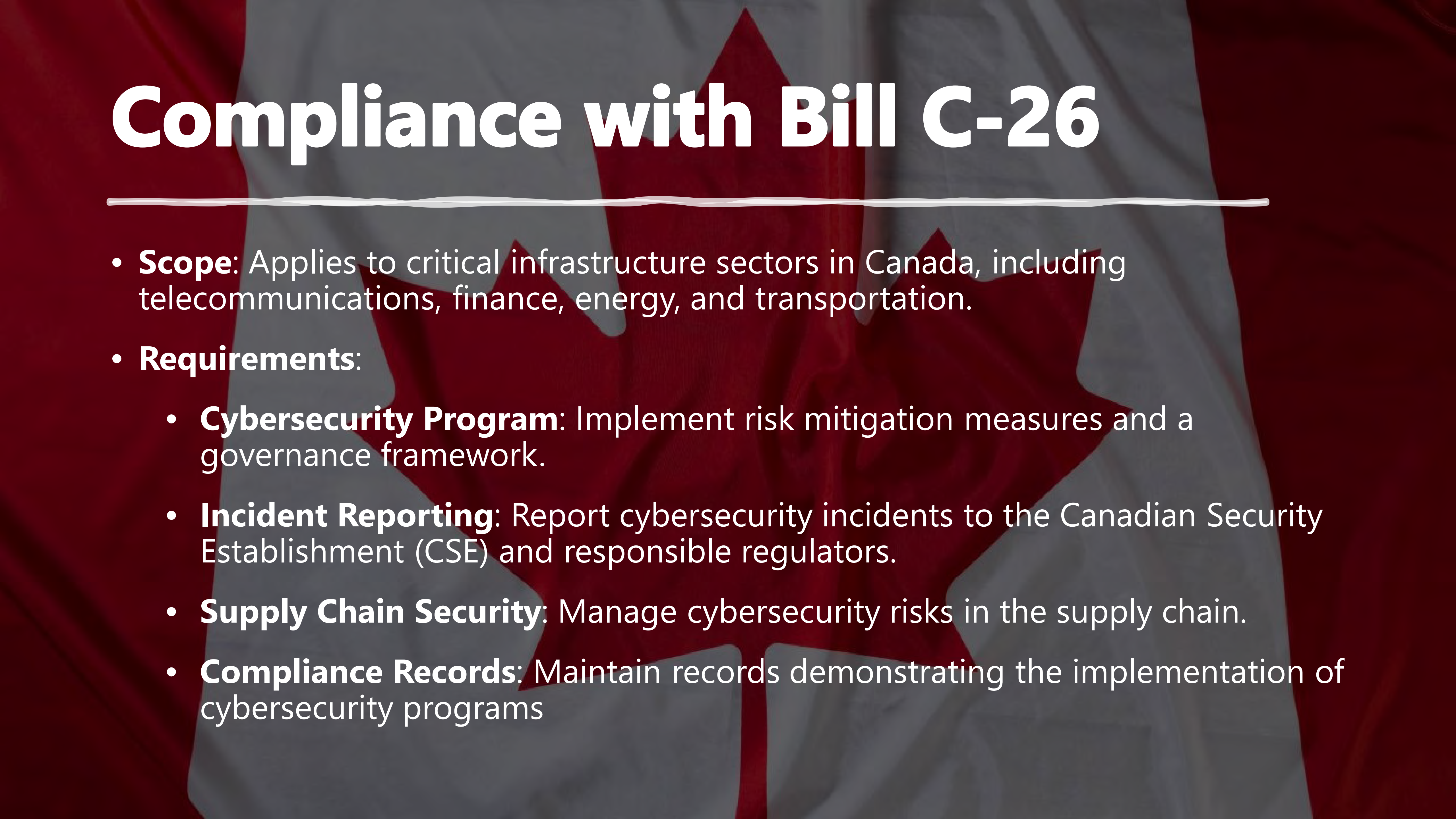
- **Scope**: Applies to essential and important entities in sectors like energy, transport, banking, healthcare, and digital infrastructure.
- **Requirements**:
  - **Risk Management**: Implement robust risk management practices.
  - **Incident Reporting**: Report significant cybersecurity incidents within 24 hours.
  - **Supply Chain Security**: Ensure third-party providers comply with cybersecurity measures.
  - **Business Continuity**: Develop plans for system recovery and emergency procedures

Compliance with Digital Operational Resilience Act (DORA)

- **Scope**: Applies to financial entities within the EU.
- **Requirements**:
  - **ICT Risk Management**: Establish frameworks to identify, assess, and mitigate ICT risks.
  - **Incident Reporting**: Report significant ICT-related incidents to competent authorities.
  - **Resilience Testing**: Conduct regular digital operational resilience testing.
  - **Third-Party Risk Management**: Ensure third-party providers adhere to ICT risk management standards

Compliance with PSD2

- **Scope**: Applies to banks, financial institutions, and payment service providers in the EU.
- **Requirements**:
  - **Strong Customer Authentication (SCA)**: Implement multi-factor authentication for user login.
  - **Open API**: Provide APIs for third-party access to customer information.
  - **Customer Transparency**: Clearly communicate terms, conditions, and currency conversion rates.
  - **Complaint Resolution**: Resolve consumer complaints promptly



Compliance with Bill C-26

- **Scope**: Applies to critical infrastructure sectors in Canada, including telecommunications, finance, energy, and transportation.
- **Requirements**:
  - **Cybersecurity Program**: Implement risk mitigation measures and a governance framework.
  - **Incident Reporting**: Report cybersecurity incidents to the Canadian Security Establishment (CSE) and responsible regulators.
  - **Supply Chain Security**: Manage cybersecurity risks in the supply chain.
  - **Compliance Records**: Maintain records demonstrating the implementation of cybersecurity programs

Compliance with HIPAA

- **Scope**: Applies to healthcare providers, health plans, and healthcare clearinghouses in the US.
- **Requirements**:
    - **Privacy Rule**: Protect the privacy of individuals' health information.
    - **Security Rule**: Ensure the confidentiality, integrity, and availability of electronic health information.
    - **Breach Notification Rule**: Notify affected individuals and authorities of data breaches

Compliance with GLBA

- **Scope**: Applies to financial institutions in the US.
- **Requirements**:
  - **Privacy Notices**: Inform customers about information-sharing practices.
  - **Opt-Out Rights**: Allow customers to opt-out of information sharing with third parties.
  - **Safeguards Rule**: Implement an information security program to protect customer data

Compliance with China Cybersecurity Law

- **Scope**: Applies to network operators and businesses in critical sectors in China.
- **Requirements**:
    - **Data Localization**: Store select data within China.
    - **Security Obligations**: Implement measures to safeguard network operations and prevent data breaches.
    - **Incident Reporting**: Report cybersecurity incidents to authorities

Compliance with Information Technology Act, 2000

- **Scope**: Applies to electronic transactions, digital signatures, and cybercrimes in India.
- **Requirements**:
  - **Data Protection**: Implement reasonable security practices to protect personal data.
  - **Cybersecurity Measures**: Ensure the security of electronic records and digital signatures.
  - **Incident Reporting**: Report cybersecurity incidents to the relevant authorities

Compliance with Act on the Protection of Personal Information (APPI)

- **Scope**: Applies to businesses handling personal information in Japan.
- **Requirements**:
  - **Consent**: Obtain consent before collecting, using, or sharing personal information.
  - **Data Protection**: Implement security measures to protect personal information.
  - **Cross-Border Transfers**: Obtain informed consent for transferring personal information outside Japan

Compliance with Personal Data Protection Act (PDPA)

- **Scope**: Applies to organizations collecting, using, or disclosing personal data in Singapore.
- **Requirements**:
    - **Consent**: Obtain consent before collecting, using, or disclosing personal data.
    - **Data Protection**: Implement measures to protect personal data from unauthorized access and breaches.
    - **Access and Correction**: Allow individuals to access and correct their personal data.

Compliance with Privacy Act 1988

- **Scope**: Applies to Australian government agencies and private sector organizations.
- **Requirements**:
  - **Australian Privacy Principles (APPs)**: Follow 13 principles covering the collection, use, and disclosure of personal information.
  - **Data Security**: Implement measures to protect personal information.
  - **Access and Correction**: Allow individuals to access and correct their personal information.

Cybersecurity Awareness Training (CAT)

- Educates employees on cybersecurity threats.
- Covers phishing, malware, and social engineering.
- Delivered through online courses, phishing exercises, simulated attacks, and on-demand resources.

Cybersecurity Awareness Training (CAT)

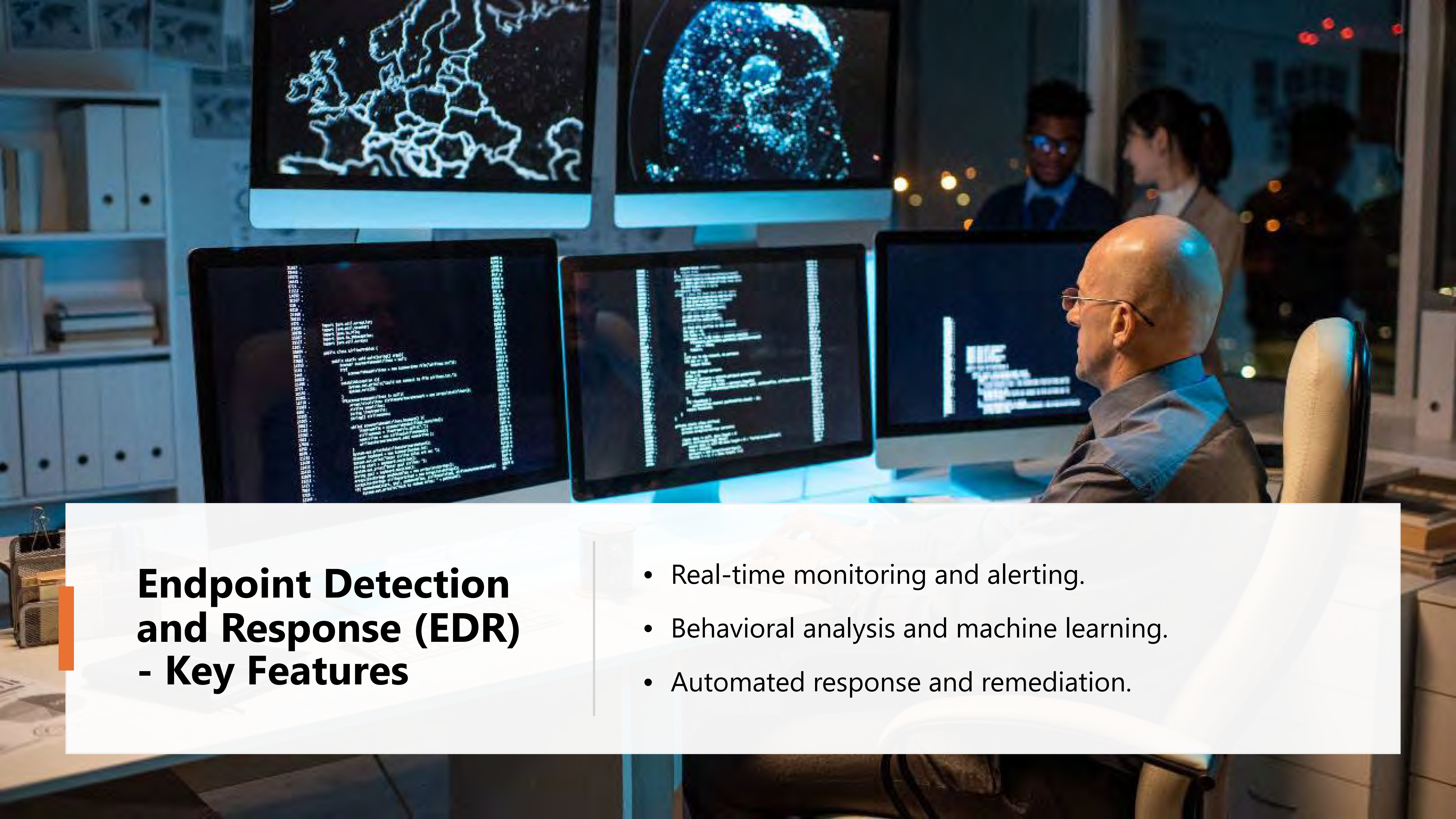
- **Online Training**: Self-paced lessons.
- **Phishing Exercises**: Test recognition of phishing threats.
- **Simulated Attacks**: Real-world attack simulations.
- **On-Demand Resources**: Quick access to training materials.

Cybersecurity Awareness Training (CAT) - Benefits of CAT

- Increases awareness of security threats.
- Meets compliance requirements for GDPR, SOC2, HIPAA, and more.
- Reduces risk of data breaches.
- Improves overall security culture.

Endpoint Detection and Response (EDR)

- **Functionality**: Continuously monitors endpoints to detect and respond to cyber threats.
- **Benefits**: Provides real-time visibility, reduces response time, and enhances threat detection accuracy.



Endpoint Detection and Response (EDR) - Key Features

- Real-time monitoring and alerting.
- Behavioral analysis and machine learning.
- Automated response and remediation.

Endpoint Detection and Response (EDR) - EDR in Action

DETECTS AND ISOLATES THREATS AT THE ENDPOINT LEVEL.

PROVIDES DETAILED FORENSIC DATA FOR INCIDENT ANALYSIS.

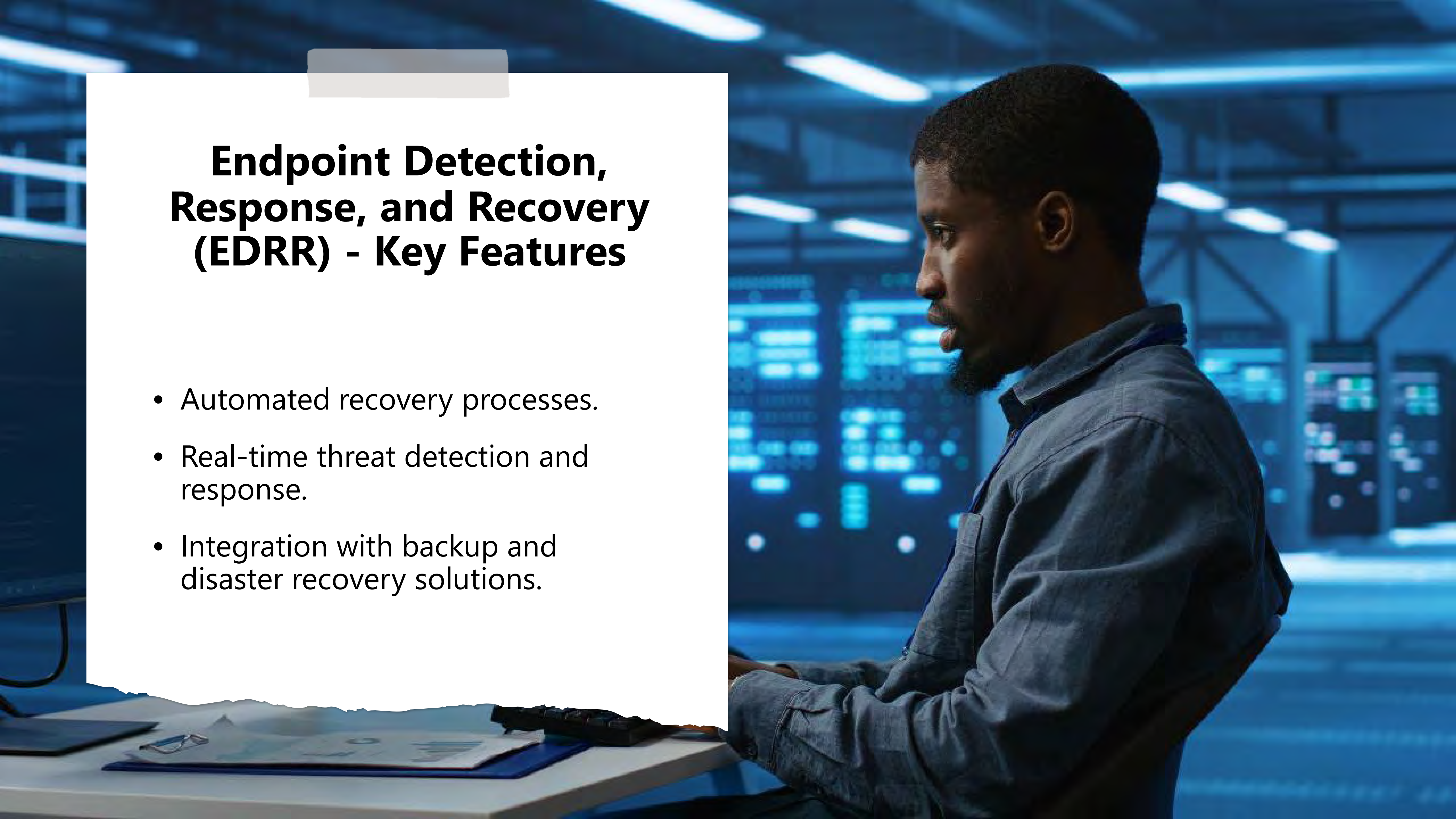
INTEGRATES WITH OTHER SECURITY TOOLS FOR COMPREHENSIVE PROTECTION.

Endpoint Detection, Response, and Recovery (EDRR)

- **Functionality**: Adds automated recovery capabilities to traditional EDR.
- **Benefits**: Ensures quick recovery from cyber incidents, minimizes downtime, and enhances overall resilience.

Endpoint Detection, Response, and Recovery (EDRR) - Key Features

- Automated recovery processes.
- Real-time threat detection and response.
- Integration with backup and disaster recovery solutions.



Endpoint Detection, Response, and Recovery (EDRR) - EDRR in Action

RAPID RECOVERY FROM RANSOMWARE ATTACKS.

MINIMIZES OPERATIONAL DISRUPTIONS.

ENSURES DATA INTEGRITY AND AVAILABILITY.

Extended Detection and Response (XDR)

- **Functionality**: Integrates data from multiple security layers, including endpoints, networks, and cloud environments.
- **Benefits**: Provides a unified view of threats, improves threat detection, and reduces complexity.

Extended Detection and Response (XDR) - Key Features

- Multi-layered threat detection.
- AI-powered insights and analytics.
- Unified threat management platform.

Extended Detection and Response (XDR) - XDR in Action

Detects and responds to advanced threats across the entire IT environment.

Enhances visibility and control over security operations.

Reduces the time to detect and respond to incidents.

Managed Detection and Response (MDR)

- **Functionality**: Provides outsourced monitoring and management of security threats.
- **Benefits**: Offers expert threat detection and response, reduces the burden on internal teams, and ensures 24/7 security coverage.

Managed Detection and Response (MDR) - Key Features

- 24/7 monitoring by cybersecurity experts.
- Proactive threat hunting and incident response.
- Regular, detailed security reports.

Managed Detection and Response (MDR) - MDR in Action

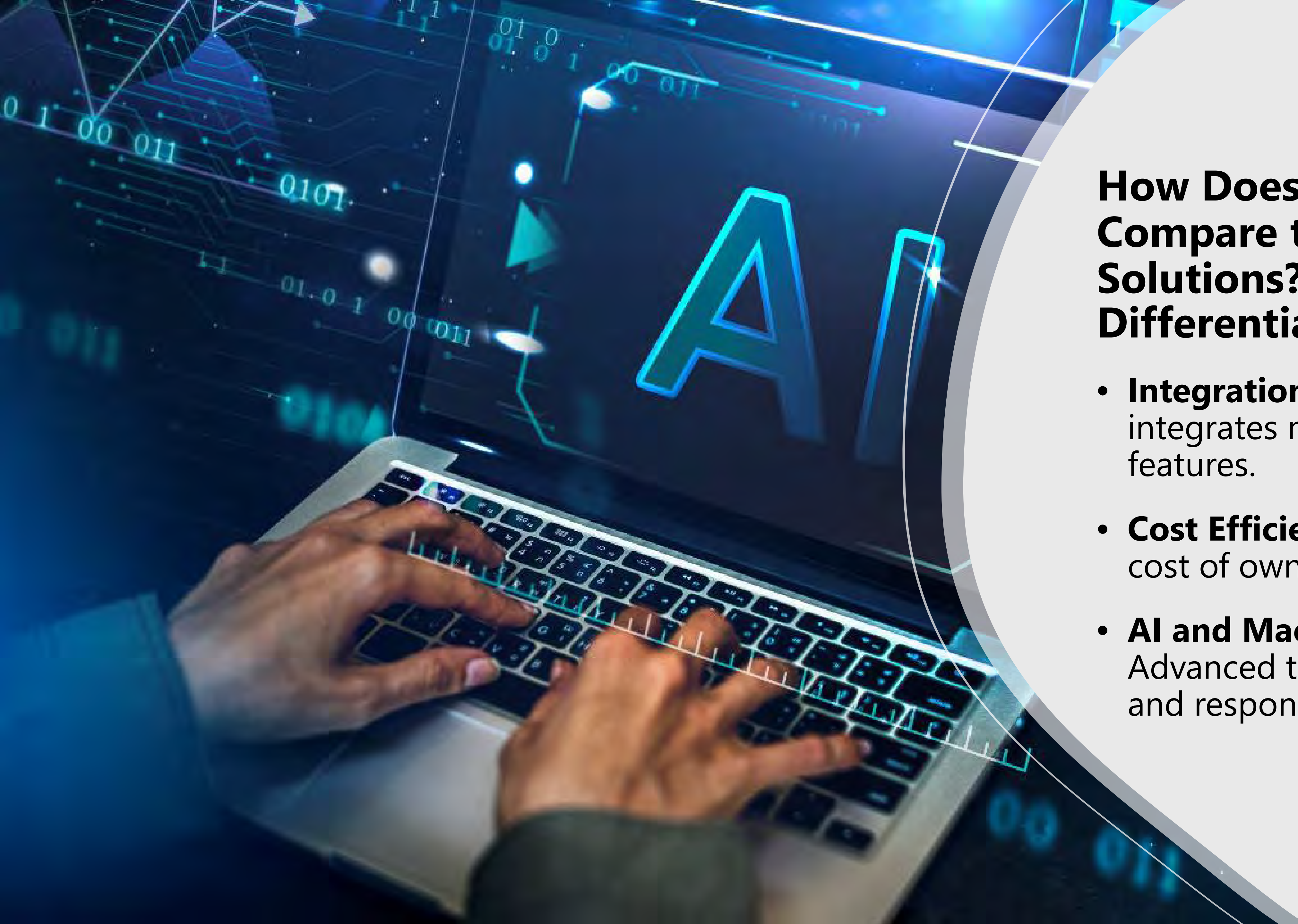
Continuous monitoring and threat detection.

Rapid response to security incidents.

Comprehensive reporting and analysis.

How Does Cy-Napea® Compare to Other Solutions? - Comparison Overview

- **Cy-Napea®**: Comprehensive, integrated cybersecurity solution.
- **Other Solutions**: Often require multiple standalone products.



How Does Cy-Napea Compare to Other Solutions? - Key Differentiators

- **Integration**: Seamlessly integrates multiple security features.
- **Cost Efficiency**: Lower total cost of ownership.
- **AI and Machine Learning**: Advanced threat detection and response.

How Does Cy-Napea Compare to Other Solutions? - Benefits of Cy-Napea®

- Comprehensive protection across endpoints, networks, and cloud environments.
- Proactive threat management and rapid incident response.
- Enhanced visibility and control over security operations.

Cy-Napea®

powered by Aurora Consolidated Ltd.

Website: cy-napea.com
Email: office@cy-napea.com
Phone:
+1 (214) 646-3262 (US)
+359 884 04 88 03 (EU)