Trellix

24-26 OCTOBER 2023

EMEA Security Summit

Rome, Italy

Trellix

Before, During, After

Ransomware Attacks

Speaker Intro

Who's that Guy

Mo Cashman

EMEA Field CTO

Steen Pedersen

PM, Endpoint

AGENDA

- Welcome
- State of Ransomware
- Anatomy of Attack
- Endpoint - Before, During and After
- Q/A

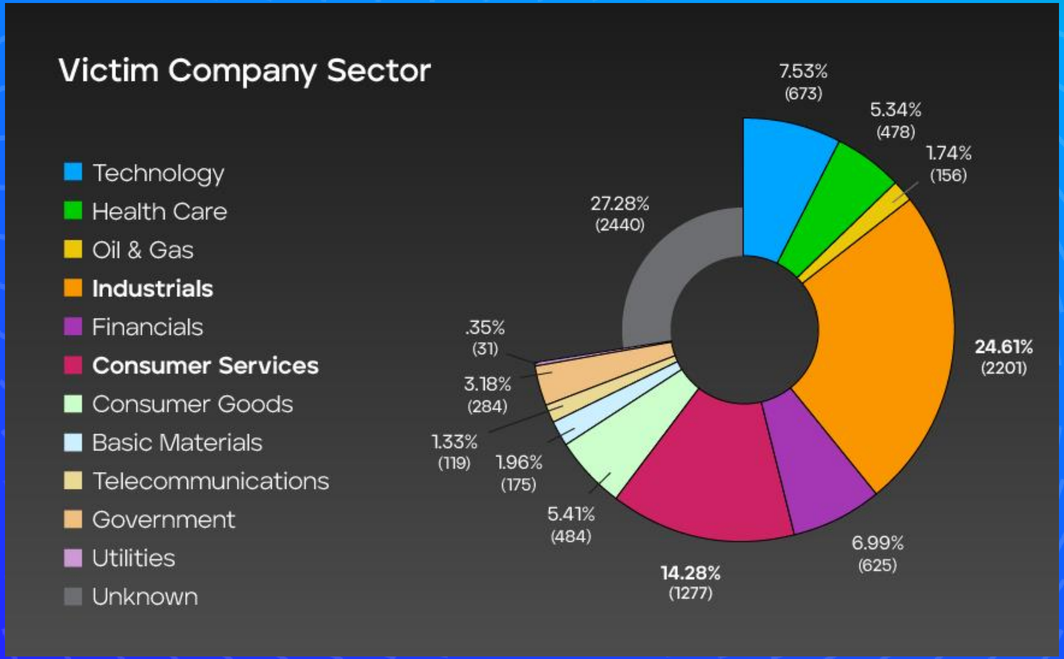
State of Ransomware

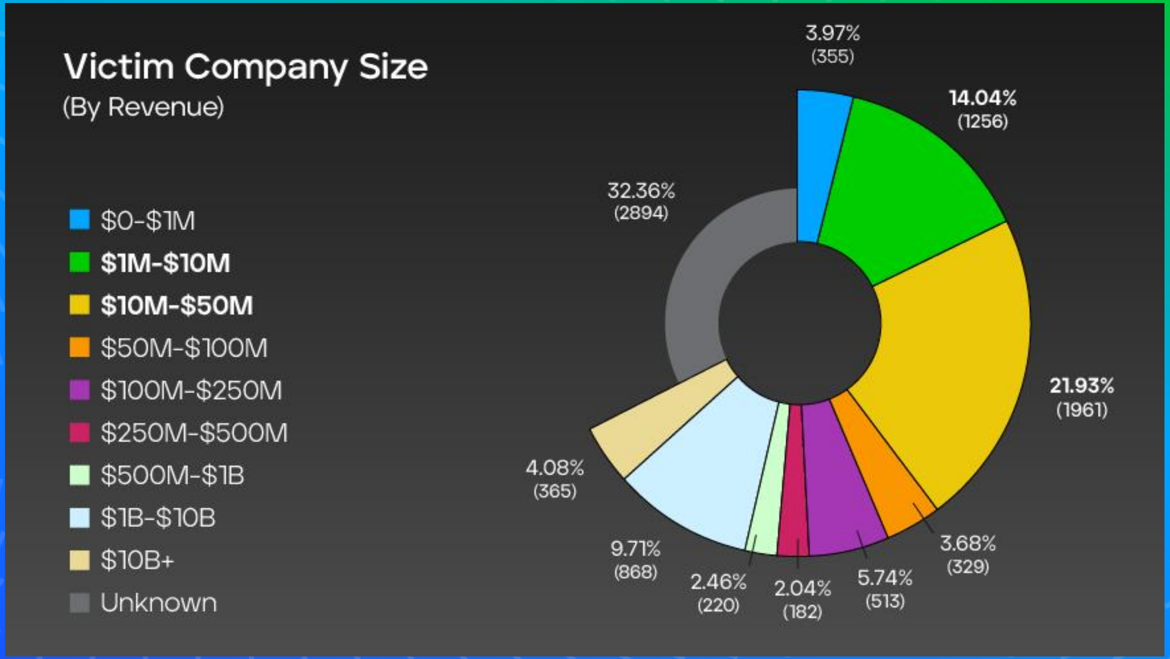
How has Ransomware evolved?

Trellix

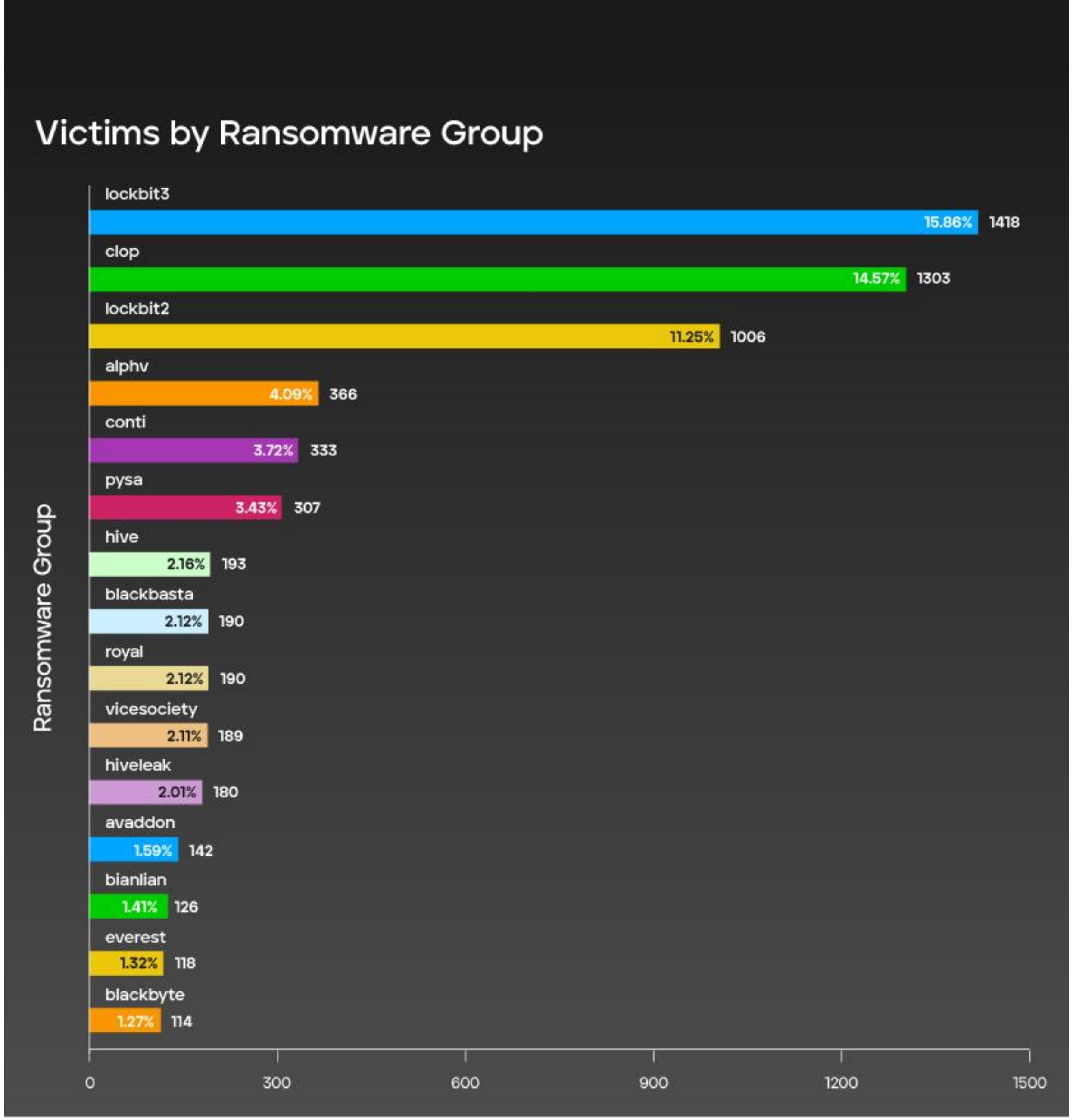
1

Ransomware Prevalence


Victim Company Sector


Victim Company Size
(By Revenue)

Victims by Ransomware Group



Constantly Under Attack

Ransomware

54%

Organizations reported ransomware blocked access to systems / data[1]

Gaps in visibility

21 days

Average attacker dwell time before being discovered[2]

Ignored Alerts

35%

Security analysts who say alerts are ignored when the queue is full[3]

Reoccurring Attacks

43%

Organizations hit by ransomware were hit more than once[4]

[1] Future Enterprise Resiliency & Spending Survey - Wave 11, IDC, December 2021
[2] Infosecurity magazine
[3] IDC Survey 2021
[4] 2022 Third-party breach report, Black Kite

Trellix

The nature and velocity of collaboration has changed

New avenues of entry and risk

Email

Still the primary attack vector. Over 90 % of cyberattacks begin with phishing.

Collaboration Platforms (Box, Teams, Slack etc.)

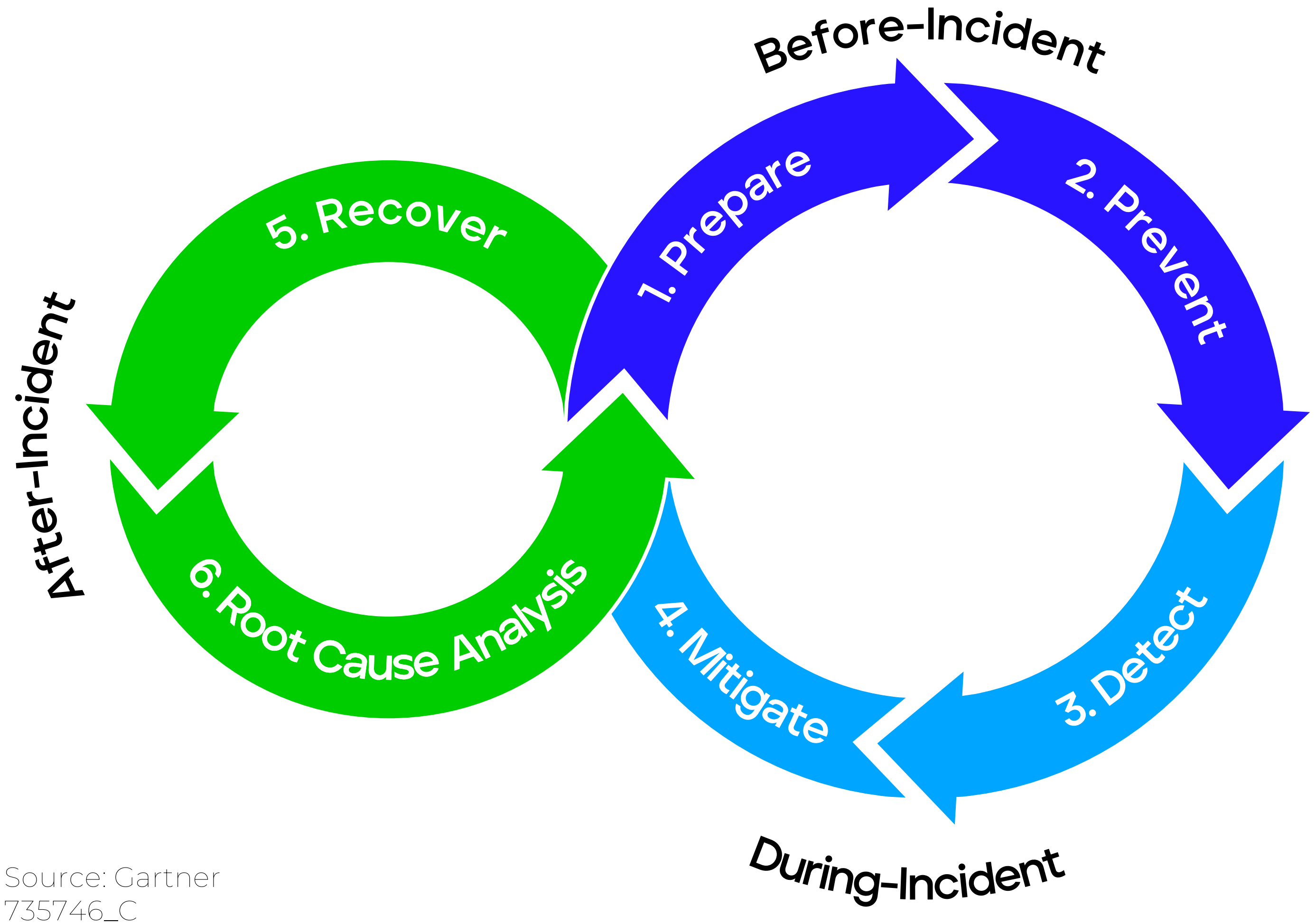
Allow us to freely share information, but do not ensure the integrity of what is being shared

Enterprise Applications (Workday, Salesforce etc.)

Digital transformation initiatives grant access to suppliers, vendors, customers – and threat actors

Ransomware Defense is a constant process

Ransomware Defensive Lifecycle

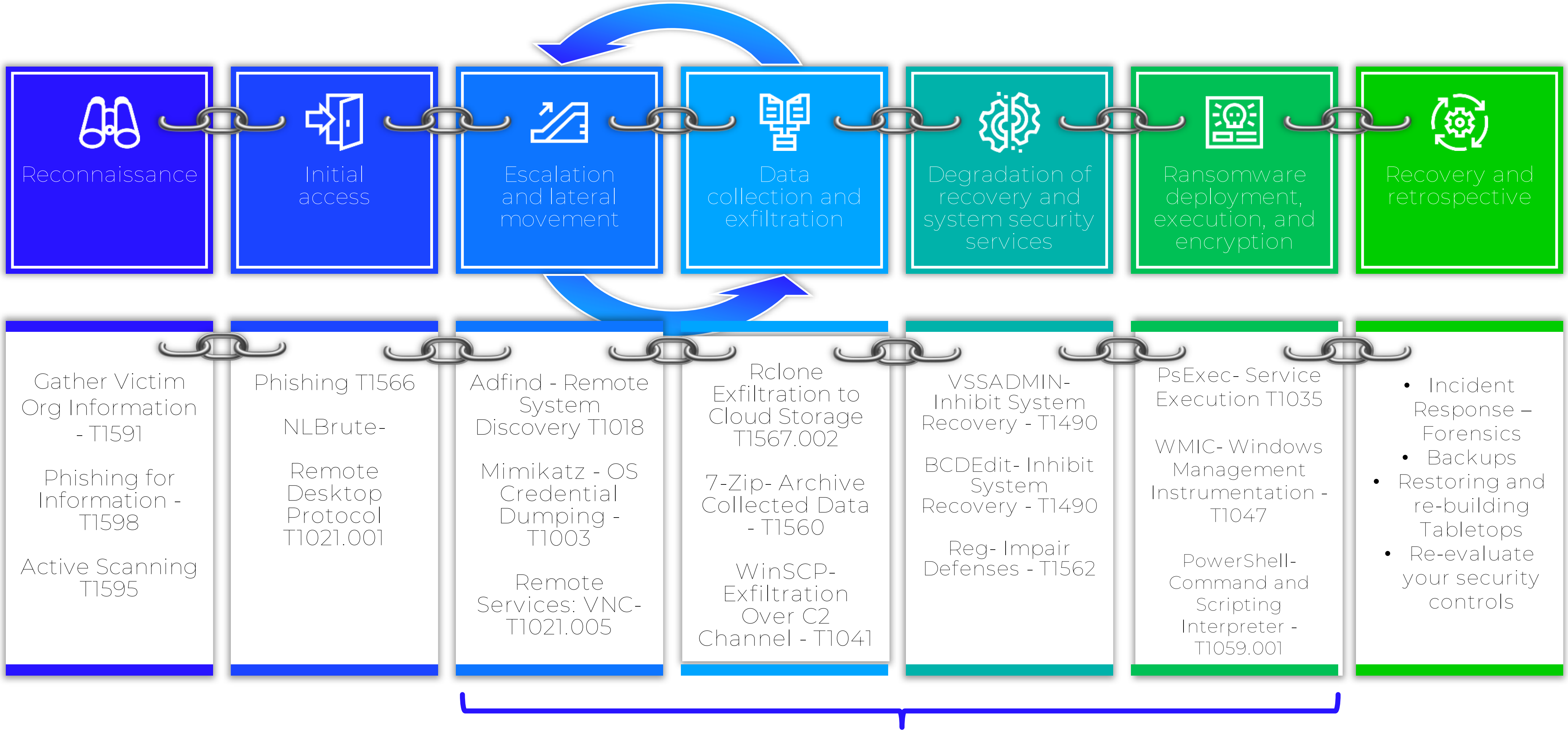


The defense life cycle is a continuous process of **Preparation, Prevention, Detection and Mitigating Attacks**. When a ransomware attack is successful, the **Recovery** and **Root Cause Analysis** phases are triggered.

Source: Gartner
735746_C

Trellix

The Phases of a Ransomware Attack

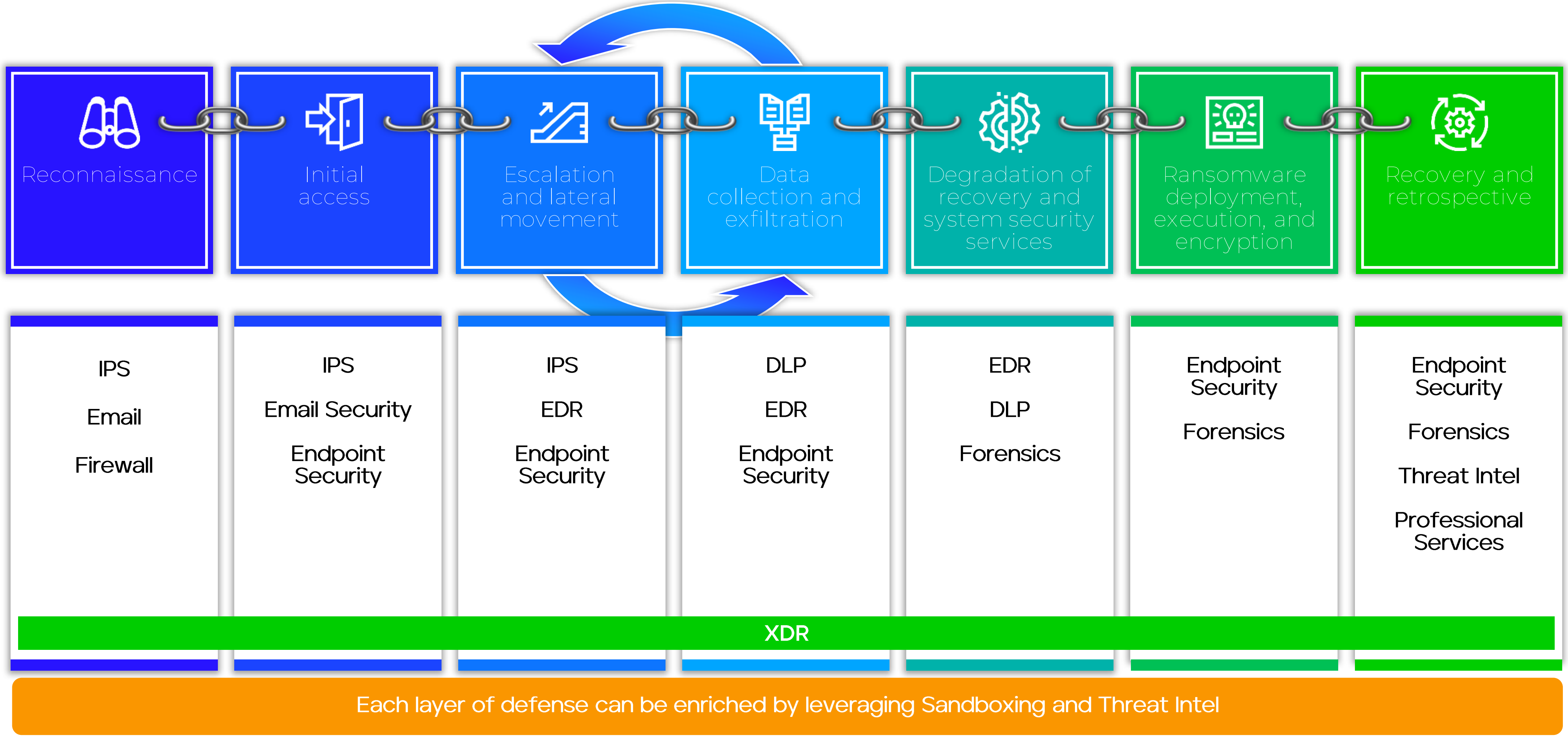


Reconnaissance	Initial access	Escalation and lateral movement	Data collection and exfiltration	Degradation of recovery and system security services	Ransomware deployment, execution, and encryption	Recovery and retrospective
Gather Victim Org Information - T1591 Phishing for Information - T1598 Active Scanning T1595	Phishing T1566 NLBrute- Remote Desktop Protocol T1021.001	Adfind - Remote System Discovery T1018 Mimikatz - OS Credential Dumping - T1003 Remote Services: VNC- T1021.005	Rclone Exfiltration to Cloud Storage T1567.002 7-Zip- Archive Collected Data - T1560 WinSCP- Exfiltration Over C2 Channel - T1041	VSSADMIN- Inhibit System Recovery - T1490 BCDEdit- Inhibit System Recovery - T1490 Reg- Impair Defenses - T1562	PsExec- Service Execution T1035 WMIC- Windows Management Instrumentation - T1047 PowerShell- Command and Scripting Interpreter - T1059.001	• Incident Response – Forensics • Backups • Restoring and re-building Tabletops • Re-evaluate your security controls

COBALT STRIKE / SLIVER/ METASPLOIT

The Phases of a Ransomware Attack

Trellix Kill Chain



Reconnaissance	Initial access	Escalation and lateral movement	Data collection and exfiltration	Degradation of recovery and system security services	Ransomware deployment, execution, and encryption	Recovery and retrospective
IPS Email Firewall	IPS Email Security Endpoint Security	IPS EDR Endpoint Security	DLP EDR Endpoint Security	EDR DLP Forensics	Endpoint Security Forensics	Endpoint Security Forensics Threat Intel Professional Services

XDR

Each layer of defense can be enriched by leveraging Sandboxing and Threat Intel

Trellix

Trellix Endpoint Security Capability Overview

Management Capability

- Asset Discovery & Policy Management
- Cloud or On-Premise Deployment
- Event Monitoring & Reporting
- Compliance Reporting
- Third Party Integration
- XDR Integration

Security Capability

Attack Surface Management

- Exposure Monitoring
- Device Control
- Host Firewall
- Web Control
- Configuration Audit

Attack Prevention

- Signature Anti-Malware
- Behavioral Threat Protection
- Global Threat Intelligence
- Local Threat Intelligence
- Exploit Prevention
- Custom IOCs
- Sandboxing
- Mobile Threat Detection
- Application Whitelisting
- Roll back remediation

Endpoint Detection Response and Forensics

- MITRE Att&ck Mapping
- Behavioral Detections
- Guided Investigations
- Enterprise Search
- Attack Timelines
- OS Event Streaming
- Credential Monitoring
- Custom IOCs
- Forensic Data Acquisition
- Remediation

Data Protection

- Device Control
- Data Discovery
- Data Classification
- Data Loss Prevention
- Drive Encryption

Threat Research and Intelligence

- Threat Research
- Product Testing
- Signatures
- Global Threat Intelligence
- Threat Campaigns

Trellix

Before

- ✓ Are we protected?
- ✓ How do we minimize the attack surface?
- ✓ How do we improve our security posture?

During

- ✓ What is happening?
- ✓ What is the blast radius?
- ✓ What should we investigate and what action should we take?

After

- ✓ What is the scope? Are other endpoints affected?
- ✓ How did the attacker get in?
- ✓ How do we make sure it does not happen again?

Trellix Endpoint: Visibility & Control over the full life cycle of all your Endpoints

- Endpoint security management at scale
- Pro-active attack surface management
- Rich & fully-featured threat prevention stack

- Efficient and effective alerts and incidents triage
- Fast response and containment
- AI Guided investigation

- Forensics and root cause analysis
- Real-time and historical artifacts search
- Long-term remediation

Trellix

Attack Surface Management

Endpoint Posture + Security Intelligence

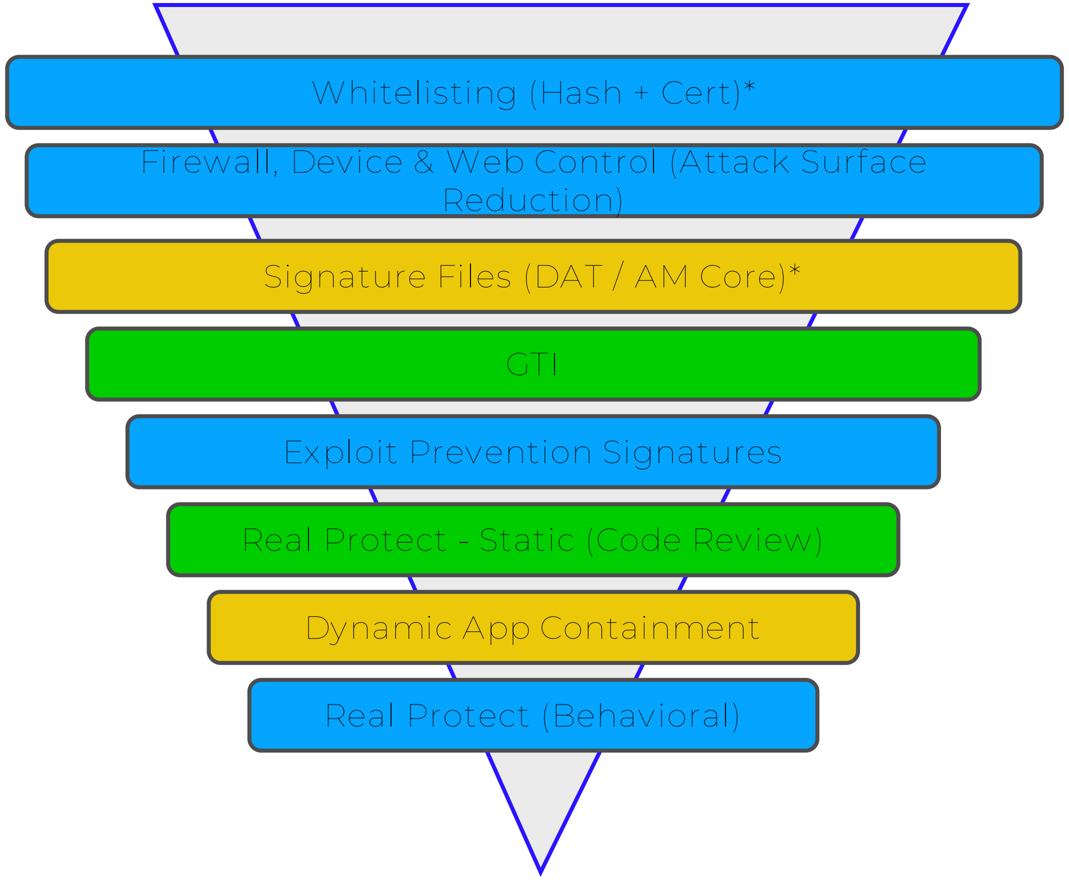
Threat Readiness Problems	Causes	Solution
"Are you at risk? What is a priority?"	Global Visibility, Priority	Rank worldwide threats to you
"Are you susceptible? Will your protections hold?"	Predict and Prioritize Impact	Assess your security posture risks
"What do you need to change to be protected?"	Proactively Adapt	Proactively tune countermeasures

Trellix

Insights Demo

Attack Prevention

What makes ENS so good?


Whitelisting (Hash + Cert)*

Firewall, Device & Web Control (Attack Surface Reduction)

Signature Files (DAT / AM Core)*

GTI

Exploit Prevention Signatures

Real Protect - Static (Code Review)

Dynamic App Containment

Real Protect (Behavioral)

1. Layered Defense
2. Customizable Signatures
3. Optimized for PC or Servers
4. On Prem or Cloud Managed
5. Third Party Validation

	AV-Comparatives [1]			SE Labs [2]		AV Test [3]
	False Positives	Malware Protection Rate	Impact Score (lower is better)	Protection Score	Not blocked (Neutralized or Compromised)	Protection / Performance / Usability (max 6)
Trellix	**Very Low**	**99.9%**	**10.9**	**100%**	**0**	**6 / 6 / 6**
Brand C	Very High	99.7%	16.8	98%	1	-
Brand M	Medium	99.9%	18.1	100%	1	6 / 6 / 6
Brand S	-	-	-	97%	6	-

Trellix

Endpoint Security - ASR

Attack Surface Reduction

1. Limit what unknown processes can do
   - Prevent processes which are contained getting Write or Read access to documents - Based on filename or folder
   - Simple example for Expert rule:

```
Rule {
    Process {
        Include PROCESS_STATE_BITS -name DAC_CONTAIN_PID_BITS { -v 0x1 }
    }
    Target {
        Match FILE {
                Include OBJECT_NAME { -v "**.doc" }
                Include OBJECT_NAME { -v "**.docx" }
                Include OBJECT_NAME { -v "**.xls" }
                Include OBJECT_NAME { -v "**.xlsx" }
            Include -access "WRITE DELETE"
        }
    }
}
```

https://github.com/trellix-enterprise/ExpertRules/blob/main/TRELLIX/ACCESS_PROTECTION/T1486_Attempt_to_Encrypt_data_for_Impact.md#t1486---attempt-to-encrypt-data-for-impact

Endpoint Security - ASR

Attack Surface Reduction

2. WebControl - Block access to uncatagorized websites
3. Firewall – Block unknown processes network access
4. ATP – Key Behavior Signtaures to contain malicious use of powershell, office apps, credential theft
5. TIE – Add your own indicators for fast reaction

Attack Surface Reduction

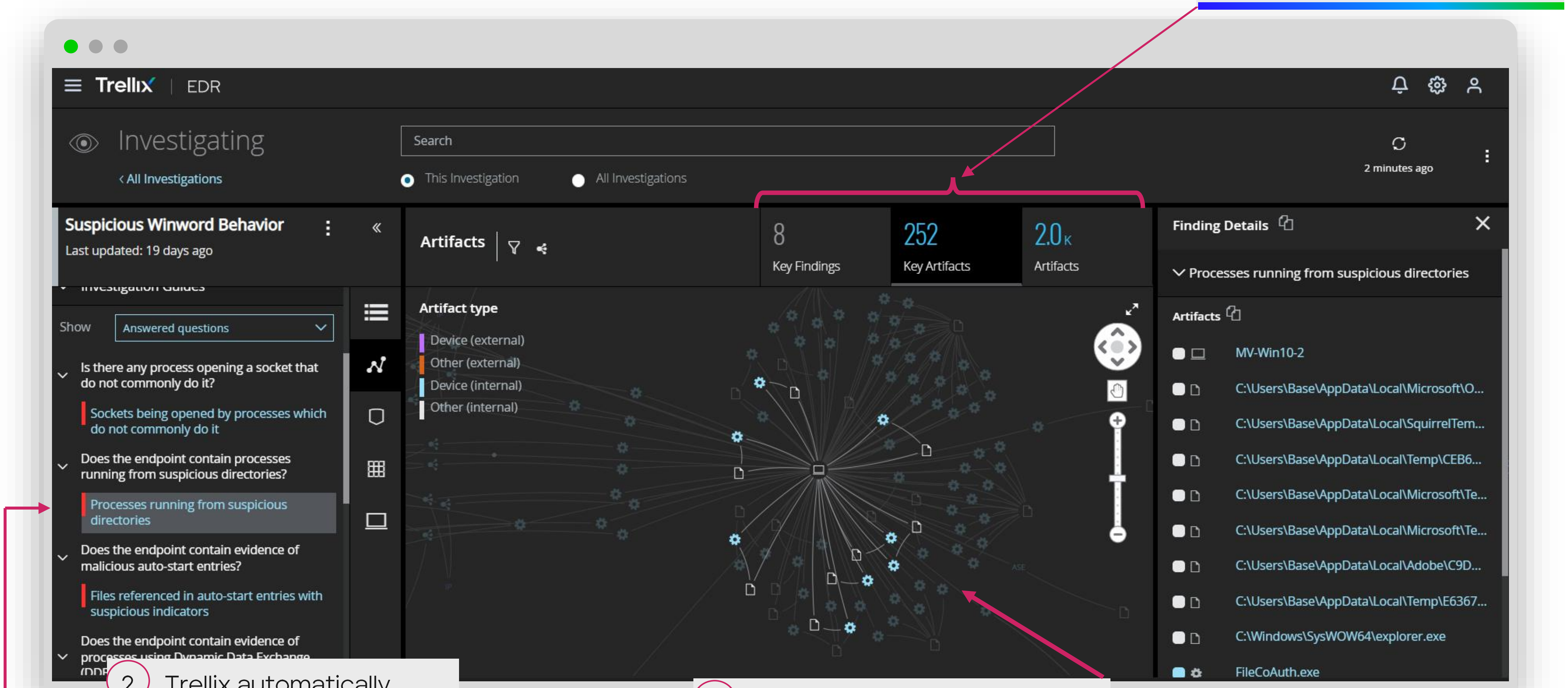
Prevention Through Intelligent Application Control

Dynamic Whitelisting	Prevents all unauthorized code from running
Memory Protection	Prevents allow listed apps from being exploited via buffer overflow attacks
File Reputation	Integrates with GTI and TIE to classify binaries as Good, Bad and Unknown
Containment	Coordinates with ATD to assess unknown behavior and immunize endpoints

Threat Detection

AI-Guided Investigations with EDR

1. 2,000 artifacts analyzed, narrowed down to 252 key artifacts and 8 key findings



Trellix | EDR

Investigating

‹ All Investigations

Search

● This Investigation ○ All Investigations

2 minutes ago

Suspicious Winword Behavior

Last updated: 19 days ago

Investigation Guides

Show: Answered questions

- Is there any process opening a socket that do not commonly do it?
  - Sockets being opened by processes which do not commonly do it
- Does the endpoint contain processes running from suspicious directories?
  - Processes running from suspicious directories
- Does the endpoint contain evidence of malicious auto-start entries?
  - Files referenced in auto-start entries with suspicious indicators
- Does the endpoint contain evidence of processes using Dynamic Data Exchange (DDE

Artifacts

8	252	2.0K
Key Findings	Key Artifacts	Artifacts

Artifact type

- Device (external)
- Other (external)
- Device (internal)
- Other (internal)

Finding Details

Processes running from suspicious directories

Artifacts

- MV-Win10-2
- C:\Users\Base\AppData\Local\Microsoft\O...
- C:\Users\Base\AppData\Local\SquirrelTem...
- C:\Users\Base\AppData\Local\Temp\CEB6...
- C:\Users\Base\AppData\Local\Microsoft\Te...
- C:\Users\Base\AppData\Local\Microsoft\Te...
- C:\Users\Base\AppData\Local\Adobe\C9D...
- C:\Users\Base\AppData\Local\Temp\E6367...
- C:\Windows\SysWOW64\explorer.exe
- FileCoAuth.exe

2. Trellix automatically provides answers to the SOC analysts

3. Graphical view of Step 2 results to guide the analyst to get further details

Trellix

EDR/XDR Demo

Incident Response

Scoping and Forensics with HX

Protection

Malware Prevention

ENS

MalwareGuard

ENS

ExploitGuard

Real-time Indicators of Compromise (IoC)

Detect and Investigate

Enterprise Search EDR

Forensic Acquisition

Attack Summary and Audit Viewer EDR

Endpoint Automated Investigation

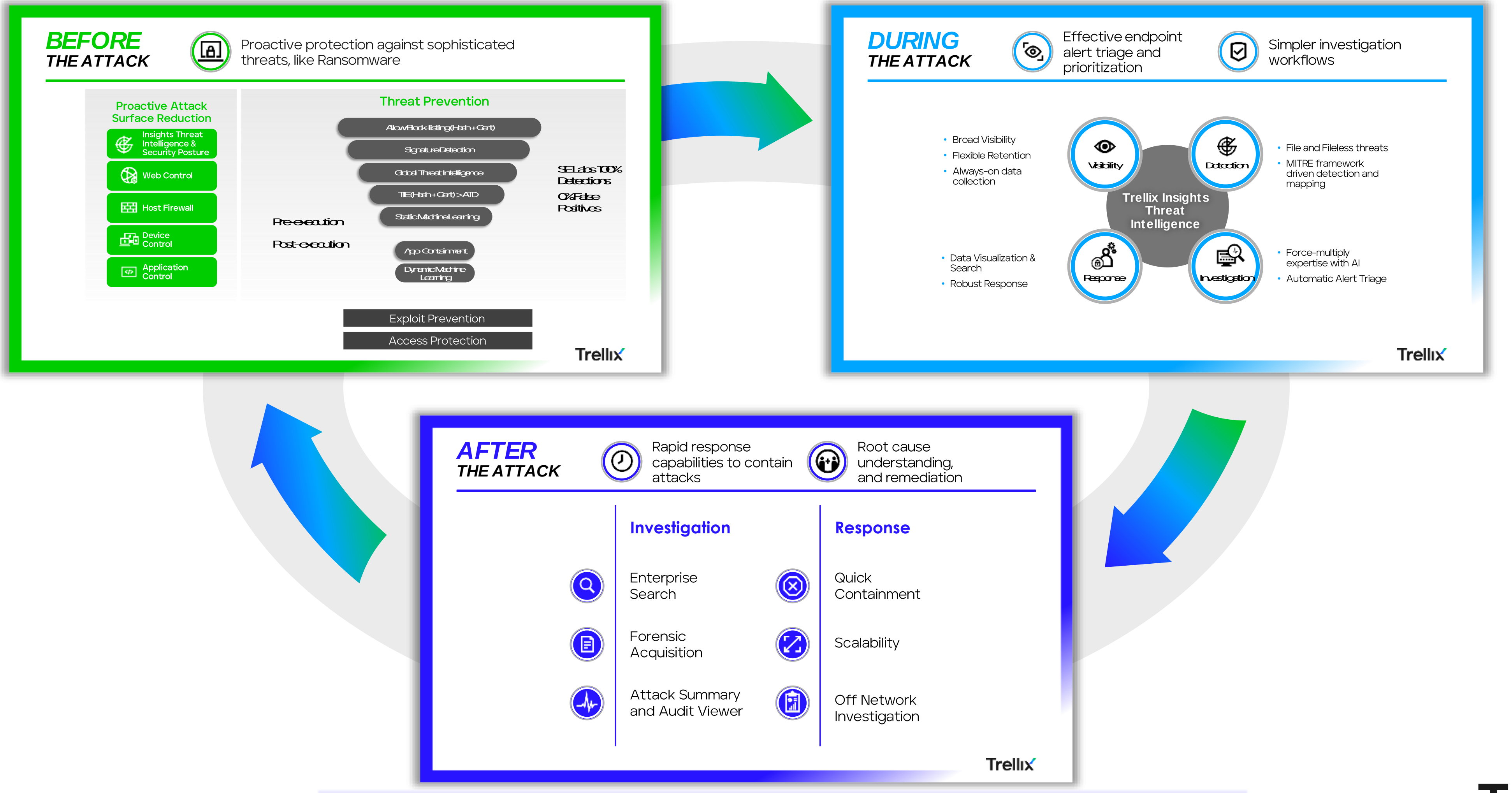
Logon Tracker

Event Streamer

Off-Network Investigation

Trellix

Defense in Depth – Layered Security



BEFORE THE ATTACK

Proactive protection against sophisticated threats, like Ransomware

Proactive Attack Surface Reduction

- Insights Threat Intelligence & Security Posture
- Web Control
- Host Firewall
- Device Control
- Application Control

Threat Prevention

Pre-execution

- Allow/Block-listing (Hash + Cert)
- Signature Detection
- Global Threat Intelligence
- TIE (Hash + Cert) > ATD
- Static Machine Learning

Post-execution

- App Containment
- Dynamic Machine Learning

SE Labs 100% Detections

0% False Positives

Exploit Prevention

Access Protection

Trellix

DURING THE ATTACK

Effective endpoint alert triage and prioritization

Simpler investigation workflows

Trellix Insights Threat Intelligence

Visibility
- Broad Visibility
- Flexible Retention
- Always-on data collection

Detection
- File and Fileless threats
- MITRE framework driven detection and mapping

Response
- Data Visualization & Search
- Robust Response

Investigation
- Force-multiply expertise with AI
- Automatic Alert Triage

Trellix

AFTER THE ATTACK

Rapid response capabilities to contain attacks

Root cause understanding, and remediation

Investigation	Response
Enterprise Search	Quick Containment
Forensic Acquisition	Scalability
Attack Summary and Audit Viewer	Off Network Investigation

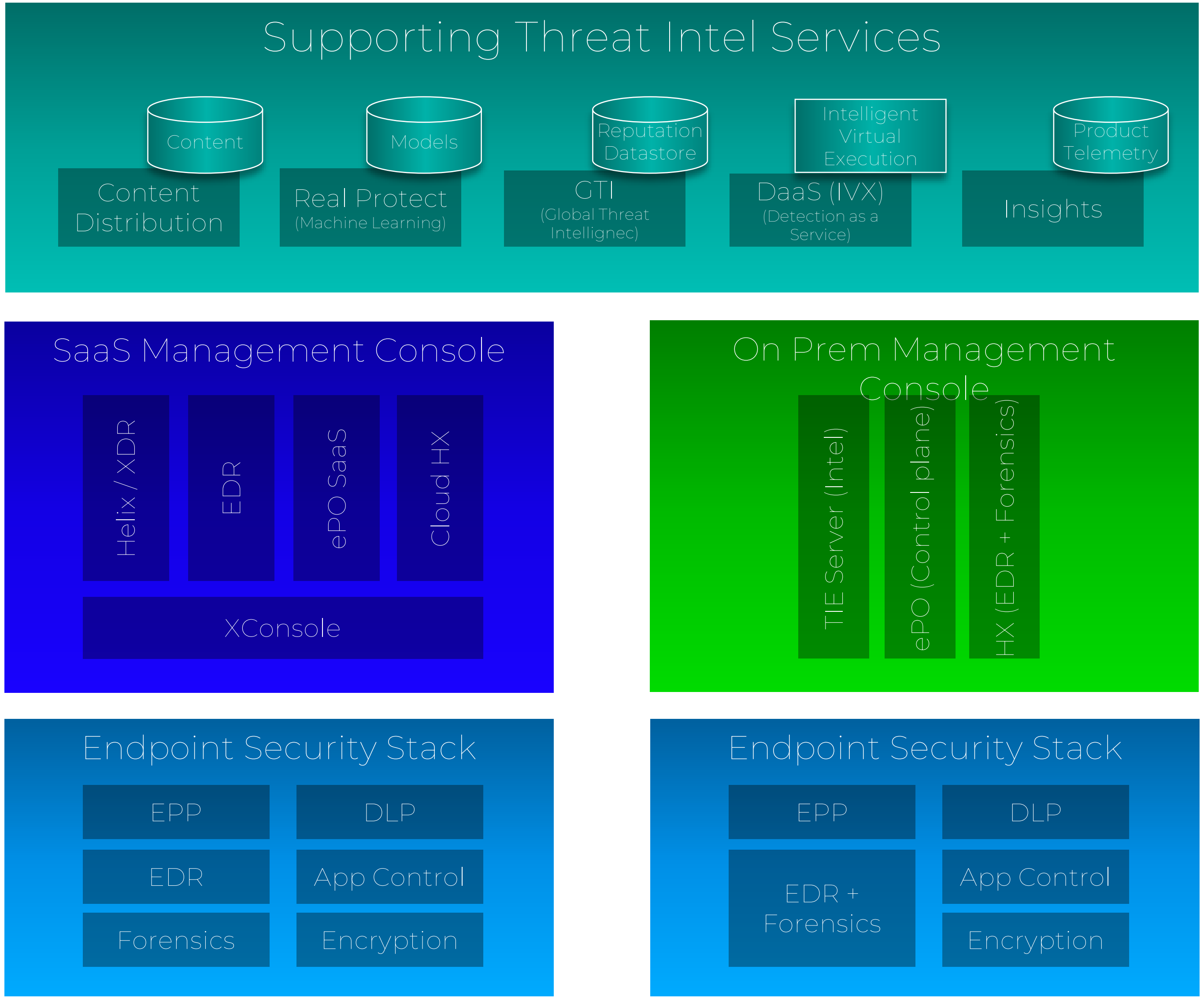
Trellix

Proactive and reactive security controls with differentiated advanced forensic capabilities

Trellix

Deployment Architectures

Support for diverse deployment architectures



Supporting Threat Intel Services

Content

Content Distribution

Models

Real Protect
(Machine Learning)

Reputation Datastore

GTI
(Global Threat Intellignec)

Intelligent Virtual Execution

DaaS (IVX)
(Detection as a Service)

Product Telemetry

Insights

SaaS Management Console

Helix / XDR

EDR

ePO SaaS

Cloud HX

XConsole

On Prem Management Console

TIE Server (Intel)

ePO (Control plane)

HX (EDR + Forensics)

Endpoint Security Stack

EPP

DLP

EDR

App Control

Forensics

Encryption

Endpoint Security Stack

EPP

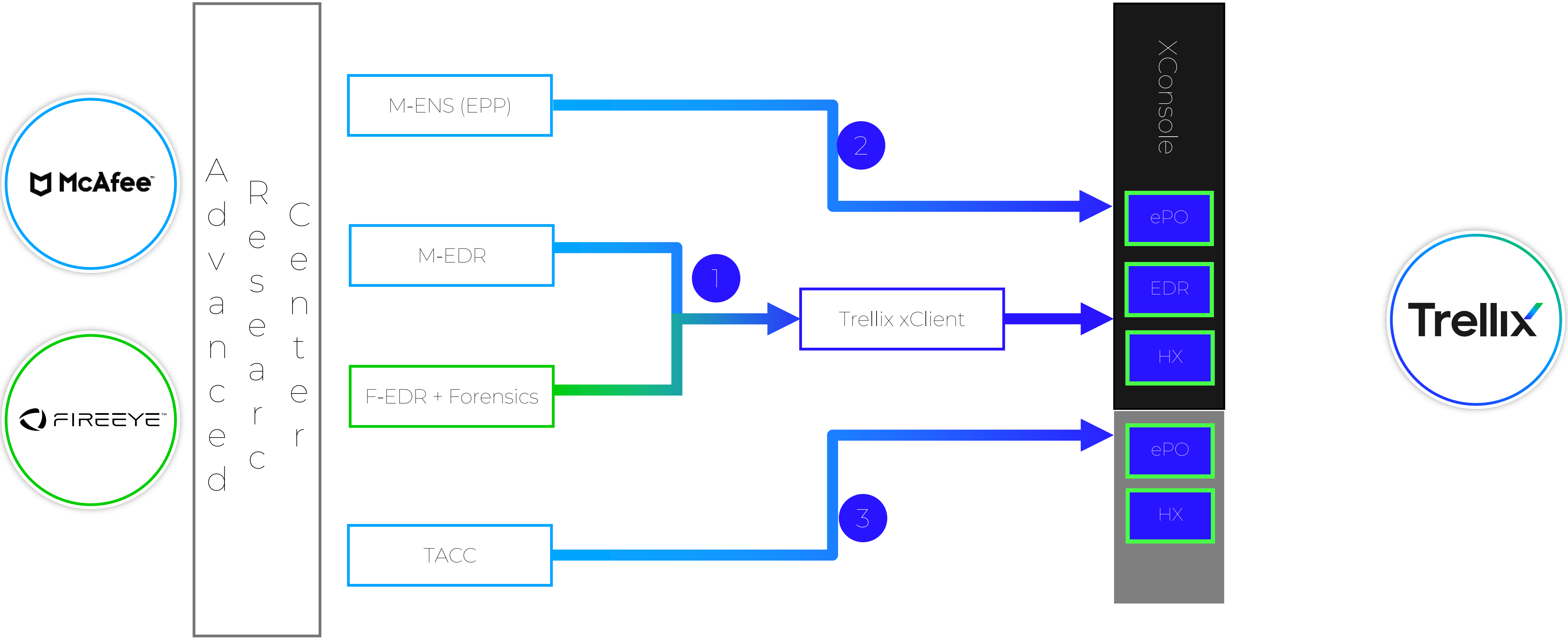
DLP

EDR + Forensics

App Control

Encryption

Trellix Endpoint Security Stack



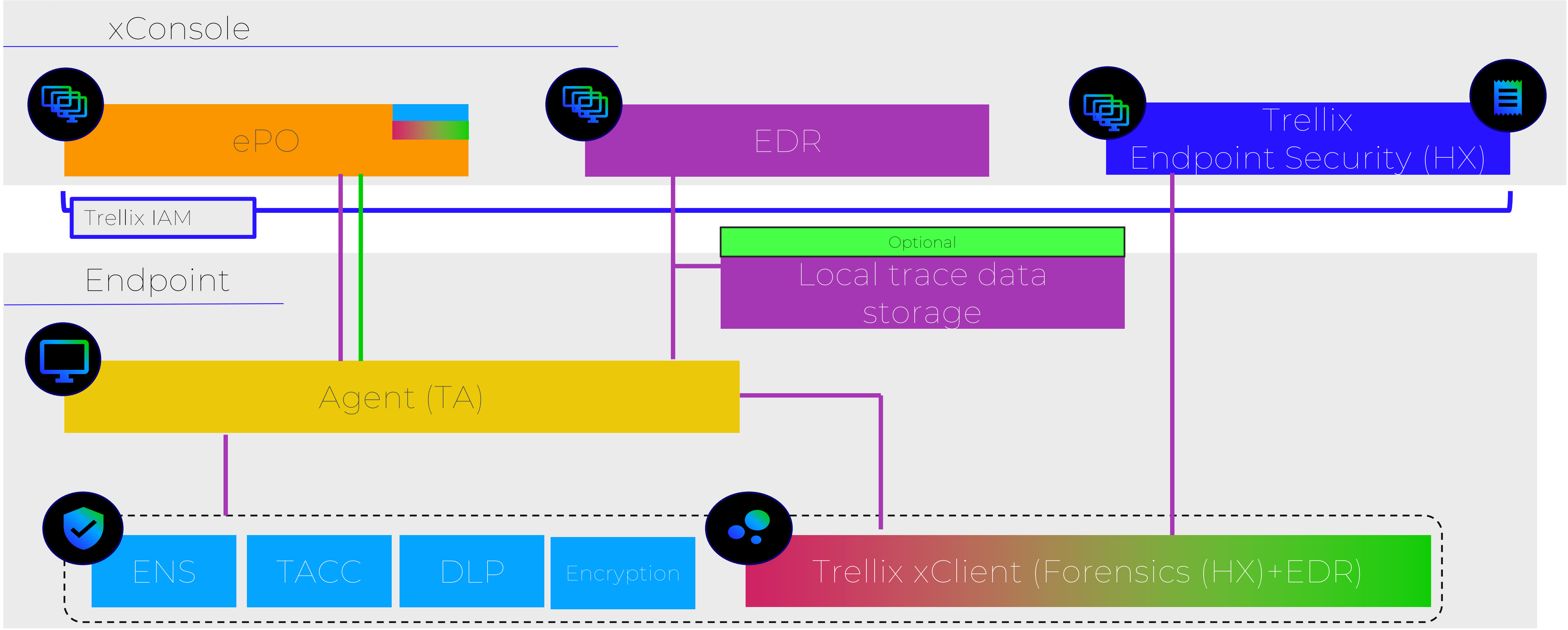
Trellix

Conceptual Endpoint Journey

Value Propositions

1) Single EDR/Forensics (HX) agent called Trellix xClient
2) Policy for all Trellix endpoint products to be managed from ePO

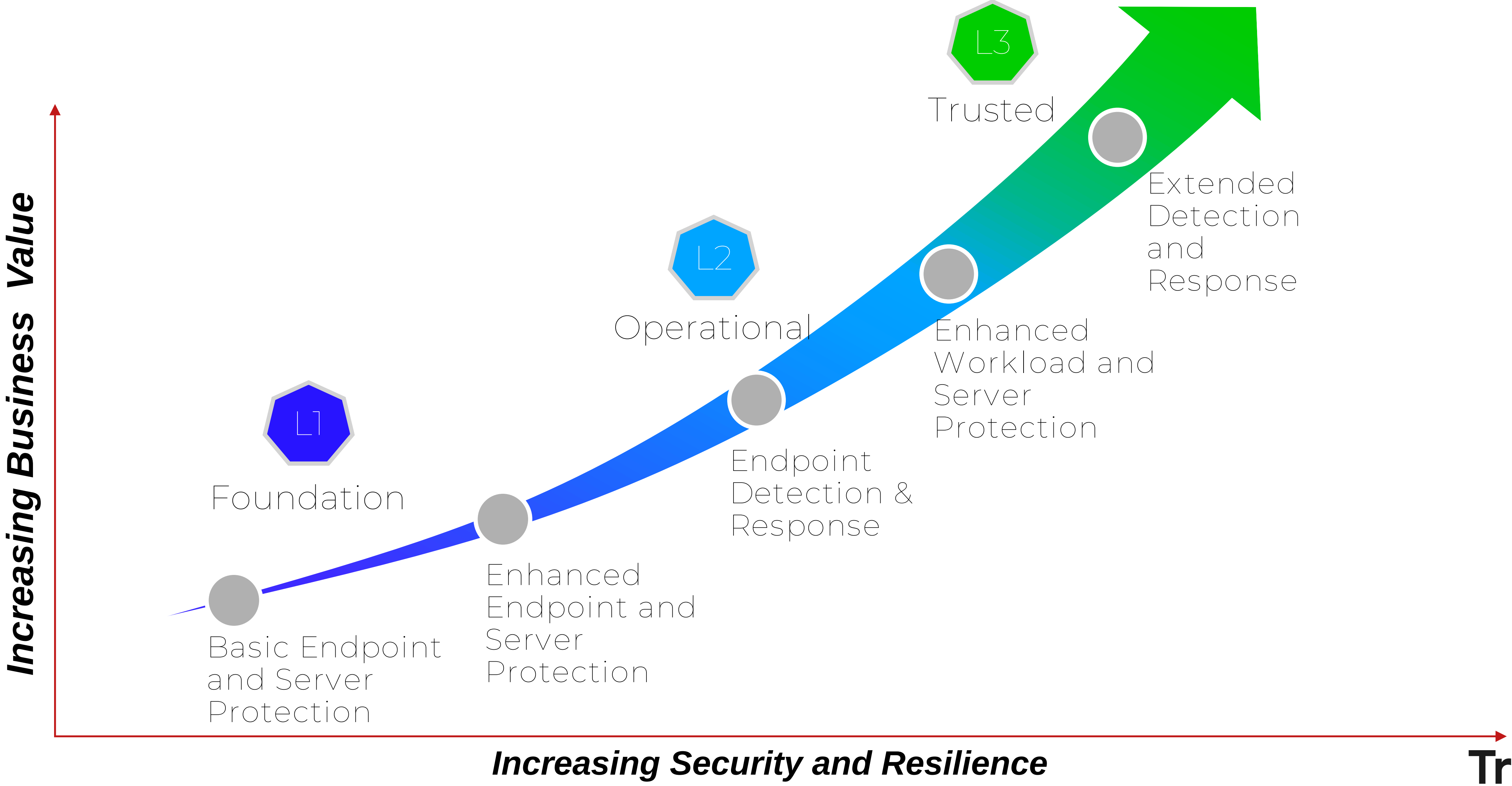
Phase 2.0 (SaaS)



Trellix

Endpoint Security

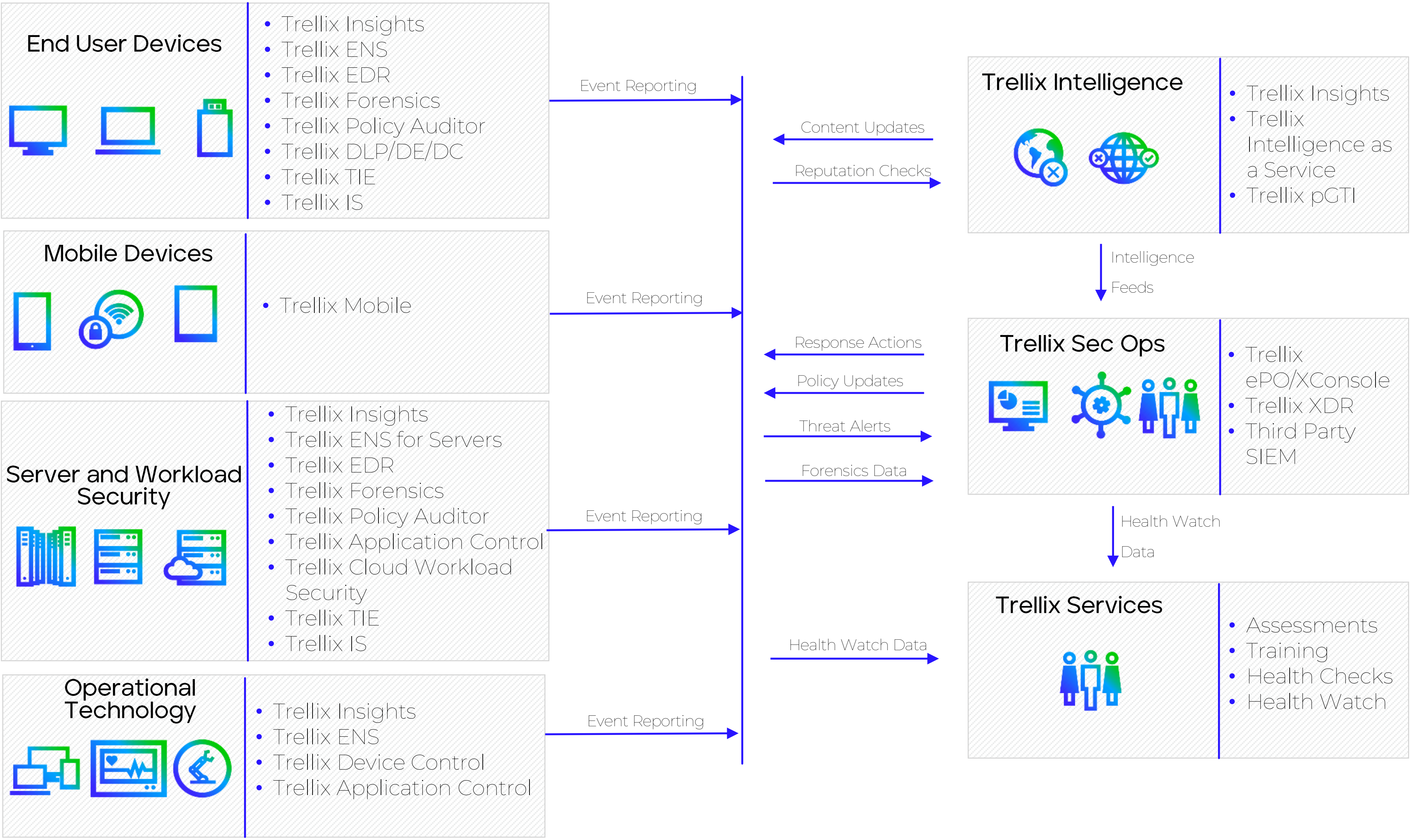
Customer Outcomes Journey Map



L3
Trusted
L2
Operational
L1
Foundation
Basic Endpoint and Server Protection
Enhanced Endpoint and Server Protection
Endpoint Detection & Response
Enhanced Workload and Server Protection
Extended Detection and Response
Increasing Business Value
Increasing Security and Resilience

Trellix

Endpoint Security Solution Reference Architecture



End User Devices

- Trellix Insights
- Trellix ENS
- Trellix EDR
- Trellix Forensics
- Trellix Policy Auditor
- Trellix DLP/DE/DC
- Trellix TIE
- Trellix IS

Event Reporting

Mobile Devices

- Trellix Mobile

Event Reporting

Server and Workload Security

- Trellix Insights
- Trellix ENS for Servers
- Trellix EDR
- Trellix Forensics
- Trellix Policy Auditor
- Trellix Application Control
- Trellix Cloud Workload Security
- Trellix TIE
- Trellix IS

Event Reporting

Operational Technology

- Trellix Insights
- Trellix ENS
- Trellix Device Control
- Trellix Application Control

Event Reporting

Content Updates

Reputation Checks

Trellix Intelligence

- Trellix Insights
- Trellix Intelligence as a Service
- Trellix pGTI

Intelligence Feeds

Response Actions

Policy Updates

Threat Alerts

Forensics Data

Trellix Sec Ops

- Trellix ePO/XConsole
- Trellix XDR
- Third Party SIEM

Health Watch Data

Health Watch Data

Trellix Services

- Assessments
- Training
- Health Checks
- Health Watch

Trellix

QA

Trellix

Thank You!