From Panic to Protocol

Building a Resilient Cybersecurity Program to Safeguard Against Emerging Threats

Don Ikhtiari
vCISO, Principal Cybersecurity Architect

Agenda

The Current State of Ransomware

Prevalent Cybersecurity Threats

Building a Resilient Cybersecurity Program

Key Tactical Recommendations / Takeaways

Insight

The Current State of Ransomware

123% increase in reported ransomware attacks over a two-year period

2025 Ransomware Report: How Ransomware Wars Threaten Third-Party Cyber Ecosystems, Black Kite Research & Intelligence Team (BRITE)

64% of organizations impacted by ransomware paid the ransom.

2025 Ransomware Trends and Proactive Strategies, Veeam

$9.48M

average cost of data breach in the US[3].

IBM Cost of a Data Breach 2024

Prevalent Cybersecurity Threats

Ineffective Vulnerability Management Program

Threat-actors often access outdated, vulnerable, systems to enter an organization’s network

Human Error

Threats initiated via social engineering tactics like Phishing, which often target credential harvesting

Third Party Vulnerabilities

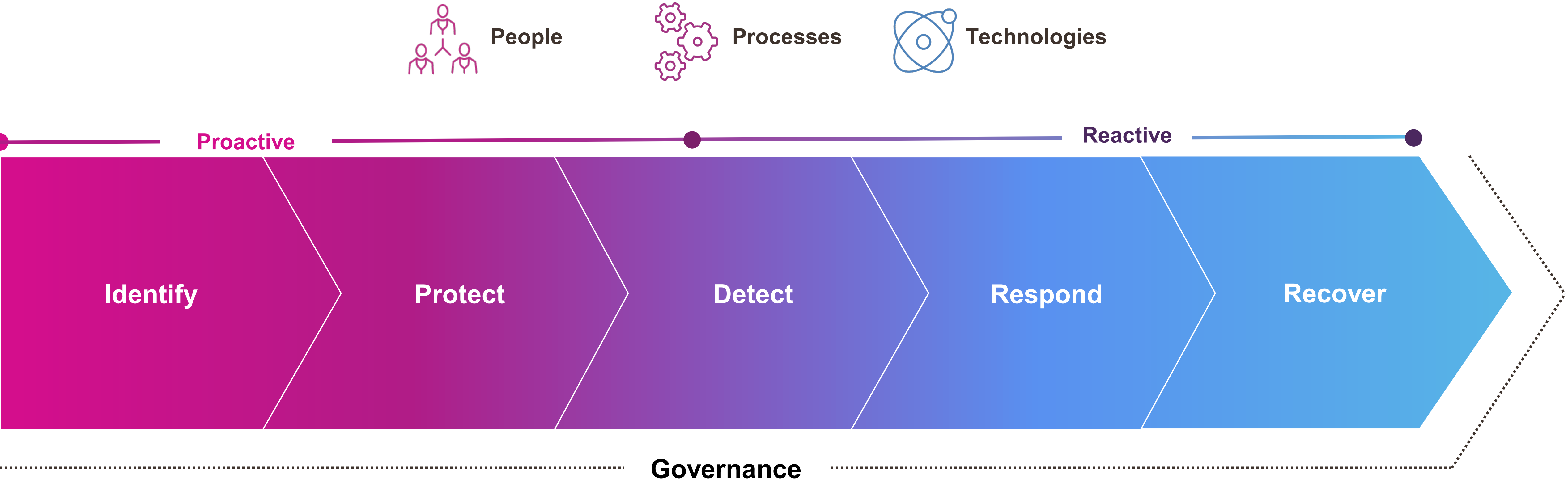
Vulnerabilities can be present in third party applications and supply chains, providing another entry point

Unsecured Web Applications

Insecure public-facing web-applications enable easy access to an organization’s environment.

Align with a Cybersecurity Framework

Industry-accepted cybersecurity frameworks



People

Processes

Technologies

Proactive

Reactive

Identify

Protect

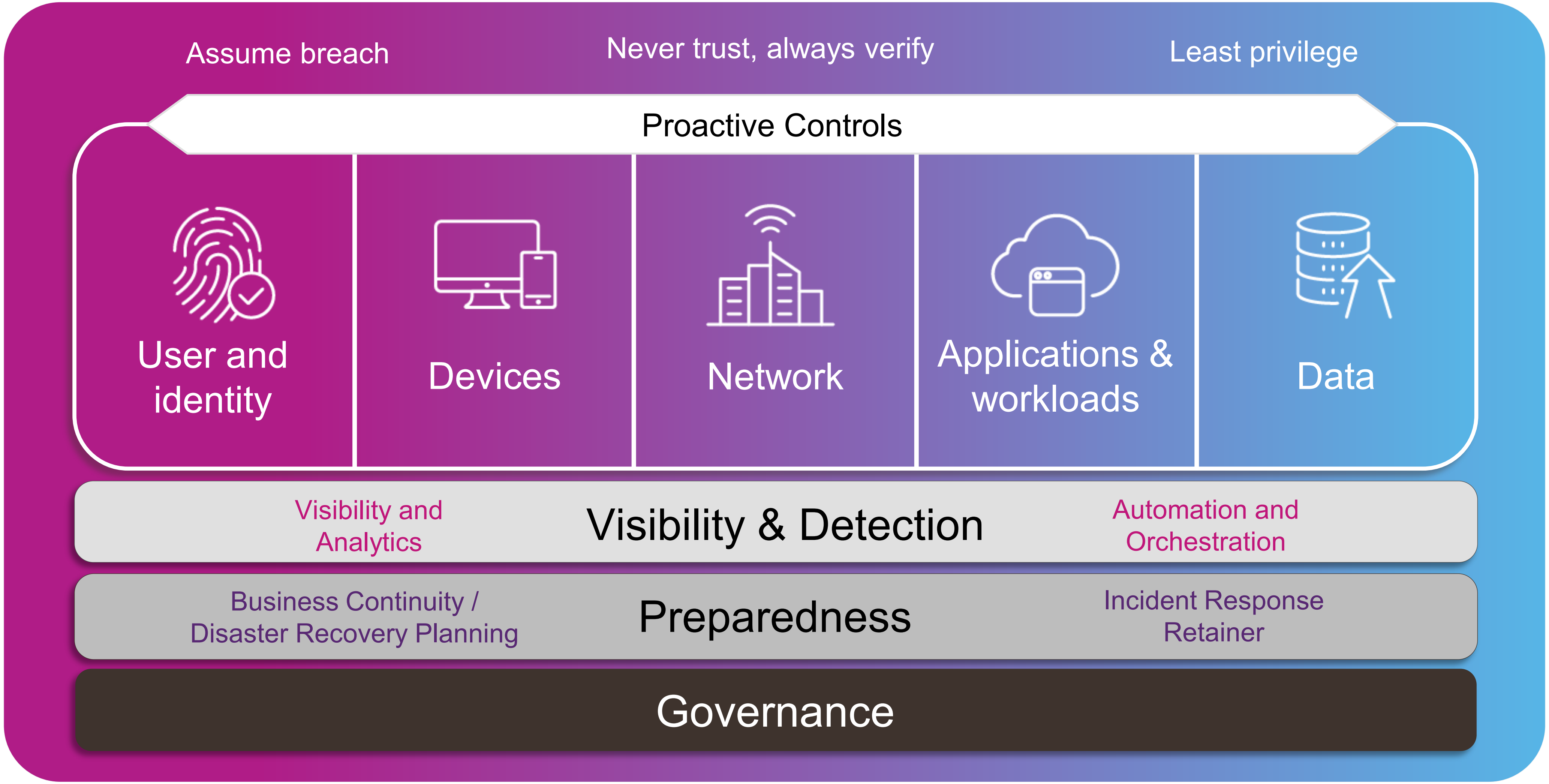
Detect

Respond

Recover

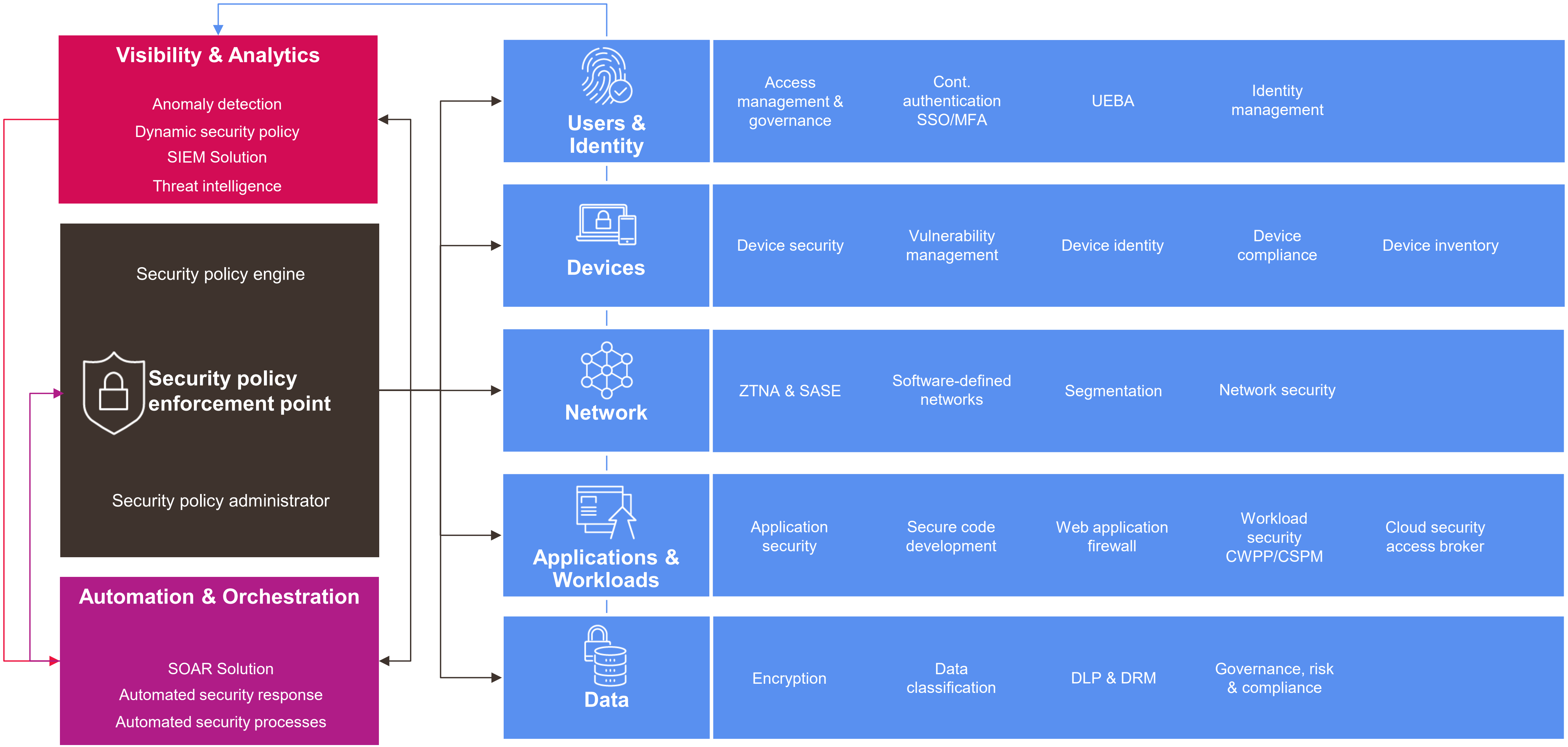
Governance

Building a Resilient Cybersecurity Program



Insight

Zero Trust Architecture



Visibility & Analytics

Anomaly detection

Dynamic security policy

SIEM Solution

Threat intelligence

Security policy engine

Security policy enforcement point

Security policy administrator

Automation & Orchestration

SOAR Solution

Automated security response

Automated security processes

Users & Identity	Access management & governance	Cont. authentication SSO/MFA	UEBA	Identity management	
Devices	Device security	Vulnerability management	Device identity	Device compliance	Device inventory
Network	ZTNA & SASE	Software-defined networks	Segmentation	Network security	
Applications & Workloads	Application security	Secure code development	Web application firewall	Workload security CWPP/CSPM	Cloud security access broker
Data	Encryption	Data classification	DLP & DRM	Governance, risk & compliance	

Insight

Business Continuity / Disaster Recovery Planning

Readiness

Primary vehicle for creating the planning structure for the business continuity effort.

The BIA focus quantifies financial and operational interruptions

Strategy

Tactical and Strategic recommendations to support recovery needs

Response and recovery strategies for plan development

Planning

Plans for Critical Business and IT functions as identified in the BIA

Integration of ERP to all plans

Testing

Testing of plans for Critical Business, IT functions and ERP

Unit and Integration of all plans

Maintenance

Maintenance of plans for Critical Business and IT functions and ERP

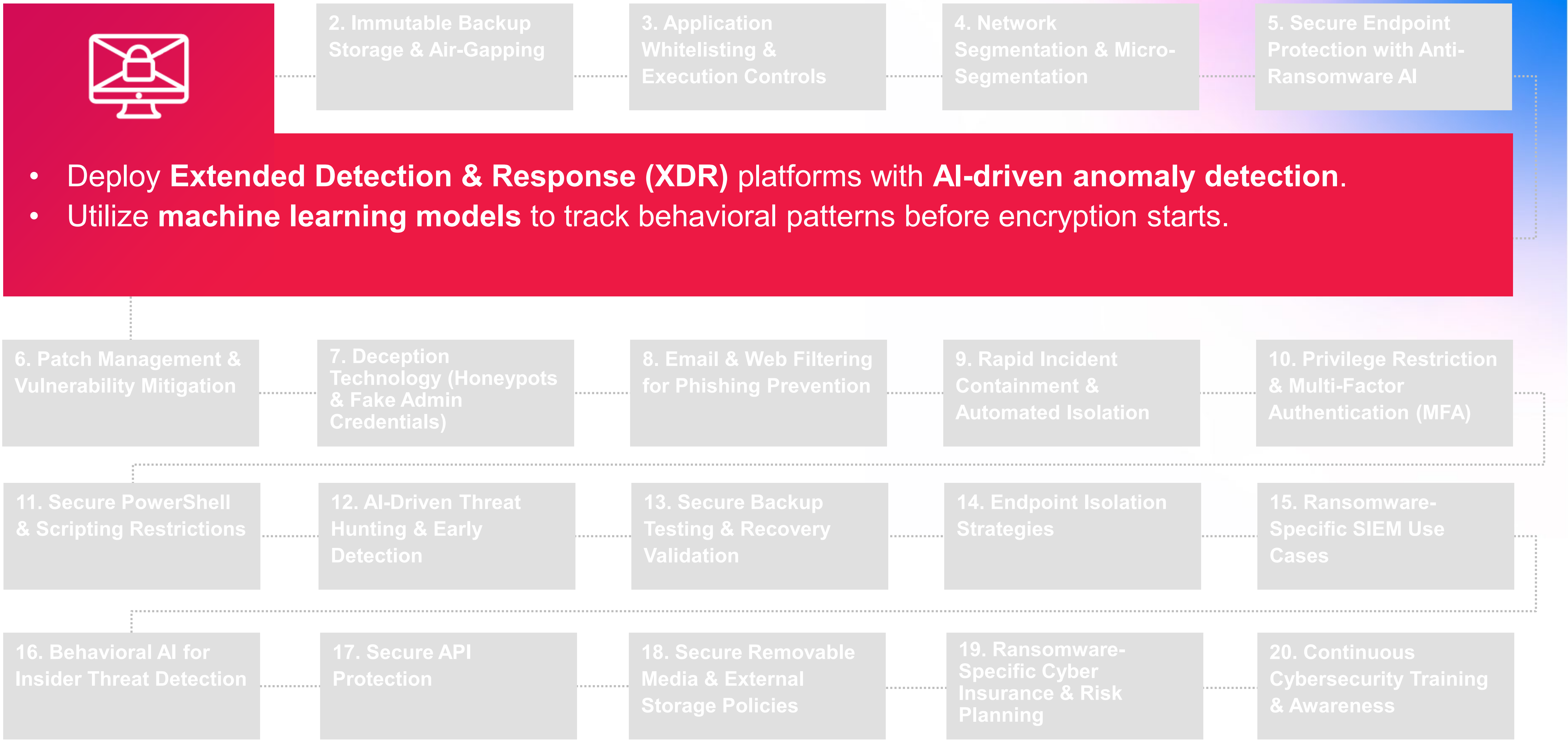
Change control and update management of plans

Tactical Implementations for Ransomware Prevention & Protection

1. AI-Powered Ransomware Behavior Detection
2. Immutable Backup Storage & Air-Gapping
3. Application Whitelisting & Execution Controls
4. Network Segmentation & Micro-Segmentation
5. Secure Endpoint Protection with Anti-Ransomware AI
6. Patch Management & Vulnerability Mitigation
7. Deception Technology (Honeypots & Fake Admin Credentials)
8. Email & Web Filtering for Phishing Prevention
9. Rapid Incident Containment & Automated Isolation
10. Privilege Restriction & Multi-Factor Authentication (MFA)
11. Secure PowerShell & Scripting Restrictions
12. AI-Driven Threat Hunting & Early Detection
13. Secure Backup Testing & Recovery Validation
14. Endpoint Isolation Strategies
15. Ransomware-Specific SIEM Use Cases
16. Behavioral AI for Insider Threat Detection
17. Secure API Protection
18. Secure Removable Media & External Storage Policies
19. Ransomware-Specific Cyber Insurance & Risk Planning
20. Continuous Cybersecurity Training & Awareness

Insight

1. AI-Powered Ransomware Behavior Detection



- Deploy **Extended Detection & Response (XDR)** platforms with **AI-driven anomaly detection**.
- Utilize **machine learning models** to track behavioral patterns before encryption starts.

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

16. Behavioral AI for Insider Threat Detection

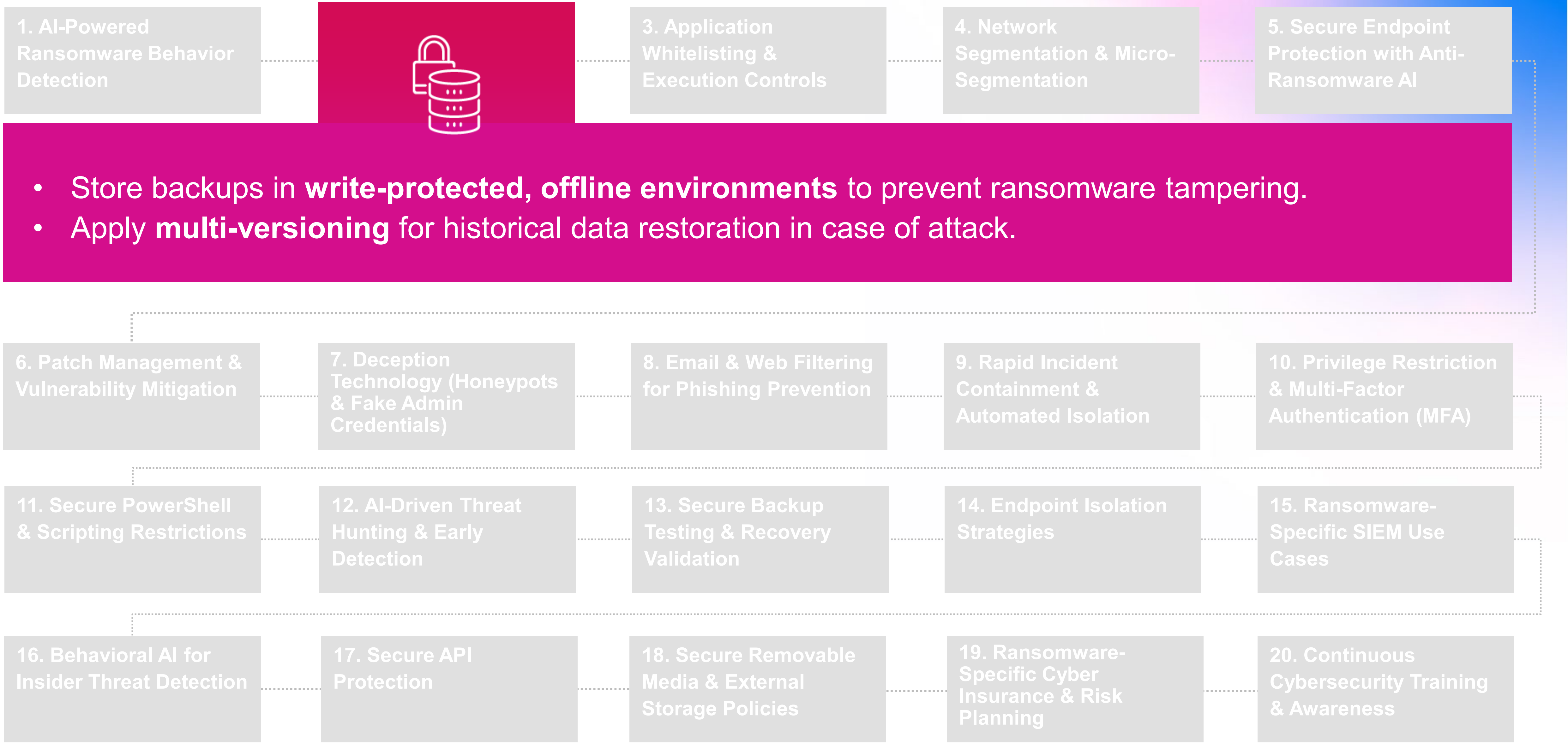
17. Secure API Protection

18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

2. Immutable Backup Storage & Air-Gapping



1. AI-Powered Ransomware Behavior Detection

- Store backups in **write-protected, offline environments** to prevent ransomware tampering.
- Apply **multi-versioning** for historical data restoration in case of attack.

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

16. Behavioral AI for Insider Threat Detection

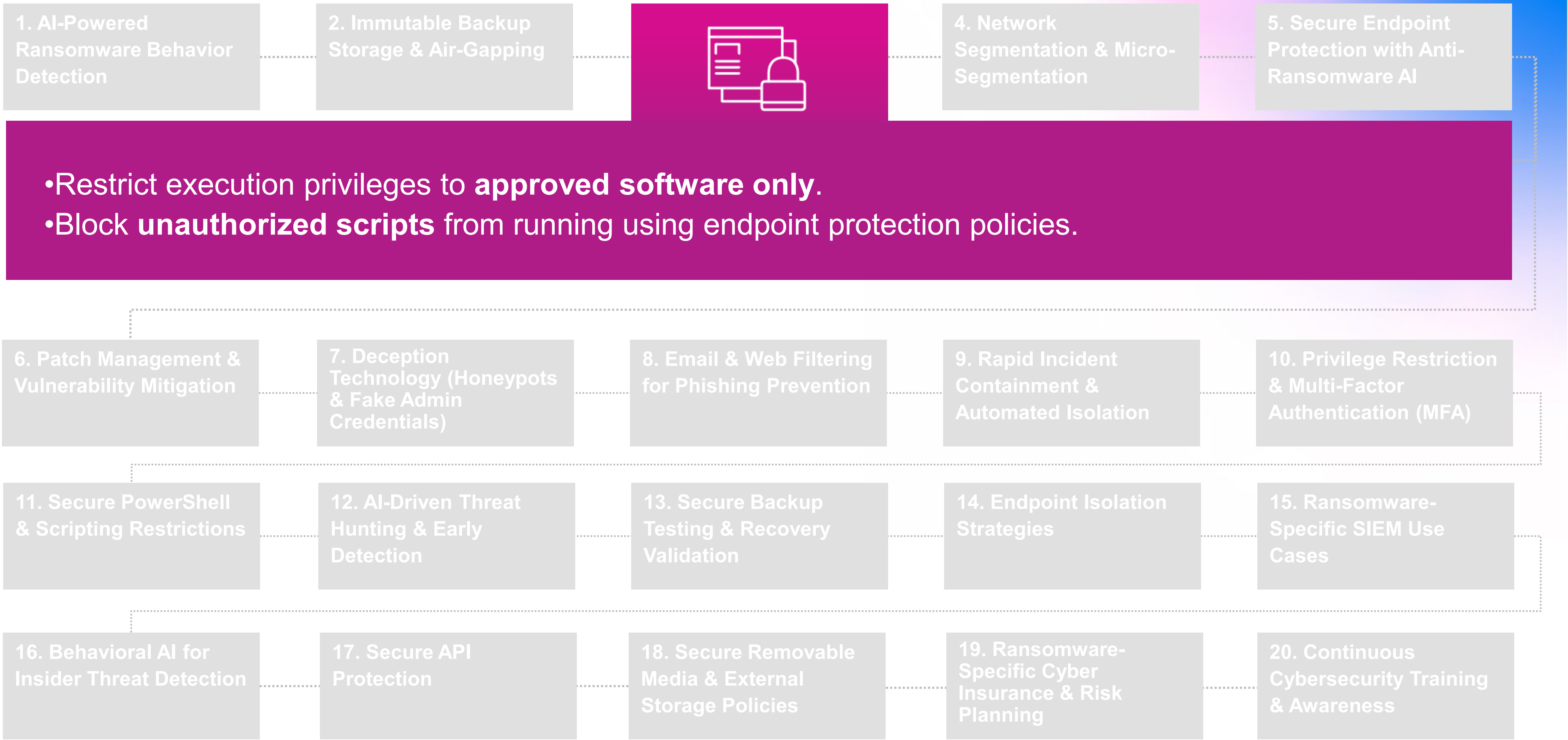
17. Secure API Protection

18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

3. Application Whitelisting & Execution Controls



1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

- Restrict execution privileges to **approved software only**.
- Block **unauthorized scripts** from running using endpoint protection policies.

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

16. Behavioral AI for Insider Threat Detection

17. Secure API Protection

18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

4. Network Segmentation & Micro-Segmentation

1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

5. Secure Endpoint Protection with Anti-Ransomware AI

- Isolate critical assets using **firewalls & VLANs** to prevent ransomware lateral movement.
- Apply **zero-trust architecture** for sensitive systems and data zones.

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

16. Behavioral AI for Insider Threat Detection

17. Secure API Protection

18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

5. Secure Endpoint Protection with Anti-Ransomware AI

1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

- Implement **Next-Gen Antivirus (NGAV) & Endpoint Detection and Response (EDR)** solutions.
- Enable **real-time process monitoring** to block suspicious encryption attempts.

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

16. Behavioral AI for Insider Threat Detection

17. Secure API Protection

18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

6. Patch Management & Vulnerability Mitigation

1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

- Automate updates with centralized patch management systems.
- Apply virtual patching for legacy systems to close known exploit gaps.

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

16. Behavioral AI for Insider Threat Detection

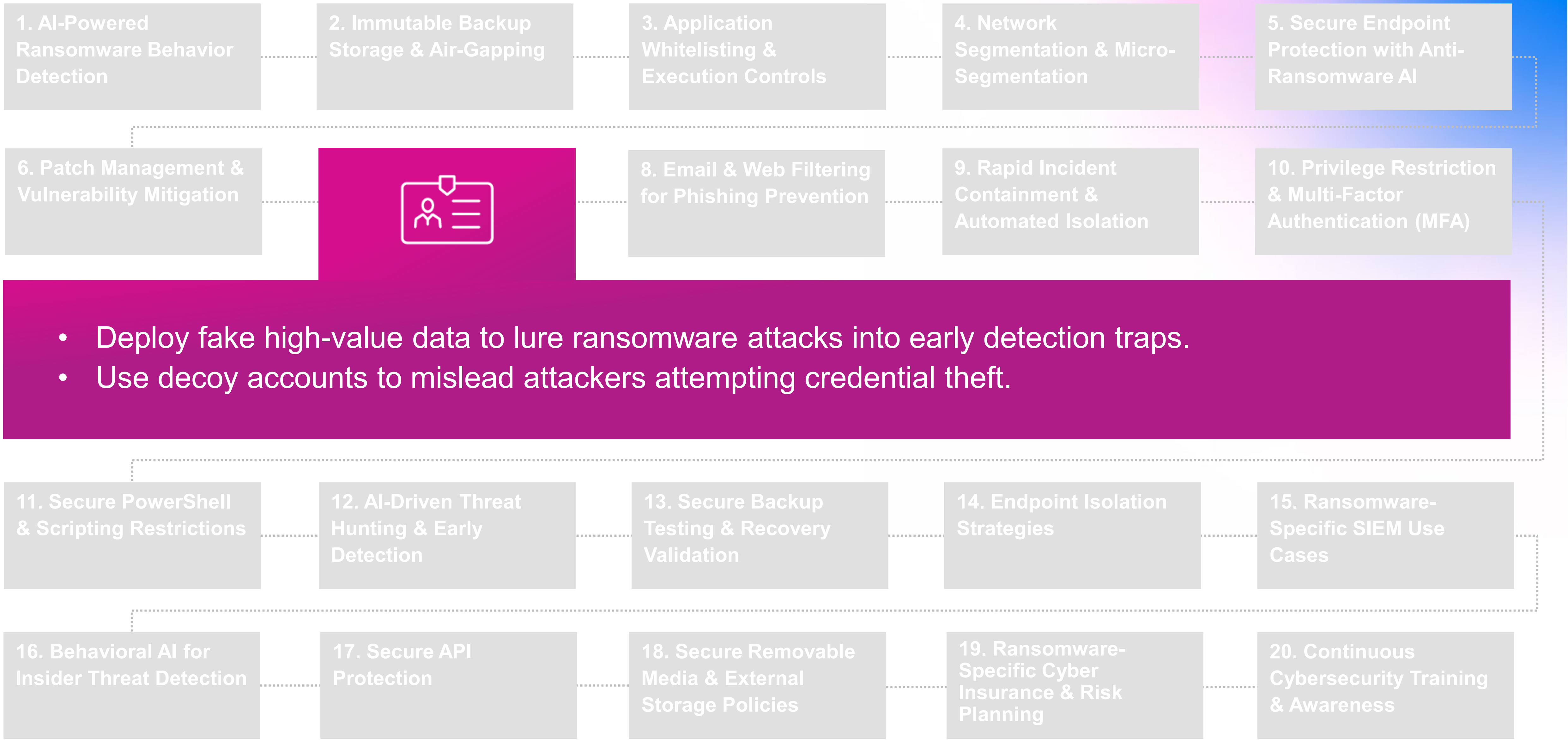
17. Secure API Protection

18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

7. Deception Technology (Honeypots & Fake Admin Credentials)

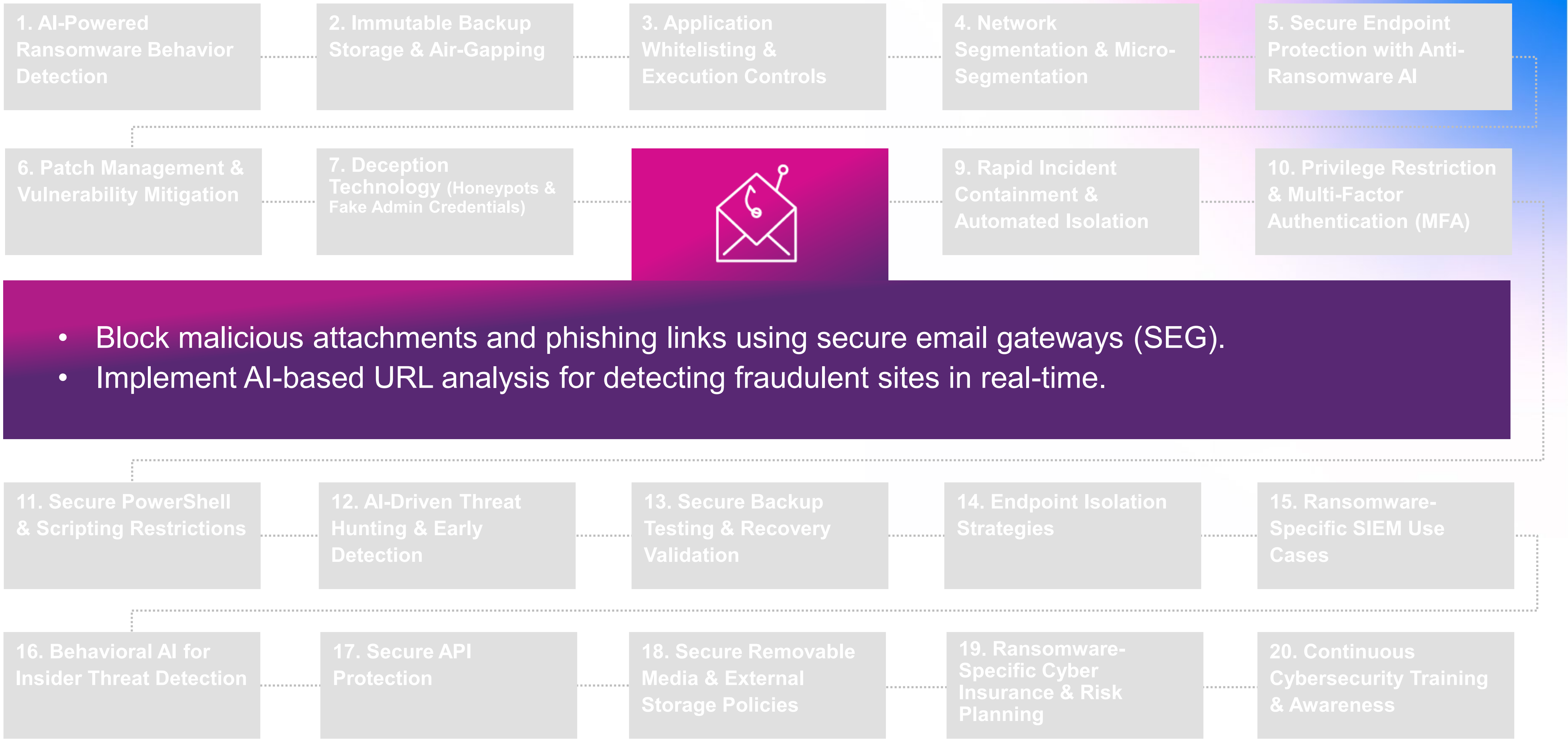


1. AI-Powered Ransomware Behavior Detection
2. Immutable Backup Storage & Air-Gapping
3. Application Whitelisting & Execution Controls
4. Network Segmentation & Micro-Segmentation
5. Secure Endpoint Protection with Anti-Ransomware AI
6. Patch Management & Vulnerability Mitigation
8. Email & Web Filtering for Phishing Prevention
9. Rapid Incident Containment & Automated Isolation
10. Privilege Restriction & Multi-Factor Authentication (MFA)

- Deploy fake high-value data to lure ransomware attacks into early detection traps.
- Use decoy accounts to mislead attackers attempting credential theft.

11. Secure PowerShell & Scripting Restrictions
12. AI-Driven Threat Hunting & Early Detection
13. Secure Backup Testing & Recovery Validation
14. Endpoint Isolation Strategies
15. Ransomware-Specific SIEM Use Cases
16. Behavioral AI for Insider Threat Detection
17. Secure API Protection
18. Secure Removable Media & External Storage Policies
19. Ransomware-Specific Cyber Insurance & Risk Planning
20. Continuous Cybersecurity Training & Awareness

8. Email & Web Filtering for Phishing Prevention



1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

- Block malicious attachments and phishing links using secure email gateways (SEG).
- Implement AI-based URL analysis for detecting fraudulent sites in real-time.

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

16. Behavioral AI for Insider Threat Detection

17. Secure API Protection

18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

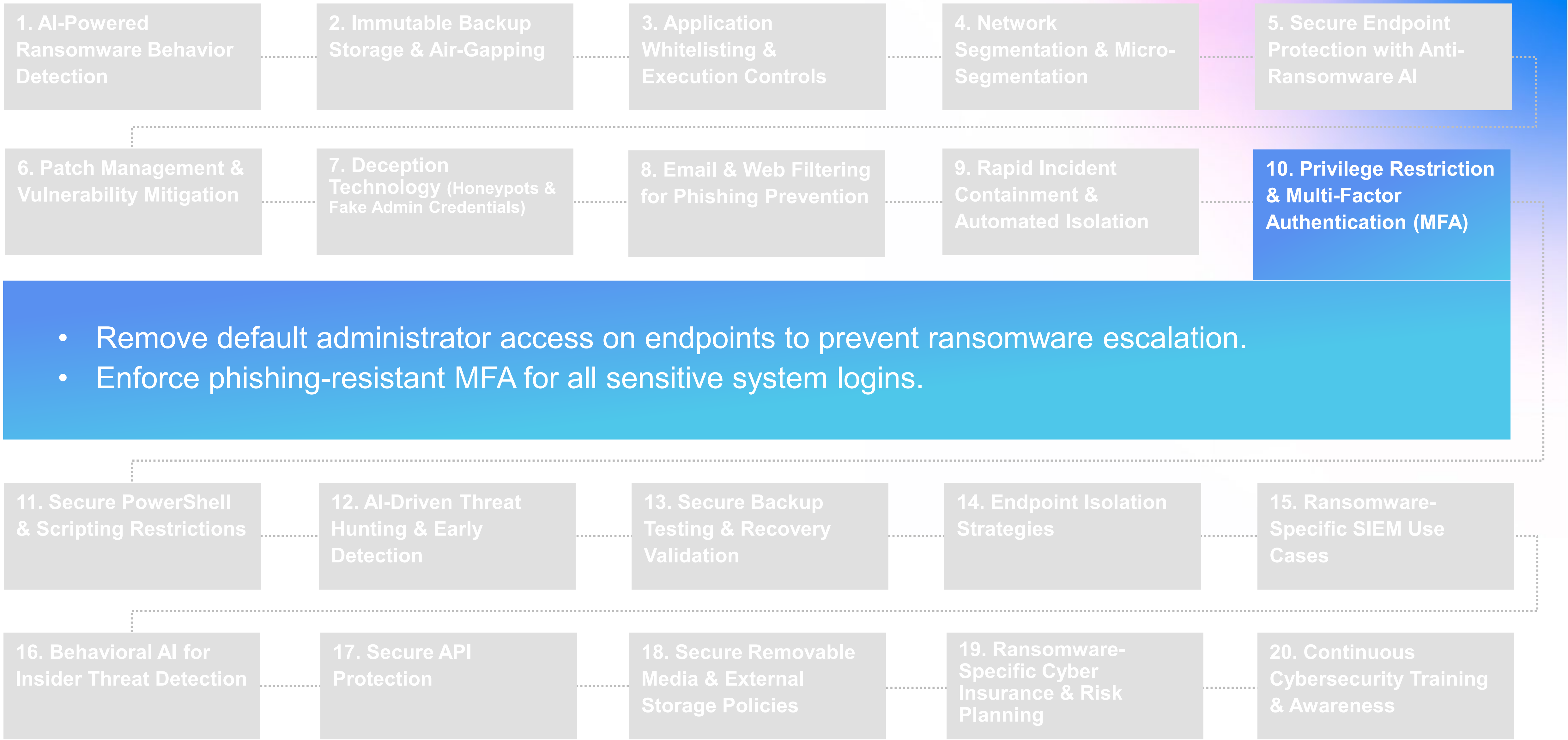
9. Rapid Incident Containment & Automated Isolation

1. AI-Powered Ransomware Behavior Detection
2. Immutable Backup Storage & Air-Gapping
3. Application Whitelisting & Execution Controls
4. Network Segmentation & Micro-Segmentation
5. Secure Endpoint Protection with Anti-Ransomware AI
6. Patch Management & Vulnerability Mitigation
7. Deception Technology (Honeypots & Fake Admin Credentials)
8. Email & Web Filtering for Phishing Prevention

- Use automated isolation playbooks to quarantine infected endpoints before ransomware spreads.
- Apply network-level behavioral analytics to detect ransomware activity instantly.

10. Privilege Restriction & Multi-Factor Authentication (MFA)
11. Secure PowerShell & Scripting Restrictions
12. AI-Driven Threat Hunting & Early Detection
13. Secure Backup Testing & Recovery Validation
14. Endpoint Isolation Strategies
15. Ransomware-Specific SIEM Use Cases
16. Behavioral AI for Insider Threat Detection
17. Secure API Protection
18. Secure Removable Media & External Storage Policies
19. Ransomware-Specific Cyber Insurance & Risk Planning
20. Continuous Cybersecurity Training & Awareness

10. Privilege Restriction & Multi-Factor Authentication (MFA)



1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

- Remove default administrator access on endpoints to prevent ransomware escalation.
- Enforce phishing-resistant MFA for all sensitive system logins.

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

16. Behavioral AI for Insider Threat Detection

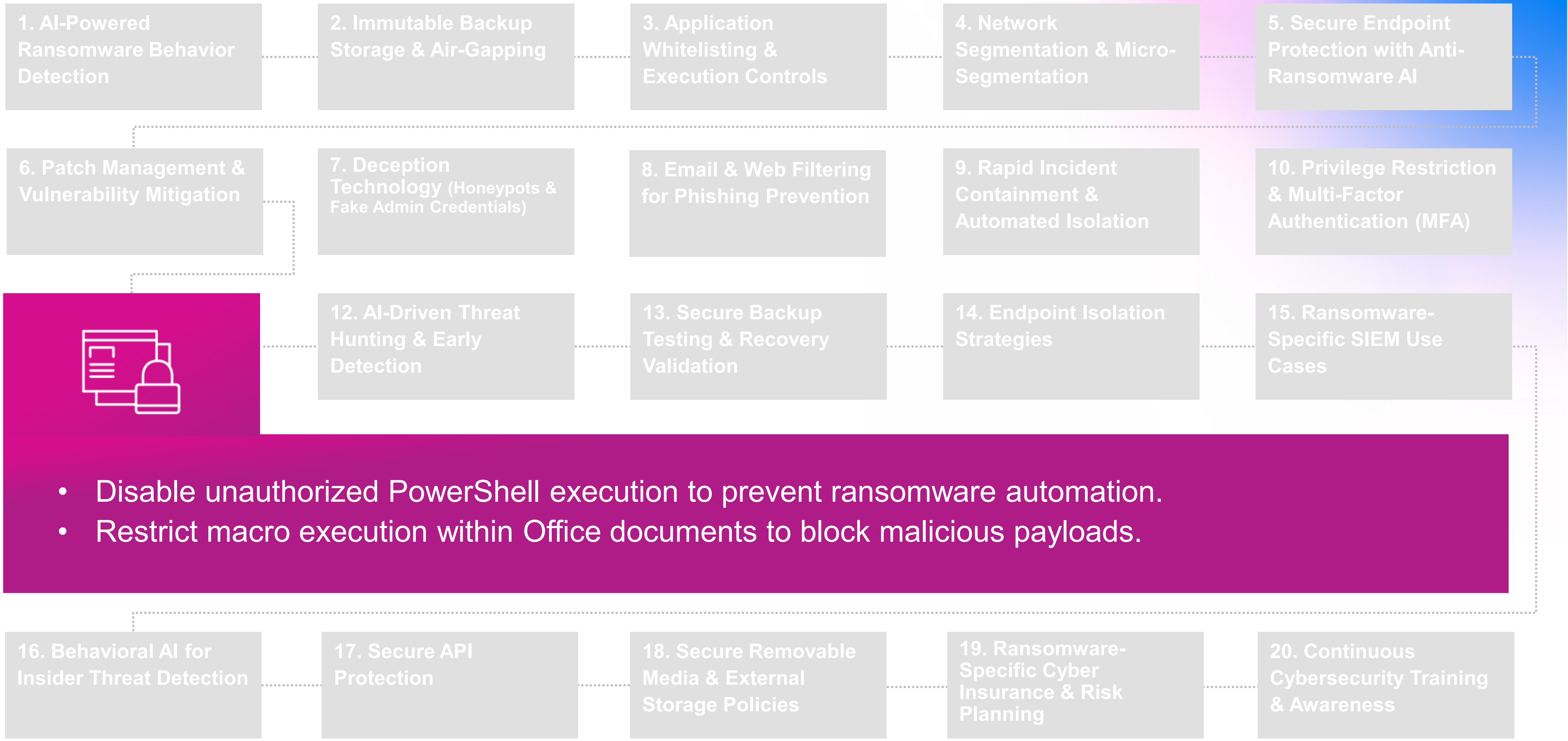
17. Secure API Protection

18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

11. Secure PowerShell & Scripting Restrictions



1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

- Disable unauthorized PowerShell execution to prevent ransomware automation.
- Restrict macro execution within Office documents to block malicious payloads.

16. Behavioral AI for Insider Threat Detection

17. Secure API Protection

18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

12. AI-Driven Threat Hunting & Early Detection

1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

- Use behavioral analytics to detect early-stage ransomware reconnaissance actions.
- Deploy threat intelligence feeds to monitor known ransomware actors.

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

16. Behavioral AI for Insider Threat Detection

17. Secure API Protection

18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

13. Secure Backup Testing & Recovery Validation

1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

- Conduct frequent backup integrity tests to ensure restoration capabilities.
- Implement instant rollback mechanisms for encrypted files.

16. Behavioral AI for Insider Threat Detection

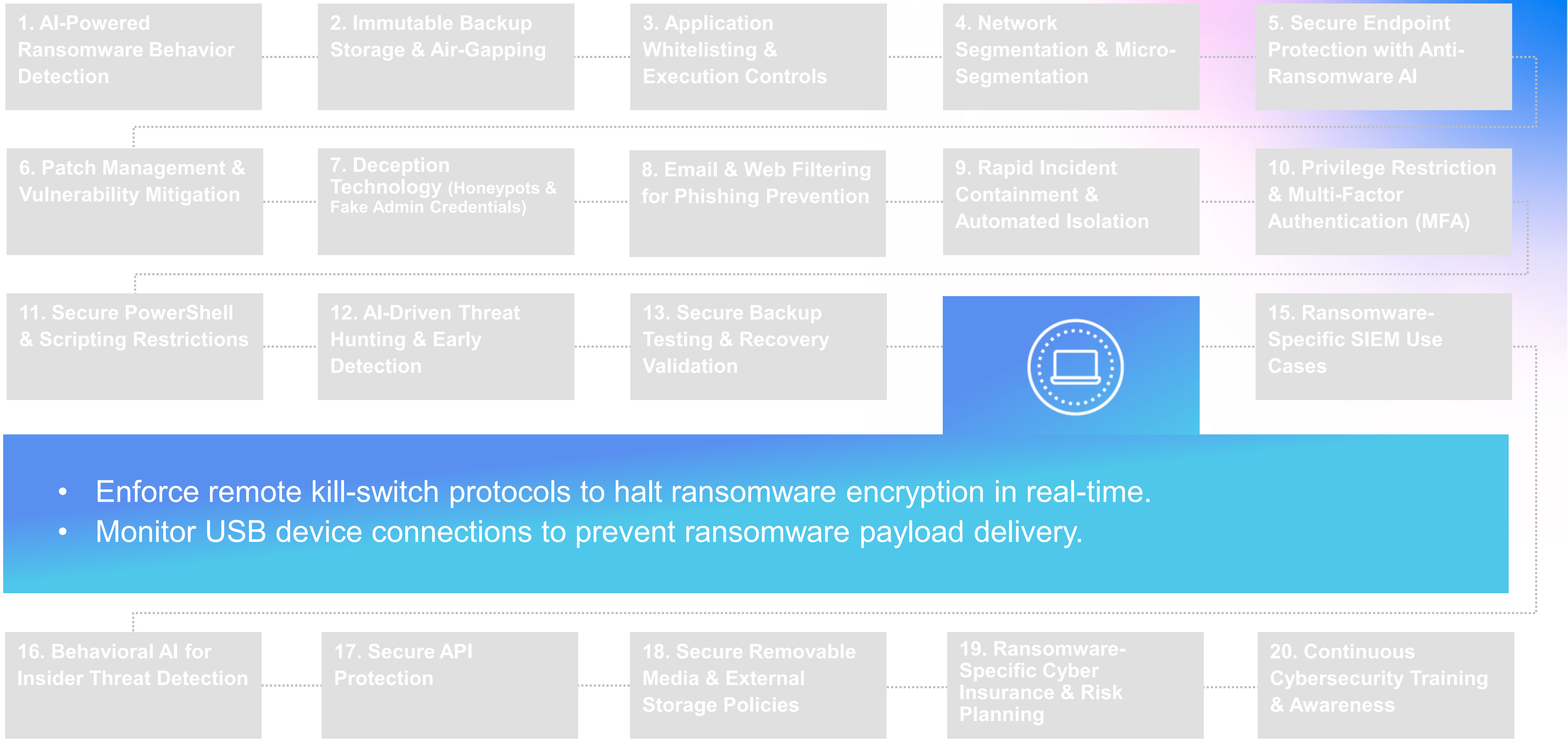
17. Secure API Protection

18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

14. Endpoint Isolation Strategies

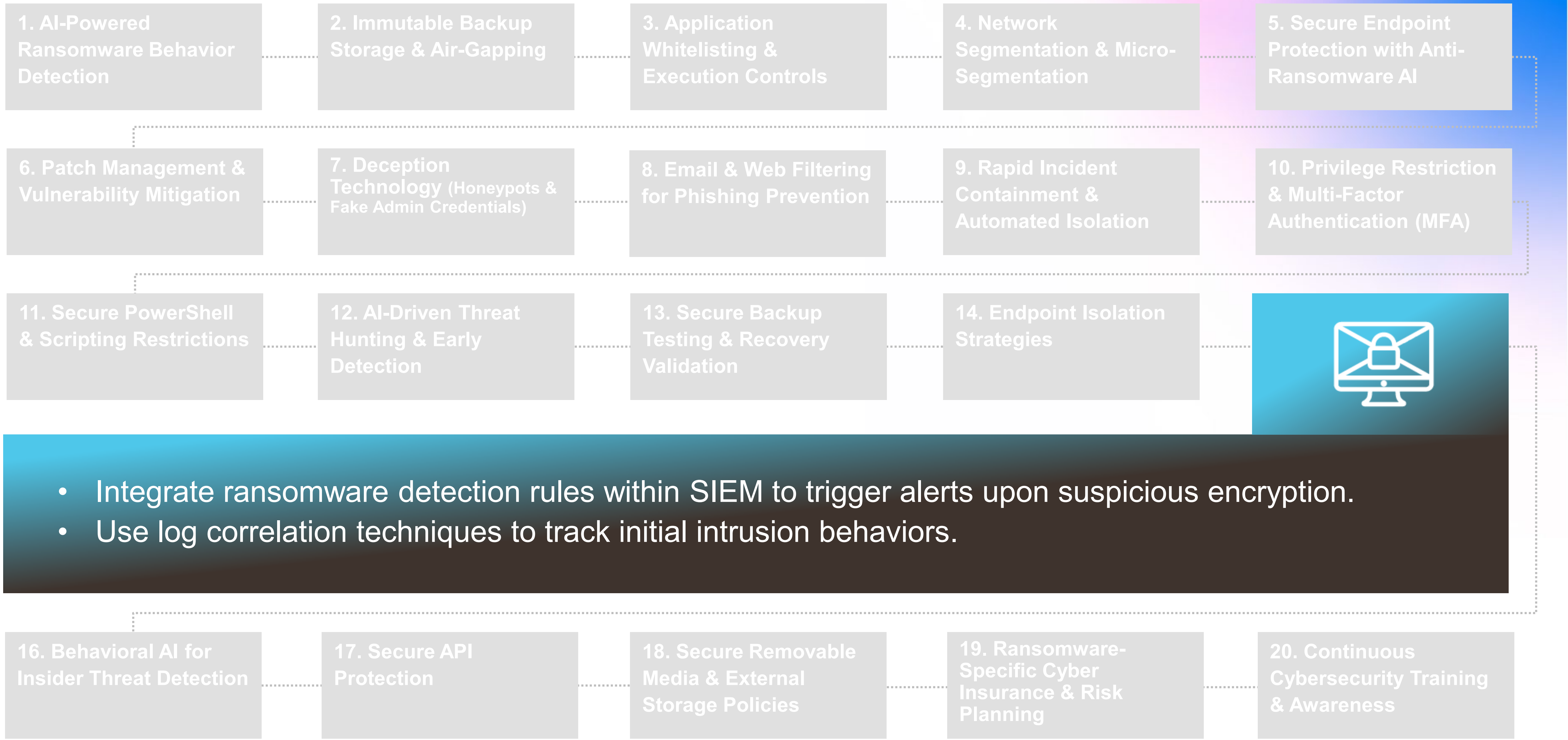


1. AI-Powered Ransomware Behavior Detection
2. Immutable Backup Storage & Air-Gapping
3. Application Whitelisting & Execution Controls
4. Network Segmentation & Micro-Segmentation
5. Secure Endpoint Protection with Anti-Ransomware AI
6. Patch Management & Vulnerability Mitigation
7. Deception Technology (Honeypots & Fake Admin Credentials)
8. Email & Web Filtering for Phishing Prevention
9. Rapid Incident Containment & Automated Isolation
10. Privilege Restriction & Multi-Factor Authentication (MFA)
11. Secure PowerShell & Scripting Restrictions
12. AI-Driven Threat Hunting & Early Detection
13. Secure Backup Testing & Recovery Validation

15. Ransomware-Specific SIEM Use Cases
16. Behavioral AI for Insider Threat Detection
17. Secure API Protection
18. Secure Removable Media & External Storage Policies
19. Ransomware-Specific Cyber Insurance & Risk Planning
20. Continuous Cybersecurity Training & Awareness

- Enforce remote kill-switch protocols to halt ransomware encryption in real-time.
- Monitor USB device connections to prevent ransomware payload delivery.

15. Ransomware-Specific SIEM Use Cases

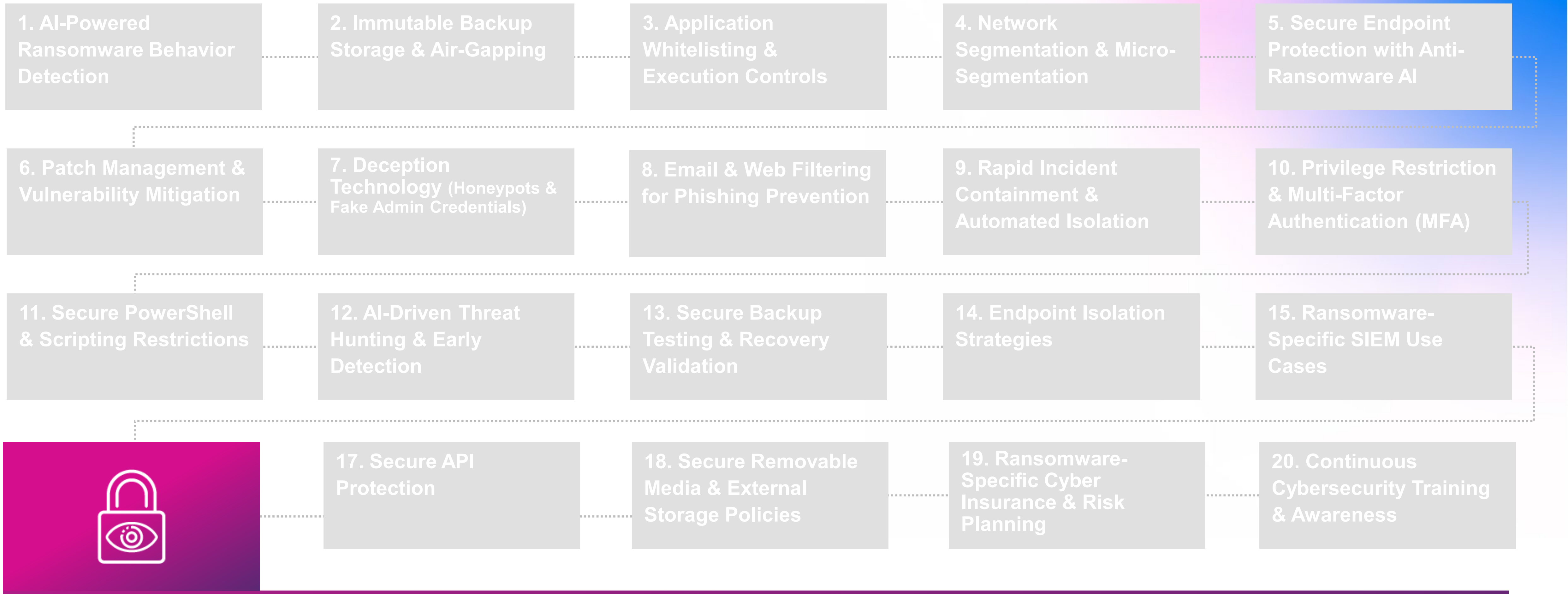


1. AI-Powered Ransomware Behavior Detection
2. Immutable Backup Storage & Air-Gapping
3. Application Whitelisting & Execution Controls
4. Network Segmentation & Micro-Segmentation
5. Secure Endpoint Protection with Anti-Ransomware AI
6. Patch Management & Vulnerability Mitigation
7. Deception Technology (Honeypots & Fake Admin Credentials)
8. Email & Web Filtering for Phishing Prevention
9. Rapid Incident Containment & Automated Isolation
10. Privilege Restriction & Multi-Factor Authentication (MFA)
11. Secure PowerShell & Scripting Restrictions
12. AI-Driven Threat Hunting & Early Detection
13. Secure Backup Testing & Recovery Validation
14. Endpoint Isolation Strategies

- Integrate ransomware detection rules within SIEM to trigger alerts upon suspicious encryption.
- Use log correlation techniques to track initial intrusion behaviors.

16. Behavioral AI for Insider Threat Detection
17. Secure API Protection
18. Secure Removable Media & External Storage Policies
19. Ransomware-Specific Cyber Insurance & Risk Planning
20. Continuous Cybersecurity Training & Awareness

16. Behavioral AI for Insider Threat Detection



1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

17. Secure API Protection

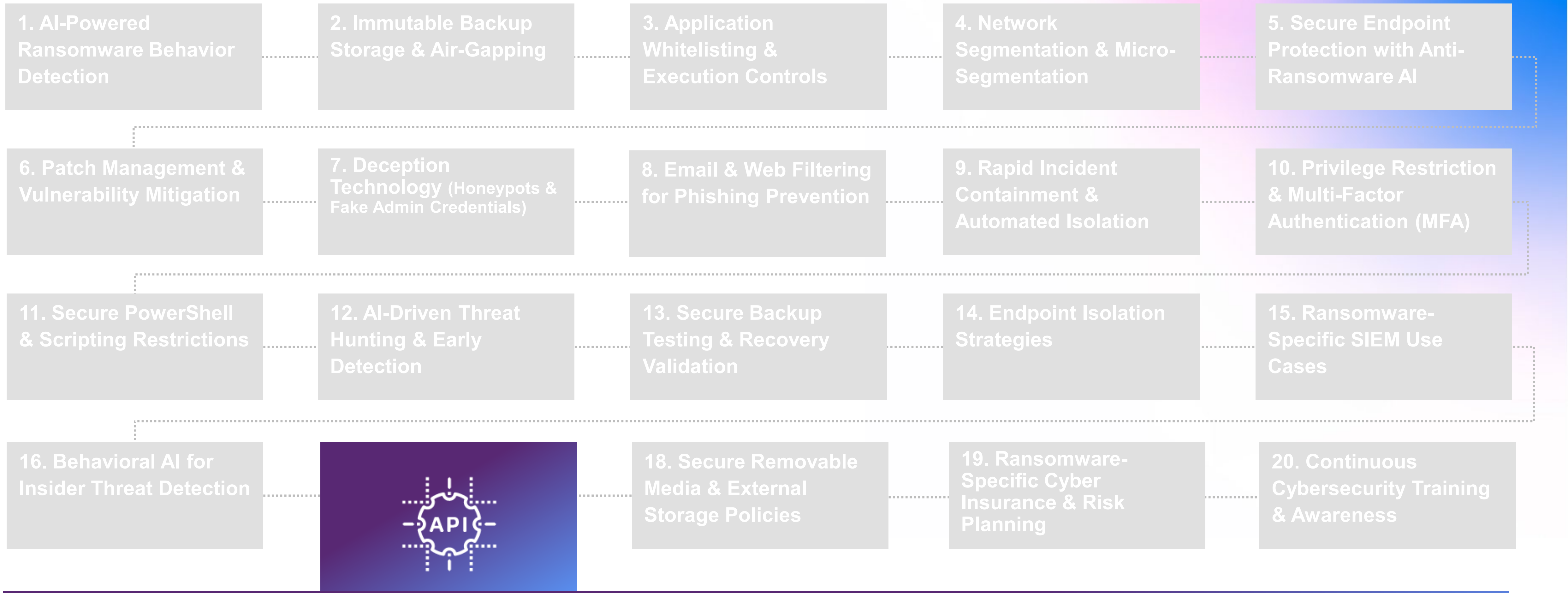
18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

- Monitor employee access patterns for potential internal ransomware execution.
- Implement zero-trust insider controls for privileged users handling sensitive data.

17. Secure API Protection



1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

16. Behavioral AI for Insider Threat Detection

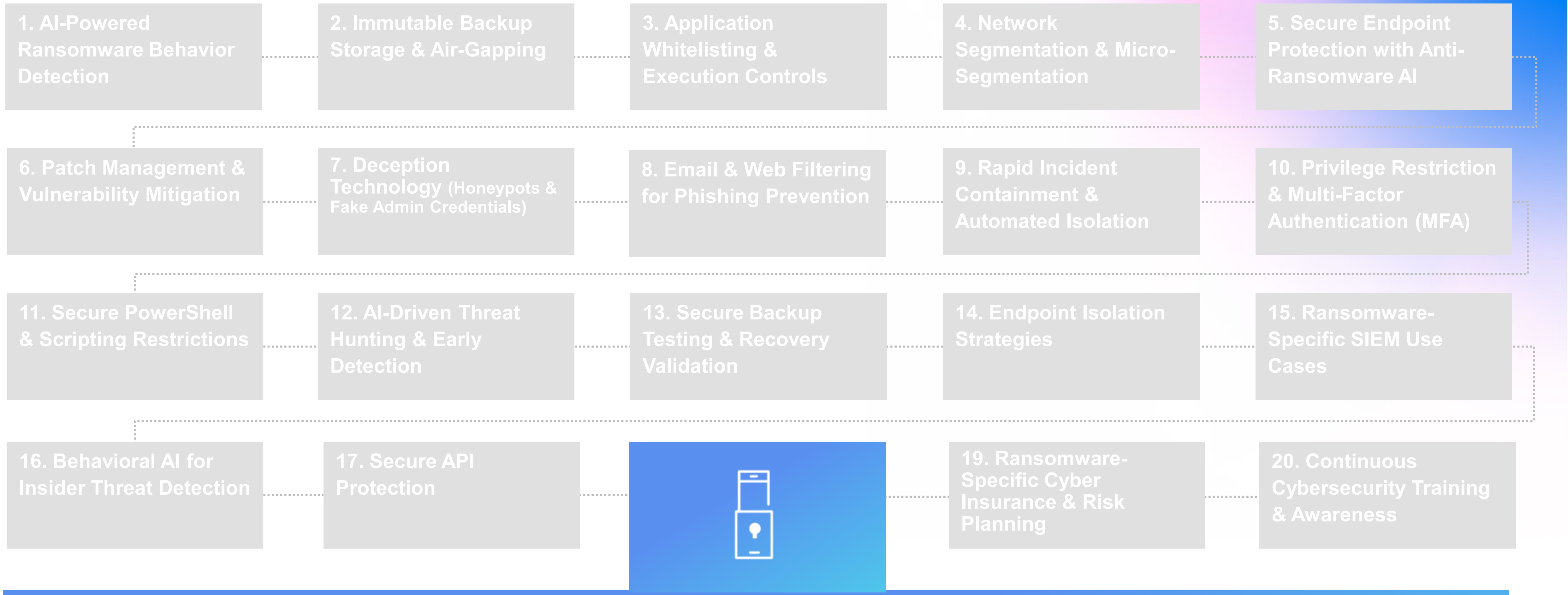
18. Secure Removable Media & External Storage Policies

19. Ransomware-Specific Cyber Insurance & Risk Planning

20. Continuous Cybersecurity Training & Awareness

- Enforce strict API security controls to prevent malware injection into cloud services.
- Utilize OAuth 2.0 & JWT authentication for secure API communications.

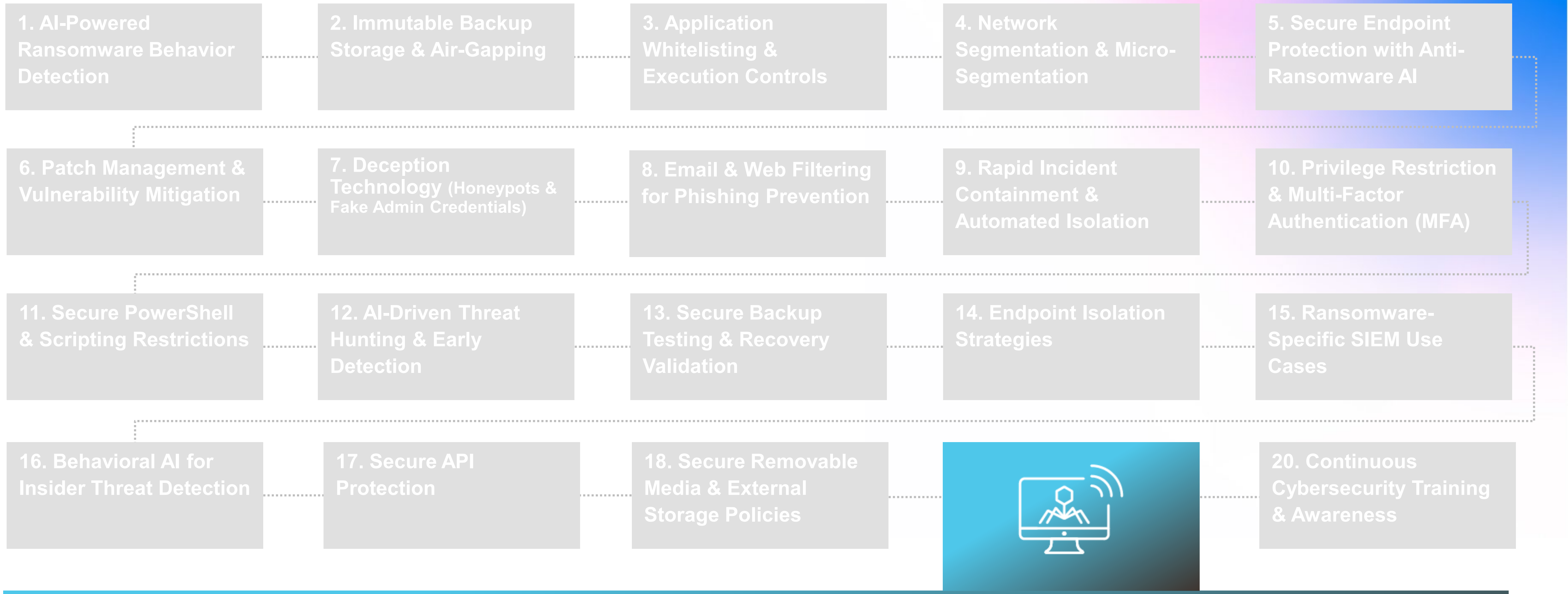
18. Secure Removable Media & External Storage Policies



1. AI-Powered Ransomware Behavior Detection
2. Immutable Backup Storage & Air-Gapping
3. Application Whitelisting & Execution Controls
4. Network Segmentation & Micro-Segmentation
5. Secure Endpoint Protection with Anti-Ransomware AI
6. Patch Management & Vulnerability Mitigation
7. Deception Technology (Honeypots & Fake Admin Credentials)
8. Email & Web Filtering for Phishing Prevention
9. Rapid Incident Containment & Automated Isolation
10. Privilege Restriction & Multi-Factor Authentication (MFA)
11. Secure PowerShell & Scripting Restrictions
12. AI-Driven Threat Hunting & Early Detection
13. Secure Backup Testing & Recovery Validation
14. Endpoint Isolation Strategies
15. Ransomware-Specific SIEM Use Cases
16. Behavioral AI for Insider Threat Detection
17. Secure API Protection
19. Ransomware-Specific Cyber Insurance & Risk Planning
20. Continuous Cybersecurity Training & Awareness

- Disable unauthorized USB devices to prevent ransomware infection vectors.
- Enforce automatic scanning of removable media before access is granted.

19. Ransomware-Specific Cyber Insurance & Risk Planning



1. AI-Powered Ransomware Behavior Detection

2. Immutable Backup Storage & Air-Gapping

3. Application Whitelisting & Execution Controls

4. Network Segmentation & Micro-Segmentation

5. Secure Endpoint Protection with Anti-Ransomware AI

6. Patch Management & Vulnerability Mitigation

7. Deception Technology (Honeypots & Fake Admin Credentials)

8. Email & Web Filtering for Phishing Prevention

9. Rapid Incident Containment & Automated Isolation

10. Privilege Restriction & Multi-Factor Authentication (MFA)

11. Secure PowerShell & Scripting Restrictions

12. AI-Driven Threat Hunting & Early Detection

13. Secure Backup Testing & Recovery Validation

14. Endpoint Isolation Strategies

15. Ransomware-Specific SIEM Use Cases

16. Behavioral AI for Insider Threat Detection

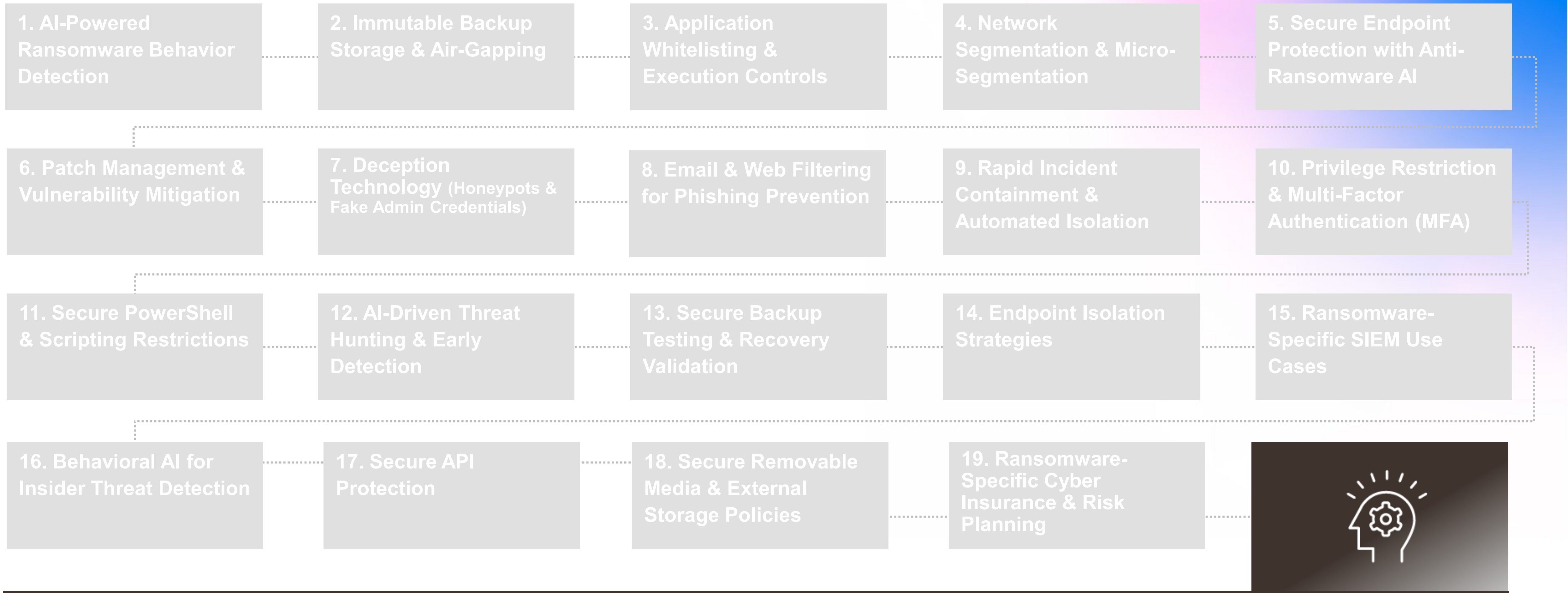
17. Secure API Protection

18. Secure Removable Media & External Storage Policies

20. Continuous Cybersecurity Training & Awareness

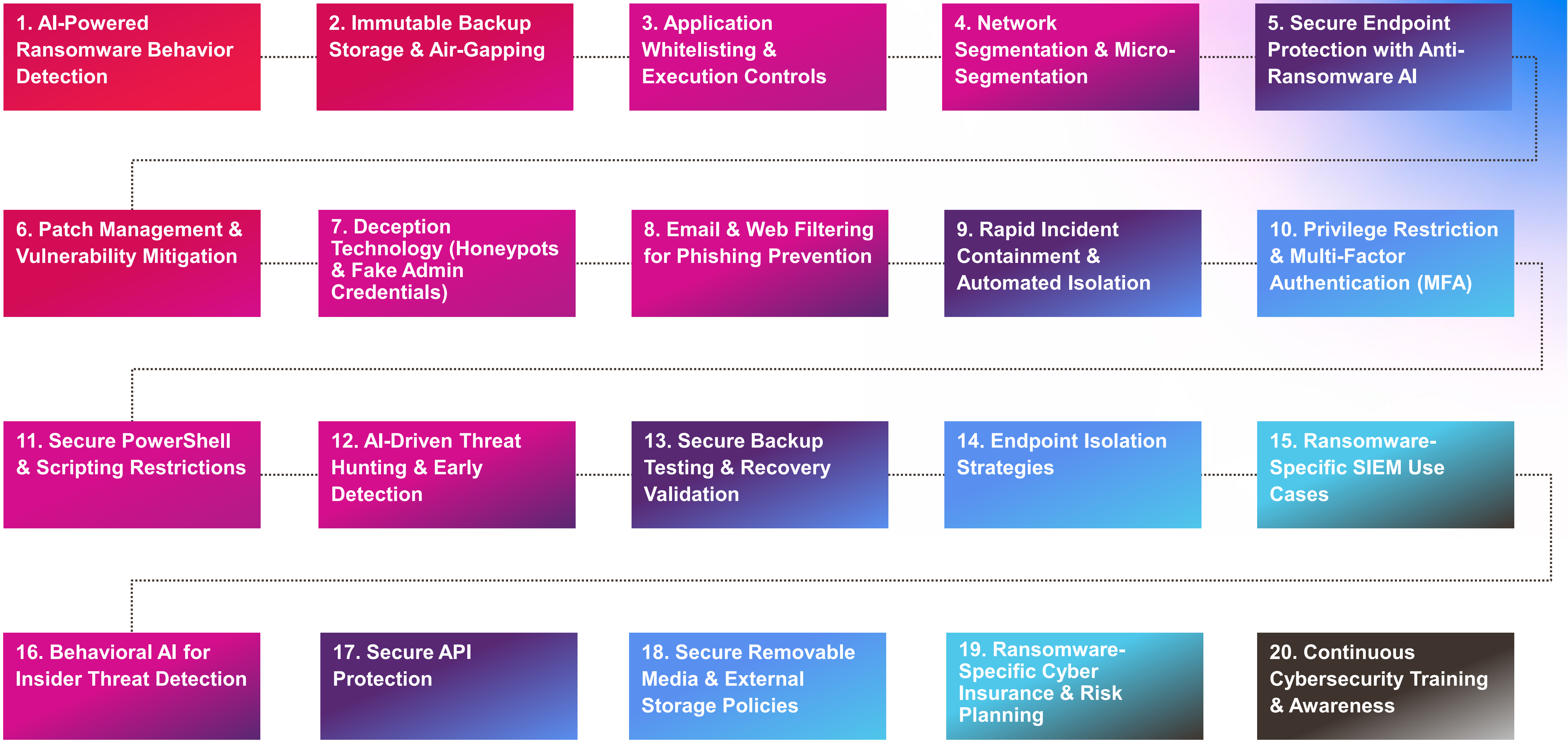
- Establish insurance-backed response plans to mitigate ransomware impact.
- Deploy legal response frameworks for ransomware negotiations (if required).

20. Continuous Cybersecurity Training & Awareness



1. AI-Powered Ransomware Behavior Detection
2. Immutable Backup Storage & Air-Gapping
3. Application Whitelisting & Execution Controls
4. Network Segmentation & Micro-Segmentation
5. Secure Endpoint Protection with Anti-Ransomware AI
6. Patch Management & Vulnerability Mitigation
7. Deception Technology (Honeypots & Fake Admin Credentials)
8. Email & Web Filtering for Phishing Prevention
9. Rapid Incident Containment & Automated Isolation
10. Privilege Restriction & Multi-Factor Authentication (MFA)
11. Secure PowerShell & Scripting Restrictions
12. AI-Driven Threat Hunting & Early Detection
13. Secure Backup Testing & Recovery Validation
14. Endpoint Isolation Strategies
15. Ransomware-Specific SIEM Use Cases
16. Behavioral AI for Insider Threat Detection
17. Secure API Protection
18. Secure Removable Media & External Storage Policies
19. Ransomware-Specific Cyber Insurance & Risk Planning

- Conduct regular ransomware tabletop exercises for IT and executive teams.
- Train employees with AI-driven phishing simulations to recognize malware-laden emails.



1. AI-Powered Ransomware Behavior Detection
2. Immutable Backup Storage & Air-Gapping
3. Application Whitelisting & Execution Controls
4. Network Segmentation & Micro-Segmentation
5. Secure Endpoint Protection with Anti-Ransomware AI
6. Patch Management & Vulnerability Mitigation
7. Deception Technology (Honeypots & Fake Admin Credentials)
8. Email & Web Filtering for Phishing Prevention
9. Rapid Incident Containment & Automated Isolation
10. Privilege Restriction & Multi-Factor Authentication (MFA)
11. Secure PowerShell & Scripting Restrictions
12. AI-Driven Threat Hunting & Early Detection
13. Secure Backup Testing & Recovery Validation
14. Endpoint Isolation Strategies
15. Ransomware-Specific SIEM Use Cases
16. Behavioral AI for Insider Threat Detection
17. Secure API Protection
18. Secure Removable Media & External Storage Policies
19. Ransomware-Specific Cyber Insurance & Risk Planning
20. Continuous Cybersecurity Training & Awareness

Thank you