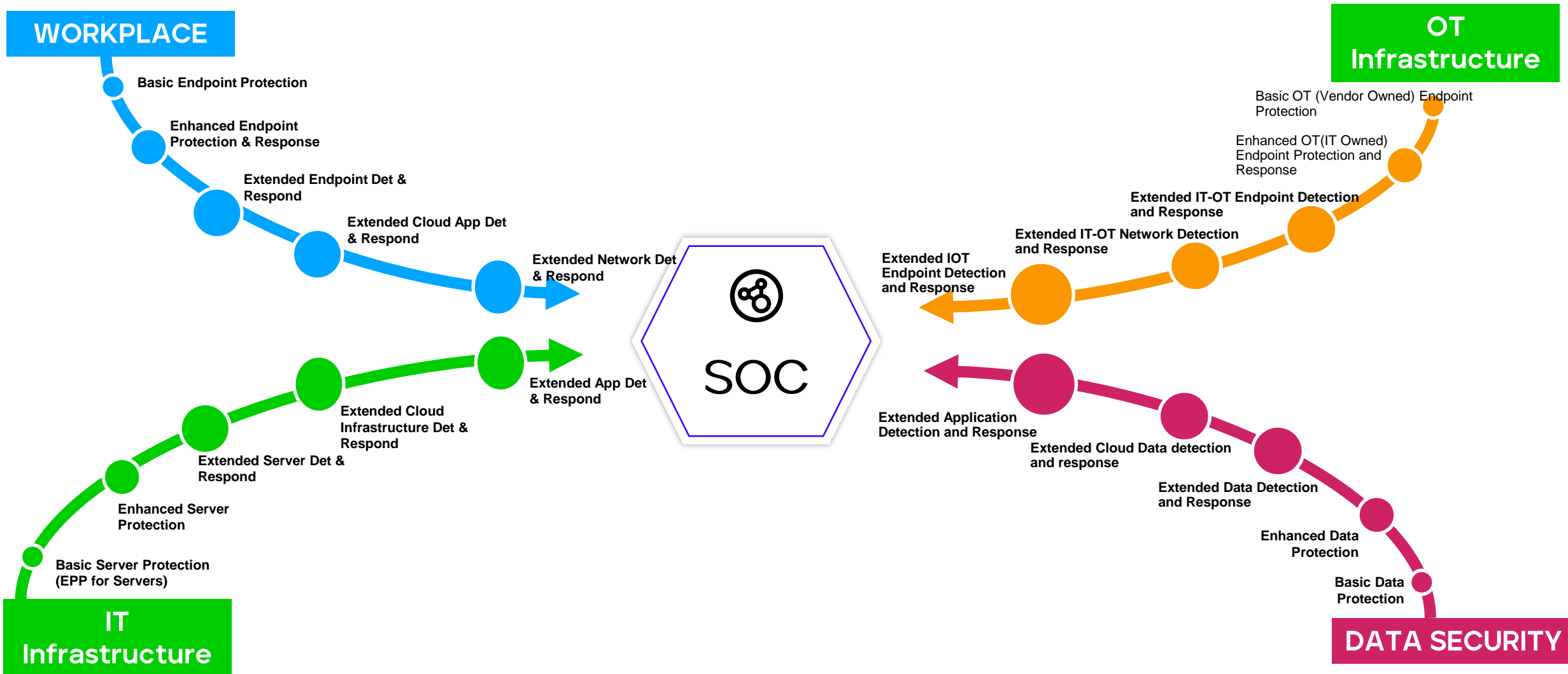
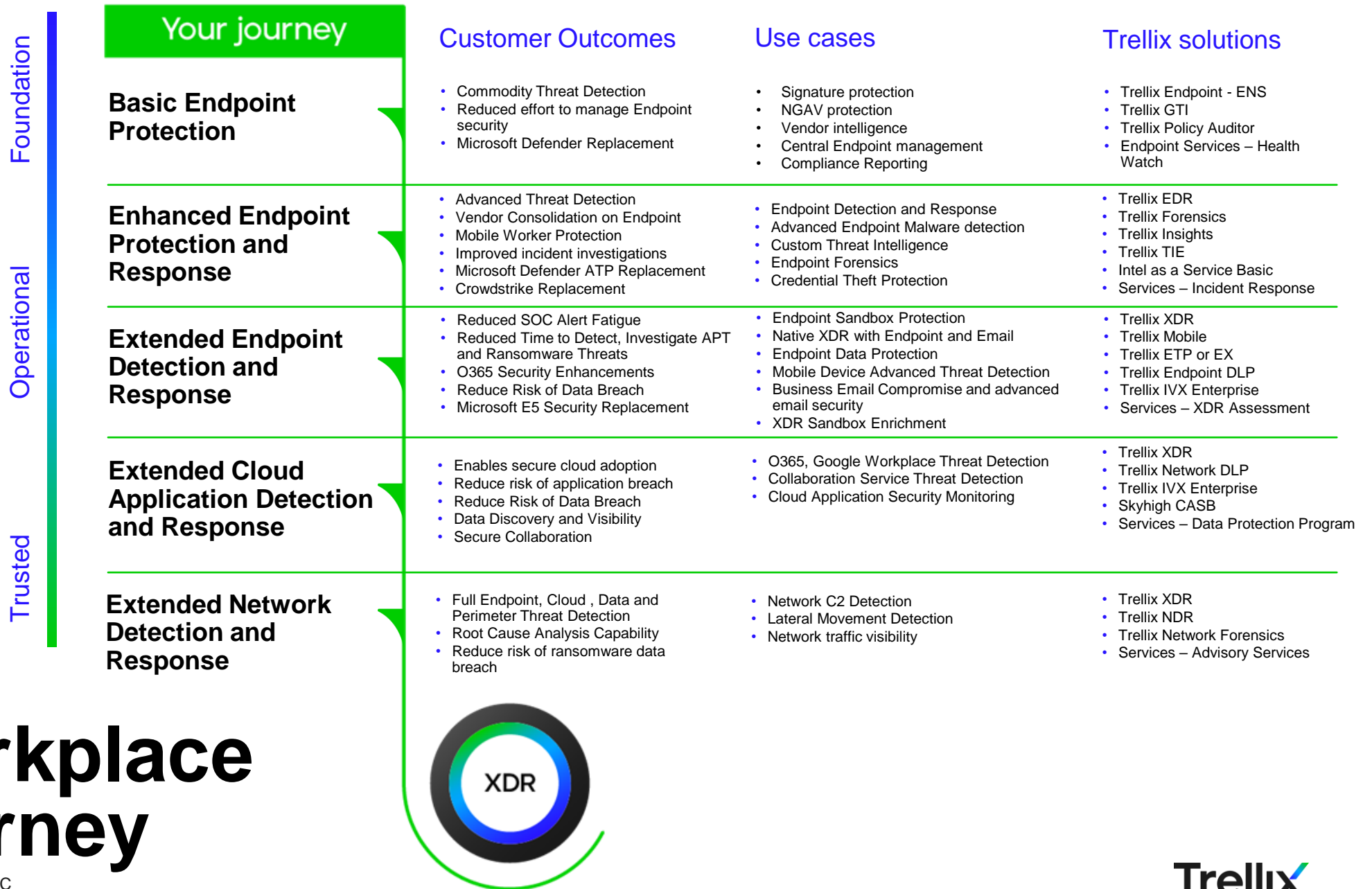


# Sec Ops Solutions Journey Map



# Your Workplace XDR Journey



# Your Infrastructure XDR Journey

	Your journey	Benefits	Use cases	Trellix solutions
Foundation	<b>Basic Server Protection</b>	<ul style="list-style-type: none"> <li>Commodity Threat Detection</li> <li>Reduced effort to manage Endpoint security</li> <li>Microsoft Defender Replacement</li> </ul>	<ul style="list-style-type: none"> <li>Signature protection</li> <li>NGAV protection</li> <li>Vendor intelligence</li> <li>Central Endpoint management</li> <li>Compliance Reporting</li> </ul>	<ul style="list-style-type: none"> <li>Trellix ENS for Servers</li> <li>Trellix GTI</li> <li>Trellix Policy Auditor</li> <li>Endpoint Services – Health Watch</li> </ul>
	<b>Enhanced Server Protection and Response</b>	<ul style="list-style-type: none"> <li>Advanced Threat Detection</li> <li>Vendor Consolidation on Server</li> <li>Improved incident investigations</li> <li>Microsoft Defender ATP Replacement</li> <li>CrowdStrike Replacement</li> <li>Legacy OS Protection</li> </ul>	<ul style="list-style-type: none"> <li>Server whitelisting</li> <li>EDR for servers</li> <li>Change and Integrity Monitoring</li> <li>Attack Surface Assessment</li> <li>Regulatory Compliance</li> </ul>	<ul style="list-style-type: none"> <li>Trellix EDR</li> <li>Trellix Insights</li> <li>Trellix Integrity Control for Servers</li> <li>Trellix Forensics</li> <li>Services – Incident Response</li> </ul>
Operational	<b>Extended Server Detection and Response</b>	<ul style="list-style-type: none"> <li>Reduced SOC Alert Fatigue</li> <li>Reduced Time to Detect, Investigate Server and Application attacks</li> <li>Reduce Risk of Data Breach</li> </ul>	<ul style="list-style-type: none"> <li>Native network and server threat detection in XDR</li> <li>Server Vulnerability Protection</li> <li>Server forensics</li> <li>Custom Threat Intel Reporting</li> <li>Threat Intel-based hunting</li> </ul>	<ul style="list-style-type: none"> <li>Trellix XDR</li> <li>Trellix Network IPS</li> <li>Trellix IVX Enterprise</li> <li>Services - XDR assessments</li> <li>Services - INTaaS</li> </ul>
	<b>Extended Cloud Infrastructure Detection and Response</b>	<ul style="list-style-type: none"> <li>Secure AWS and Azure Platforms</li> <li>Reduce risk of cloud platform breach</li> <li>Optimized Virtual Machine Protection</li> <li>Centralized management of Public, Private and On Prem Servers</li> <li>Protect Network in AWS, Azure</li> </ul>	<ul style="list-style-type: none"> <li>AWS, Azure network visualization</li> <li>Intelligence Enrichment on network logs</li> <li>Automate Workload Security</li> <li>Compliance Reporting</li> <li>Micro segmentation</li> </ul>	<ul style="list-style-type: none"> <li>Trellix XDR</li> <li>Trellix Cloud Workload Security</li> <li>Trellix Policy Auditor</li> <li>Trellix vIPS</li> <li>Trellix IVX Cloud</li> </ul>
Trusted	<b>Extended Application Detection and Response</b>	<ul style="list-style-type: none"> <li>Full endpoint, cloud, application and network visibility</li> <li>Reduced risk of data breach</li> <li>Enhanced protection for business applications</li> </ul>	<ul style="list-style-type: none"> <li>Native cloud, network, application and server threat detection in XDR</li> <li>Threat detection on business applications</li> <li>Threat detection on application databases</li> </ul>	<ul style="list-style-type: none"> <li>Trellix XDR</li> <li>Trellix IVX Enterprise</li> <li>Trellix Database Security</li> <li>Service - Application Security Assessments</li> </ul>



Foundation

Operational

Trusted

## Your journey

### Basic Data Protection

#### Benefits

- Accidental Loss Protection
- Regulatory Compliance

#### Use cases

- Removable Media Control
- Data Encryption
- Endpoint Data Protection
- Program establishment

#### Trellix solutions

- Trellix MNE
- Trellix Drive Encryption
- Trellix Endpoint DLP
- Services: Data Security Program

### Enhanced Data Protection

- Reduced risk of accidental data loss through email
- Decreased risk of accidental data loss through web usage
- Enhanced protection for mobile working

- Data discovery
- On-prem file analysis
- Email Data Protection
- Web Data Protection

- Trellix DLP Prevent
- Trellix DLP Discovery
- Trellix FX/AX
- Services: Data Security Program

### Extended Data Detection and Response

- Reduced DLP alert fatigue
- Decreased time to detect data exfiltration
- Crown jewel protection

- Native data threat detection in XDR
- Identity detection and response
- Data for root cause analysis

- Trellix XDR
- Trellix DLP Monitor
- Trellix Identity Partner integration
- Services: XDR assessments

### Extended Cloud Data detection and response

- Secure cloud adoption
- Reduced risk of cloud data breach
- Enhanced protection for business applications

- SASE data and UBA protection
- Intelligence-enriched Cloud logs
- Protection for cloud storage
- Protection for business applications

- Trellix XDR
- Trellix IVX Enterprise
- Trellix SASE partners integration

### Extended Application Detection and Response

- Full data, application and network visibility
- Reduced risk of data breach
- Enhanced protection for business applications
- Regulatory Compliance

- Native cloud, network, application and server threat detection in XDR
- Threat detection on business applications
- Threat detection on application databases

- Trellix XDR
- Trellix IVX Enterprise
- Trellix Database Security
- Trellix IPS and vIPS
- Service - Application Security Assessments



# Your Data XDR Journey

Foundation

Operational

Trusted

## Your journey

### Basic OT (Vendor Owned) Endpoint Protection

#### Benefits

- Threat Protection
- Central management of IT-OT endpoint security
- Regulatory Compliance

#### Use cases

- Signature protection
- NGAV protection
- Removeable Media protection
- System Lockdown
- Central management

#### Trellix solutions

- Trellix Endpoint
- Trellix Device Control
- Trellix Application Control
- Services: OT Security Assessment

### Enhanced OT(IT Owned) Endpoint Protection and Response

- Advanced Threat Detection
- OnPrem Endpoint Management
- Improved OT incident investigations
- Microsoft Defender ATP Replacement
- Crowdstrike Replacement

- Endpoint Detection and Response
- Advanced Endpoint Malware detection
- OT Threat Intelligence
- Endpoint Forensics
- Credential Theft Protection

- Trellix Forensics
- Trellix Insights
- Trellix TIE
- Intel as a Service Basic
- Services – Incident Response

### Extended IT-OT Endpoint Detection and Response

- Reduced endpoint alert fatigue
- Reduced time to detect OT threats
- OT visibility

- Threat Detection across IT-OT
- OT network threat detection
- OT Asset Discovery
- IT-OT Lateral Movement
- Credential Theft Detection

- Trellix XDR
- Trellix NX
- Deception Tool Partners
- Trellix Comm Broker
- Services:

### Extended IT-OT Network Detection and Response

- Reduce network alert fatigue
- OT Asset Risk Intelligence
- Root Cause Analysis

- Native network, endpoint and OT system detection in XDR
- Anomaly detections
- Network Forensics
- IT-OT DLP

- Trellix XDR
- Trellix SCADA Security Partners
- Trellix PX
- Trellix Network DLP Monitor

### Extended IOT Endpoint Detection and Response

- Secure AWS and Azure Platforms
- Reduce risk of cloud platform breach
- Optimized Virtual Machine Protection
- Centralized management of Public, Private and On Prem Servers
- Protect Network in AWS, Azure

- AWS, Azure network visualization
- Intelligence Enrichment on network logs
- Automate Workload Security
- Compliance Reporting
- Micro segmentation

- Trellix XDR
- Trellix Cloud Workload Security
- Trellix Policy Auditor
- Trellix vIPS
- Trellix IVX Cloud



# Your IT-OT XDR Journey