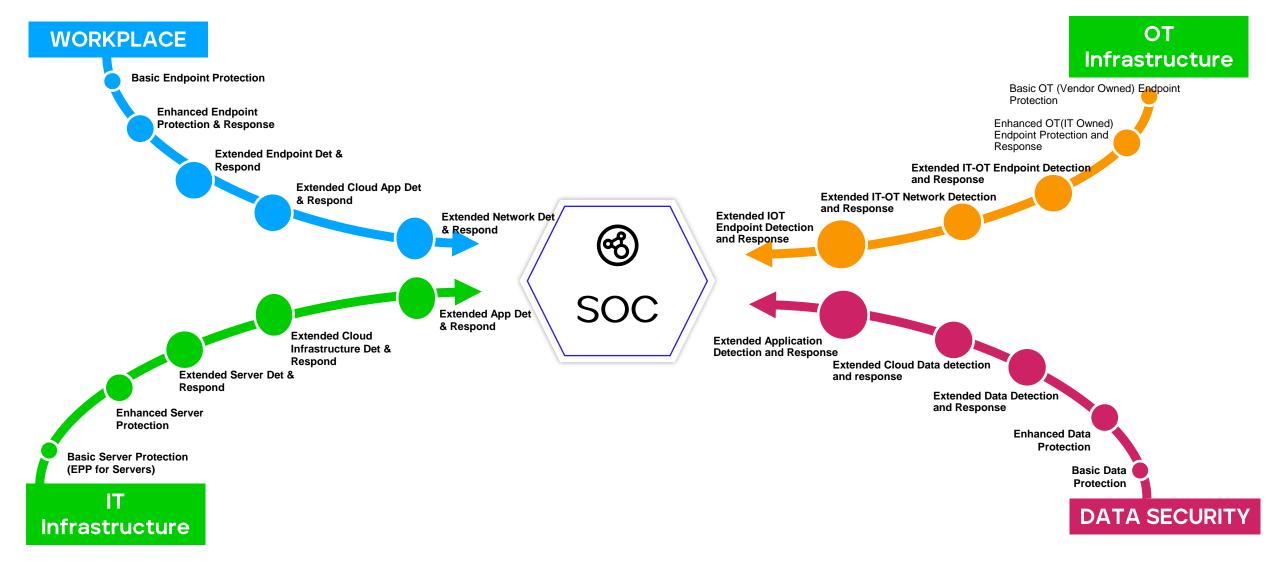
## Sec Ops Solutions Journey Map





Your journey	Customer Outcomes	Use cases	Trellix solutions
Basic Endpoint Protection	<ul> <li>Commodity Threat Detection</li> <li>Reduced effort to manage Endpoint security</li> <li>Microsoft Defender Replacement</li> </ul>	<ul> <li>Signature protection</li> <li>NGAV protection</li> <li>Vendor intelligence</li> <li>Central Endpoint management</li> <li>Compliance Reporting</li> </ul>	<ul> <li>Trellix Endpoint - ENS</li> <li>Trellix GTI</li> <li>Trellix Policy Auditor</li> <li>Endpoint Services – Health Watch</li> </ul>
Enhanced Endpoint Protection and Response	<ul> <li>Advanced Threat Detection</li> <li>Vendor Consolidation on Endpoint</li> <li>Mobile Worker Protection</li> <li>Improved incident investigations</li> <li>Microsoft Defender ATP Replacement</li> <li>Crowdstrike Replacement</li> </ul>	<ul> <li>Endpoint Detection and Response</li> <li>Advanced Endpoint Malware detection</li> <li>Custom Threat Intelligence</li> <li>Endpoint Forensics</li> <li>Credential Theft Protection</li> </ul>	<ul> <li>Trellix EDR</li> <li>Trellix Forensics</li> <li>Trellix Insights</li> <li>Trellix TIE</li> <li>Intel as a Service Basic</li> <li>Services – Incident Response</li> </ul>
Extended Endpoint Detection and Response	<ul> <li>Reduced SOC Alert Fatigue</li> <li>Reduced Time to Detect, Investigate APT and Ransomware Threats</li> <li>O365 Security Enhancements</li> <li>Reduce Risk of Data Breach</li> <li>Microsoft E5 Security Replacement</li> </ul>	<ul> <li>Endpoint Sandbox Protection</li> <li>Native XDR with Endpoint and Email</li> <li>Endpoint Data Protection</li> <li>Mobile Device Advanced Threat Detection</li> <li>Business Email Compromise and advanced email security</li> <li>XDR Sandbox Enrichment</li> </ul>	<ul> <li>Trellix XDR</li> <li>Trellix Mobile</li> <li>Trellix ETP or EX</li> <li>Trellix Endpoint DLP</li> <li>Trellix IVX Enterprise</li> <li>Services – XDR Assessment</li> </ul>
Extended Cloud Application Detection and Response	<ul> <li>Enables secure cloud adoption</li> <li>Reduce risk of application breach</li> <li>Reduce Risk of Data Breach</li> <li>Data Discovery and Visibility</li> <li>Secure Collaboration</li> </ul>	<ul> <li>O365, Google Workplace Threat Detection</li> <li>Collaboration Service Threat Detection</li> <li>Cloud Application Security Monitoring</li> </ul>	<ul> <li>Trellix XDR</li> <li>Trellix Network DLP</li> <li>Trellix IVX Enterprise</li> <li>Skyhigh CASB</li> <li>Services – Data Protection Program</li> </ul>
Extended Network Detection and Response	<ul> <li>Full Endpoint, Cloud, Data and Perimeter Threat Detection</li> <li>Root Cause Analysis Capability</li> <li>Reduce risk of ransomware data breach</li> </ul>	<ul> <li>Network C2 Detection</li> <li>Lateral Movement Detection</li> <li>Network traffic visibility</li> </ul>	<ul> <li>Trellix XDR</li> <li>Trellix NDR</li> <li>Trellix Network Forensics</li> <li>Services – Advisory Services</li> </ul>
olace ey	XDR		<b>T</b> ara II.a <b>(</b>
	Basic Endpoint ProtectionEnhanced Endpoint Protection and ResponseExtended Endpoint Detection and ResponseExtended Cloud Application Detection and ResponseExtended Network Detection and ResponseExtended Network Detection and ResponseExtended Network Detection and Response	<ul> <li>Control Concerner</li> <li>Basic Endpoint Protection</li> <li>Commodity Threat Detection</li> <li>Reduced effort to manage Endpoint security</li> <li>Microsoft Defender Replacement</li> <li>Advanced Threat Detection</li> <li>Vendor Consolidation on Endpoint</li> <li>Werder Protection</li> <li>Worker Protection</li> <li>Microsoft Defender ATP Replacement</li> <li>Crowdstrike Replacement</li> <li>Microsoft Defender ATP Replacement</li> <li>Crowdstrike Replacement</li> <li>Microsoft Defender ATP Replacement</li> <li>Crowdstrike Replacement</li> <li>Reduce Soc Alert Faigue</li> <li>Reduce Risk of Data Breach</li> <li>Microsoft E5 Security Replacement</li> <li>Reduce Risk of Data Breach</li> <li>Microsoft E5 Security Replacement</li> <li>Secure Collaboration</li> <li>Secure Callaboration</li> <li>Secure Collaboration</li> <li>Secure Collaboration&lt;</li></ul>	Basic Endpoint Protection <ul> <li>Commodity Threat Detection Reduced effort to manage Endpoint Reduced effort to manage Endpoint Protection and Response</li> <li>Microsoft Defender Replacement</li> <li>Signature protection</li> <li>Vendor intelligence</li> <li>Central Endpoint Management</li> <li>Consolidation on Endpoint Protection and Response</li> <li>Advanced Threat Detection</li> <li>Vendor Consolidation on Endpoint Protection and Response</li> <li>Advanced Threat Detection</li> <li>Vendor Consolidation on Endpoint Protection and Response</li> <li>Reduced SOC Alert Faigue Reduced Time to Detect, Investigate APT and Ransomware Threats Reduced Time to Detect, Investigate APT and Ransomware Threats Reduce Risk of Data Breach Microsoft E5 Security Replacement</li> </ul> <ul> <li>Endpoint Detection</li> <li>Endpoint Detection</li> <li>Business Email Compromise and advanced memals exclusion and Response</li> </ul> <ul> <li>Reduce Risk of Data Breach Protection Detect, Investigate APT and Response</li> <li>Microsoft E5 Security Replacement</li> <li>Endpoint Security Reduce Risk of Data Breach Protection Detection</li> <li>Business Email Compromise and advanced memal security Business Email Compromise and advanced</li> <li>Data Discovery and Visibility Becure Risk of Data Breach Prometer Threat Detection</li> <li>Claud Application Security Monitoring</li> <li>Secure Collaboration</li> <li>Claud Application Security Monitoring</li> </ul> <li>Network traffic visibility</li> <li>Reduce Risk of ransomware data breach</li> <li>Reduce Risk of ransomware data breach</li> <li>Network traffic visibility</li>

## Your Workplace XDR Journey

Copyright © 2023 Musarubra US LLC



E	Your journey	Benefits	Use cases	Trellix solutions
Foundation	Basic Server Protection	<ul> <li>Commodity Threat Detection</li> <li>Reduced effort to manage Endpoint security</li> <li>Microsoft Defender Replacement</li> </ul>	<ul> <li>Signature protection</li> <li>NGAV protection</li> <li>Vendor intelligence</li> <li>Central Endpoint management</li> <li>Compliance Reporting</li> </ul>	<ul> <li>Trellix ENS for Servers</li> <li>Trellix GTI</li> <li>Trellix Policy Auditor</li> <li>Endpoint Services – Health Watch</li> </ul>
Operational	Enhanced Server Protection and Response	<ul> <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> <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> <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>
	Extended Server Detection and Response	<ul> <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> <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> <li>Trellix XDR</li> <li>Trellix Network IPS</li> <li>Trellix IVX Enterprise</li> <li>Services - XDR assessments</li> <li>Services - INTaaS</li> </ul>
Trusted	Extended Cloud Infrastructure Detection and Response	<ul> <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> <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> <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>
	Extended Application Detection and Response	<ul> <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> <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> <li>Trellix XDR</li> <li>Trellix IVX Enterprise</li> <li>Trellix Database Security</li> <li>Service - Application Security Assessments</li> </ul>

## Your Infrastructure XDR Journey

XDR



Copyright © 2023 Musarubra US LLC

S	Your journey	Benefits	Use cases	Trellix solutions
Foundation	Basic Data Protection	<ul> <li>Accidental Loss Protection</li> <li>Regulatory Compliance</li> </ul>	<ul> <li>Removable Media Control</li> <li>Data Encryption</li> <li>Endpoint Data Protection</li> <li>Program establishment</li> </ul>	<ul> <li>Trellix MNE</li> <li>Trellix Drive Encryption</li> <li>Trellix Endpoint DLP</li> <li>Services: Data Security Program</li> </ul>
onal	Enhanced Data Protection	<ul> <li>Reduced risk of accidental data loss through email</li> <li>Decreased risk of accidental data loss through web usage</li> <li>Enhanced protection for mobile working</li> </ul>	<ul> <li>Data discovery</li> <li>On-prem file analysis</li> <li>Email Data Protection</li> <li>Web Data Protection</li> </ul>	<ul> <li>Trellix DLP Prevent</li> <li>Trellix DLP Discovery</li> <li>Trellix FX/AX</li> <li>Services: Data Security Program</li> </ul>
Operational	Extended Data Detection and Response	<ul> <li>Reduced DLP alert fatigue</li> <li>Decreased time to detect data exfiltration</li> <li>Crown jewel protection</li> </ul>	<ul> <li>Native data threat detection in XDR</li> <li>Identity detection and response</li> <li>Data for root cause analysis</li> </ul>	<ul> <li>Trellix XDR</li> <li>Trellix DLP Monitor</li> <li>Trellix Identity Partner integration</li> <li>Services: XDR assessments</li> </ul>
g	Extended Cloud Data detection and response	<ul> <li>Secure cloud adoption</li> <li>Reduced risk of cloud data breach</li> <li>Enhanced protection for business applications</li> </ul>	<ul> <li>SASE data and UBA protection</li> <li>Intelligence-enriched Cloud logs</li> <li>Protection for cloud storage</li> <li>Protection for business applications</li> </ul>	<ul> <li>Trellix XDR</li> <li>Trellix IVX Enterprise</li> <li>Trellix SASE partners integration</li> </ul>
Trusted	Extended Application Detection and Response	<ul> <li>Full data, application and network visibility</li> <li>Reduced risk of data breach</li> <li>Enhanced protection for business applications</li> <li>Regulatory Compliance</li> </ul>	<ul> <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> <li>Trellix XDR</li> <li>Trellix IVX Enterprise</li> <li>Trellix Database Security</li> <li>Trellix IPS and vIPS</li> <li>Service - Application Security Assessments</li> </ul>
Your Data Journey	XDR	XDR		
Copyright © 2023 Musarubra US LLC				Trellix

ы	Your journey	Benefits	Use cases	Trellix solutions
Foundation	Basic OT (Vendor Owned) Endpoint Protection	<ul> <li>Threat Protection</li> <li>Central management of IT-OT endpoint security</li> <li>Regulatory Compliance</li> </ul>	<ul> <li>Signature protection</li> <li>NGAV protection</li> <li>Removeable Media protection</li> <li>System Lockdown</li> <li>Central management</li> </ul>	<ul> <li>Trellix Endpoint</li> <li>Trellix Device Control</li> <li>Trellix Application Control</li> <li>Services: OT Security Assessment</li> </ul>
onal	Enhanced OT(IT Owned) Endpoint Protection and Response	<ul> <li>Advanced Threat Detection</li> <li>OnPrem Endpoint Management</li> <li>Improved OT incident investigations</li> <li>Microsoft Defender ATP Replacement</li> <li>Crowdstrike Replacement</li> </ul>	<ul> <li>Endpoint Detection and Response</li> <li>Advanced Endpoint Malware detection</li> <li>OT Threat Intelligence</li> <li>Endpoint Forensics</li> <li>Credential Theft Protection</li> </ul>	<ul> <li>Trellix Forensics</li> <li>Trellix Insights</li> <li>Trellix TIE</li> <li>Intel as a Service Basic</li> <li>Services – Incident Response</li> </ul>
Operational	Extended IT-OT Endpoint Detection and Response	<ul> <li>Reduced endpoint alert fatigue</li> <li>Reduced time to detect OT threats</li> <li>OT visibility</li> </ul>	<ul> <li>Threat Detection across IT-OT</li> <li>OT network threat detection</li> <li>OT Asset Discovery</li> <li>IT-OT Lateral Movement</li> <li>Credential Theft Detection</li> </ul>	<ul> <li>Trellix XDR</li> <li>Trellix NX</li> <li>Deception Tool Partners</li> <li>Trellix Comm Broker</li> <li>Services:</li> </ul>
eq	Extended IT-OT Network Detection and Response	<ul> <li>Reduce network alert fatigue</li> <li>OT Asset Risk Intelligence</li> <li>Root Cause Analysis</li> </ul>	<ul> <li>Native network, endpoint and OT system detection in XDR</li> <li>Anomaly detections</li> <li>Network Forensics</li> <li>IT-OT DLP</li> </ul>	<ul> <li>Trellix XDR</li> <li>Trellix SCADA Security Partners</li> <li>Trellix PX</li> <li>Trellix Network DLP Monitor</li> </ul>
Trusted	Extended IOT Endpoint Detection and Response	<ul> <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> <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> <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>
T-OT	XDR	XDR		
ubra US LLC				Trellix

Your IT Journe Copyright © 2023 Musarubra US LLC