First Response Secure Endpoint

EXTENDED DETECTION AND RESPONSE

THREAT AND VULNERABILITY MANAGEMENT

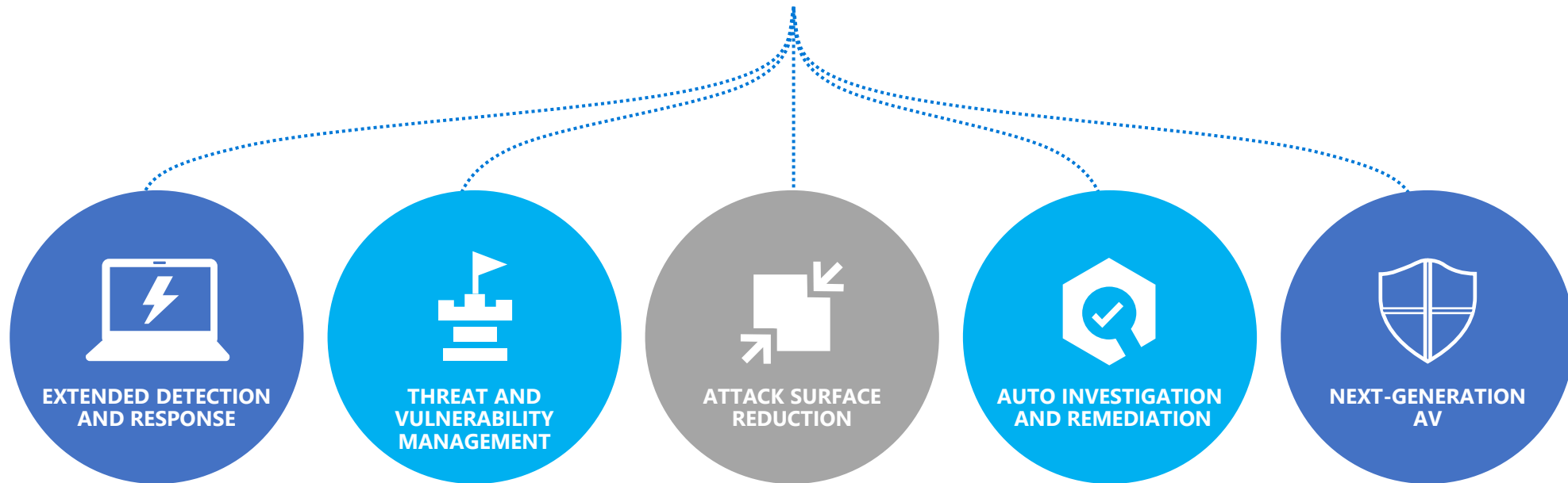**ATTACK SURFACE REDUCTION**

AUTO INVESTIGATION AND REMEDIATION

NEXT-GENERATION AV

24/7 Managed Detection & Response

Alert Monitoring

Pre-authorised Containment & Remediation

Custom Incident Playbooks & Workflows

Pro-active Threat & Vulnerability Hunting

Attack Reports

On-site/Off-site Incident Response Capabilities

UK Based SOC & Support

Full/co-outsource Service

Low Maintenance Deployment

Extended Detection & Response

- **Next-generation AV**

- **Endpoint Detection & Response**

- **User & Entity Behavioural Analysis**

- **Network Traffic Analysis**

- **Automated Investigation & Remediation**

- **Threat & Vulnerability management**

- **Integrated Threat Intelligence**

EXTENDED DETECTION & RESPONSE

first response

MANAGED DETECTION & RESPONSE

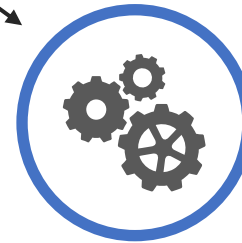ENDPOINT & MOBILE

VIRTUAL PRIVATE CLOUD

1 MONITORING OF SERVICES

2 360 UI
• Detection details
• Root cause & impact analysis

3 CORRELATION ENGINE
• Leverage threat intel feeds
• Advanced machine learning
• Unique algorithm for IOC classification enrichment & scoring

4 SOC TEAM

5 • Breach notification
• Incident response service

• Highly skilled security team
• 24/7 alert monitoring
• Pro-active threat hunting