AVASOFT
SHAPING NEXT GEN

Microsoft

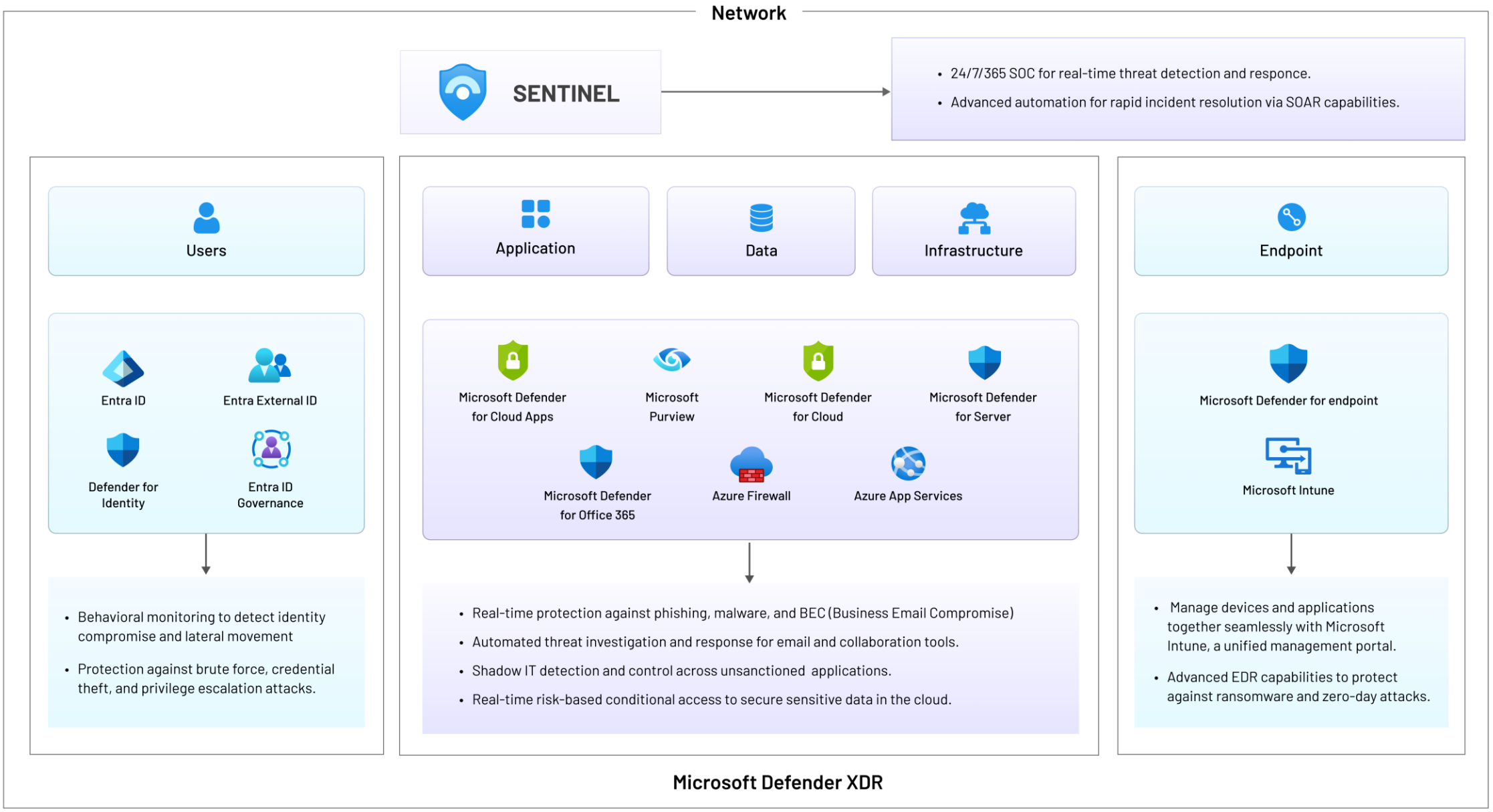
AVASecure 360

Next-Gen MXDR Managed Services

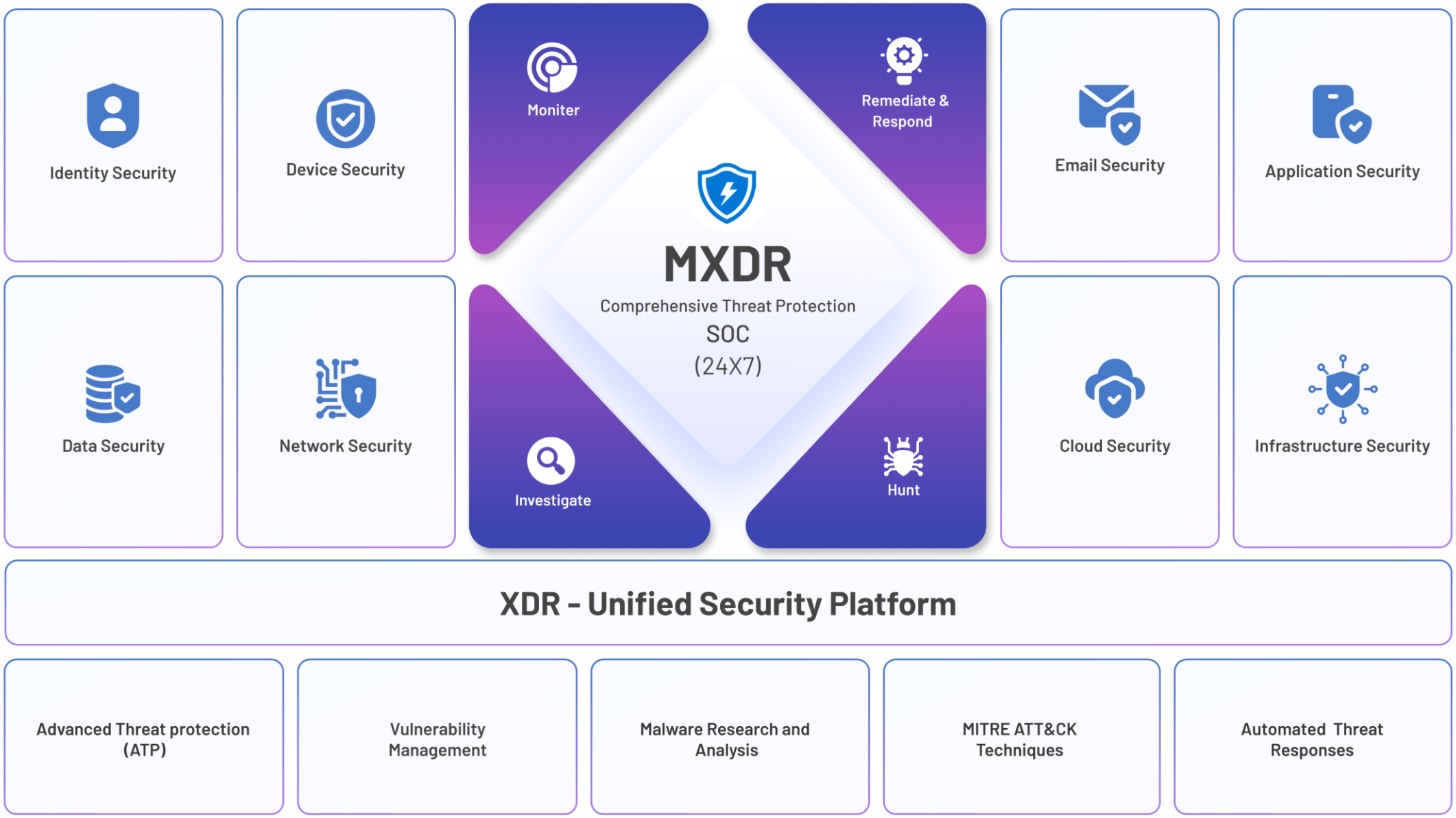
Impacts of No unified management system

- Increased vulnerability to cyber attacks
- Regulatory non-compliance
- Data breach risk
- Loss of customer trust and reputation
- Ineffective incidence response
- Escalating operational cost and penalties
- Delayed detection of threats
- Uncontrolled data exfiltration and limited incident visibility

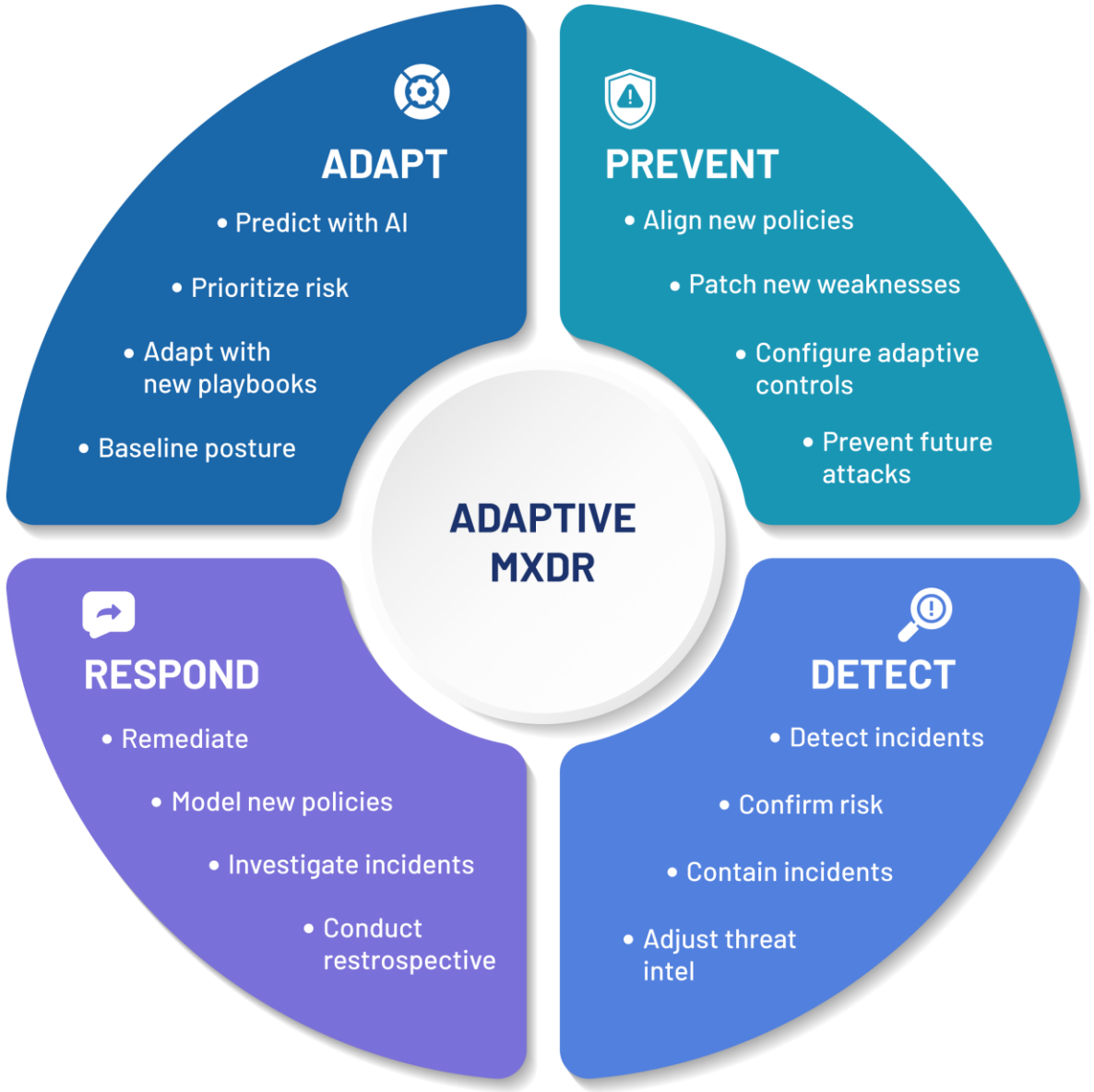
MXDR coverage



Why MXDR?


Identity Security
Device Security
Moniter
Remediate & Respond
Email Security
Application Security
MXDR
Comprehensive Threat Protection
SOC
(24X7)
Data Security
Network Security
Investigate
Hunt
Cloud Security
Infrastructure Security
XDR - Unified Security Platform
Advanced Threat protection (ATP)
Vulnerability Management
Malware Research and Analysis
MITRE ATT&CK Techniques
Automated Threat Responses

What you get with MXDR?



Key Deliverables

Holistic Protection Across All Assets

Unified security for identities, endpoints, applications, data, cloud environments, and email, ensuring seamless coverage without blind spots.

AI-Driven Threat Intelligence

Leveraging Microsoft’s machine learning capabilities for real-time threat detection, reducing false positives, and enabling precise threat hunting.

Adaptive Security Measures

Tailored enforcement of Zero Trust principles with dynamic risk-based access controls, ensuring security policies evolve with your business.

Enhanced Proactive Defense

Integrated Defender solutions for 24/7 threat containment, rapid incident response, and mitigation strategies backed by comprehensive forensic analysis.

Customizable Security Insights

Interactive dashboards and in-depth reporting to monitor and fine-tune your security posture with actionable recommendations for ongoing improvements.

Scalable and Future-Ready

A modular design that adapts to your business growth and seamlessly integrates new Microsoft security advancements and tools.

Regulatory Compliance Alignment

Built-in capabilities to support compliance with industry standards like GDPR, HIPAA, and ISO 27001, reducing audit complexities.

Comprehensive Post-Incident Recovery

Full forensic analysis, root cause identification, and tailored post-incident action plans to prevent recurrence of threats.

Key benefits

Business Benefits

- Enhanced Security Posture: Proactively mitigates threats, reducing the risk of data breaches.
- Regulatory Compliance: Aligns with industry standards like GDPR, HIPAA, and others.
- Cost Efficiency: Consolidates security tools to reduce redundant investments.
- Scalability: Adaptable to evolving business needs and growth.
- Strategic Focus: Enables teams to concentrate on core business functions rather than operational firefighting.

Operational Benefits

- Improved Threat Detection: 24/7 SOC with advanced threat intelligence for quicker identification and resolution.
- Streamlined Processes: Unified dashboards for easier management and reporting.
- Reduced Downtime: Rapid incident response minimizes disruption.
- Automation: Reduces manual effort through AI-driven threat hunting and response.

Thank You