Trellix

24-26 OCTOBER 2023

EMEA Security Summit

Rome, Italy

Trellix

Ransomware

Tabletop Exercise

Speaker Intro

Who's that Guy

Mo Cashman

EMEA Field CTO

Filippo Sitzia

Sr Solutions Architect

Trellix

AGENDA

- Welcome
- State of Ransomware
- Anatomy of Attack
- Threat Response Exercise
- Solutions Architecture

State of Ransomware

How has Ransomware evolved?

Trellix

Anatomy of Attack

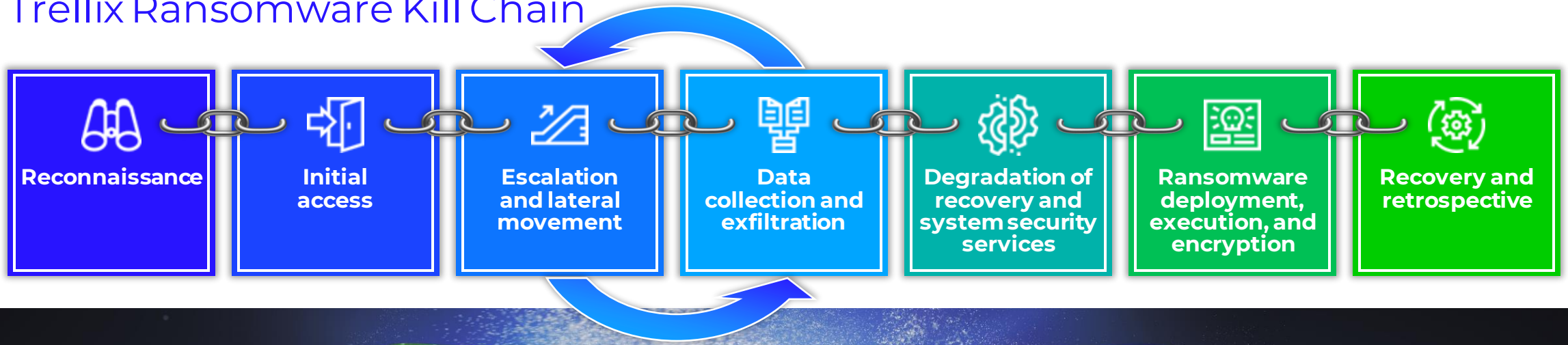
What does an attack look like?

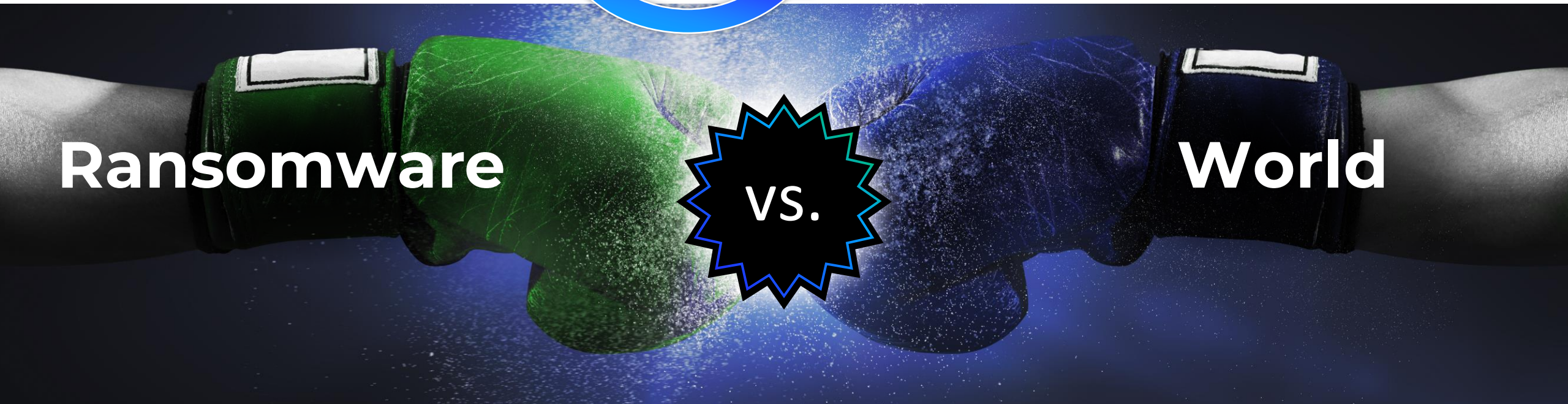
.

Trellix

The Phases of a Ransomware Attack

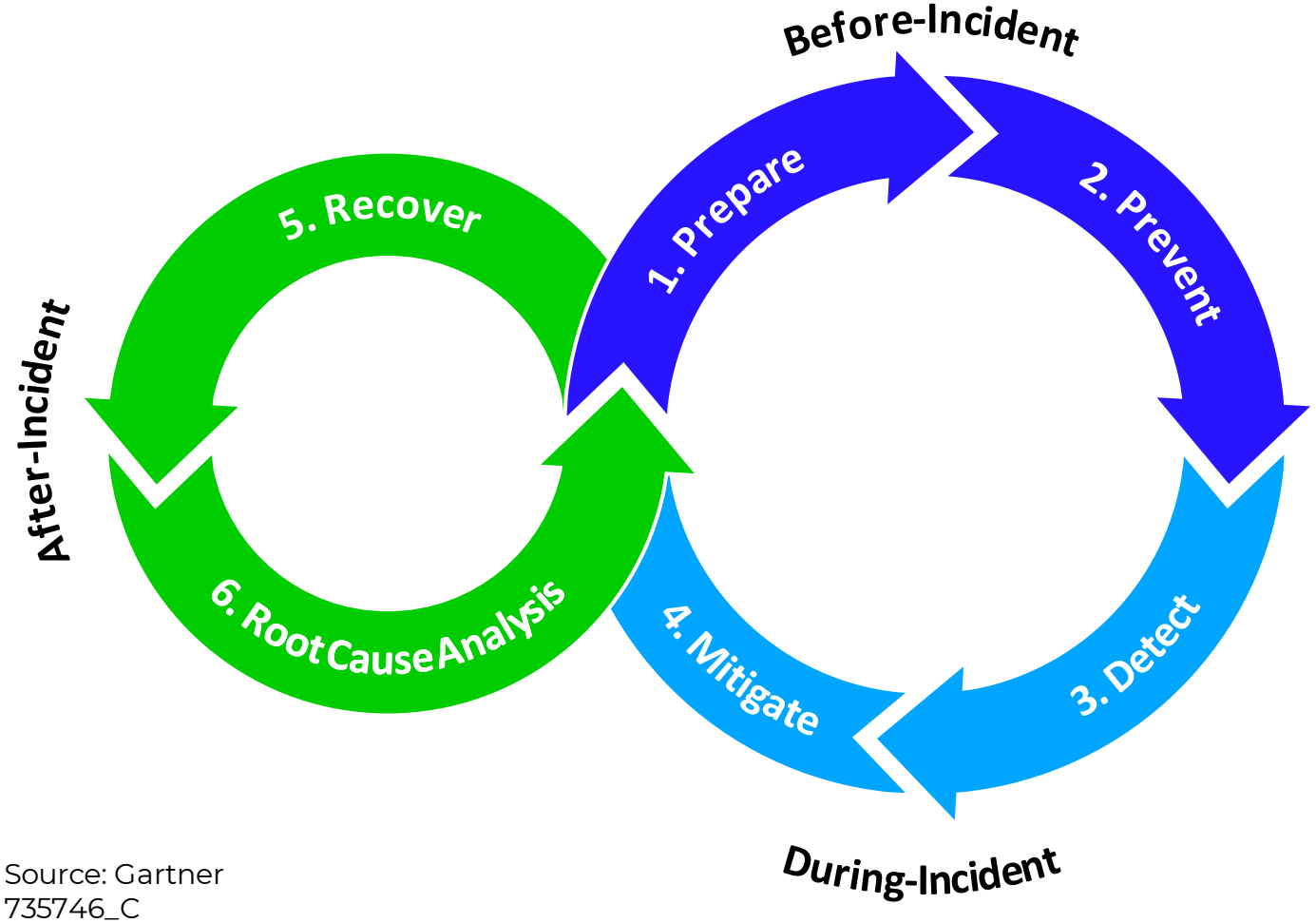
Trellix Ransomware Kill Chain





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

Xpress Threat Response

Put yourself into the throws of an incident

Trellix

Exercise Rules

1. Interactive training and learning exercise – not a test!
2. There are no “hidden agendas” or trick questions.
3. Open and interactive discussion – share your best practices
4. Use the Defense Lifecycle when thinking of best practices
5. Take notes on each stage and scenario in the Workshop Handout

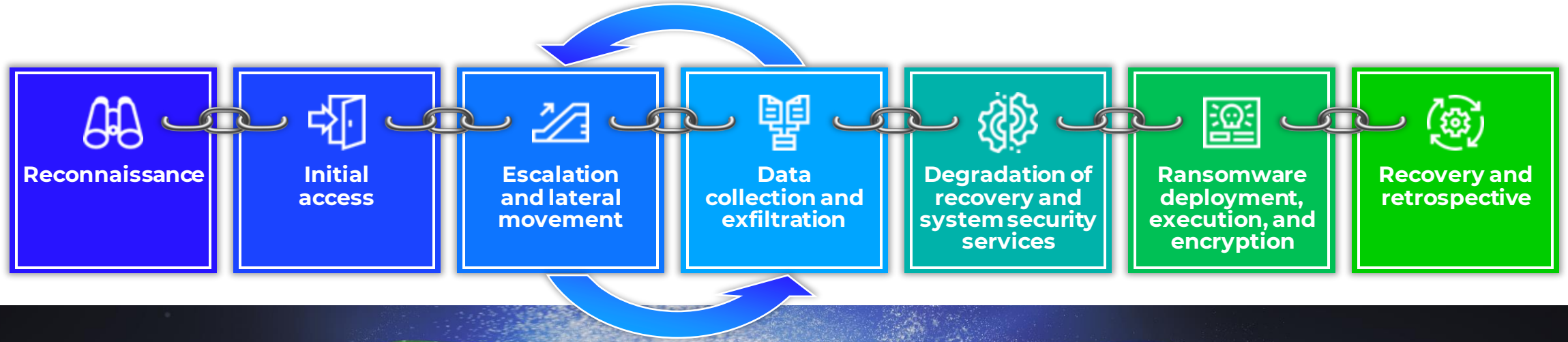
Trellix

Can you help Feelingsafe.com Feel safer?

Trellix

The Phases of a Ransomware Attack

Trellix Ransomware Kill Chain



FEELINGSAFE

Feelingsafe is a compassionate insurance provider specializing in mental health support.

Our mission is to offer a safety net for your emotional well-being.

With a deep understanding of the challenges many face, we provide comprehensive coverage tailored to mental health needs.

e-mail us today for a free consultation!

John.Butter@feelingsafe.ovh

Feelingsafe, a company that genuinely cares.

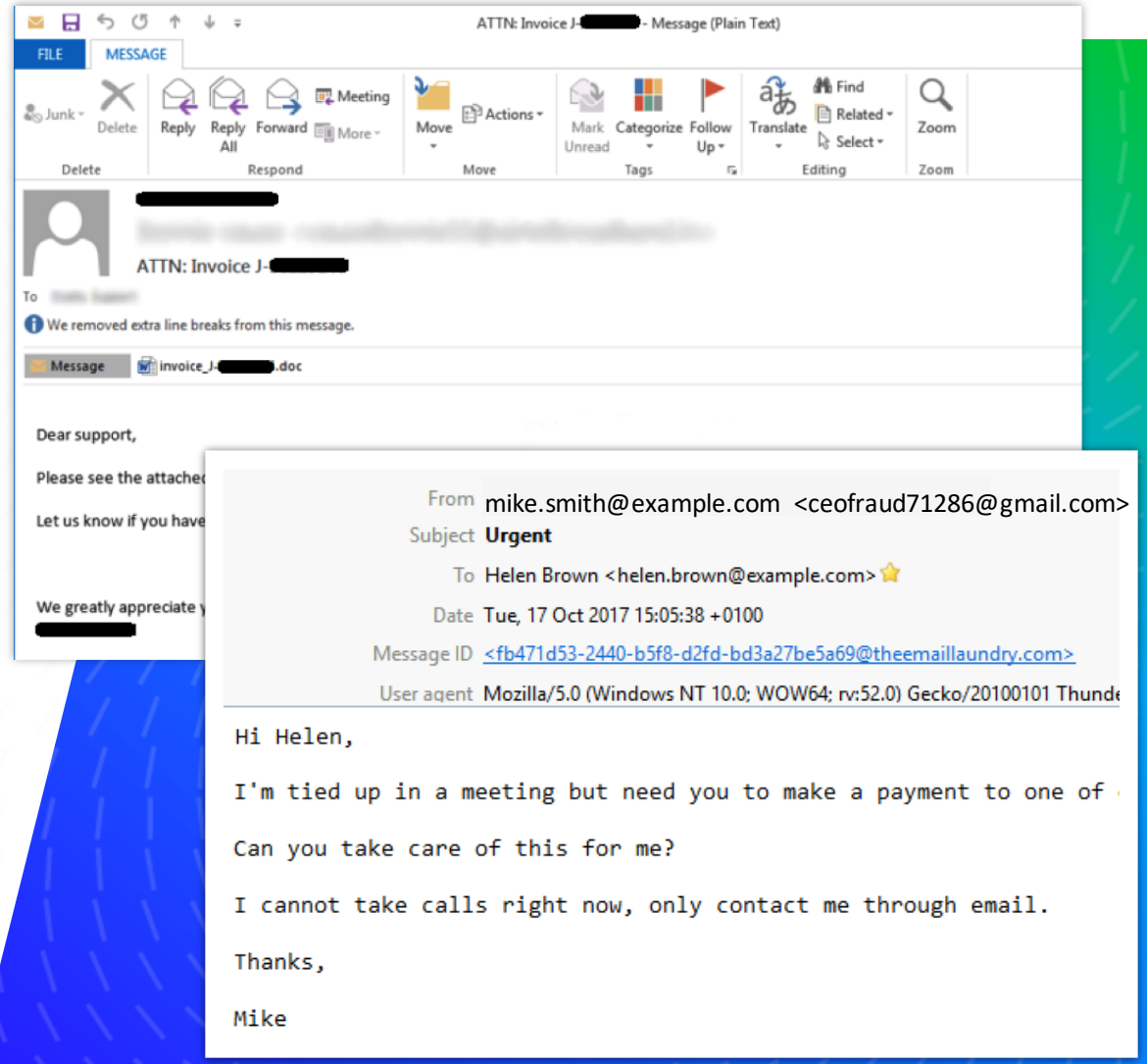
Trellix

Initial access

Time: 9:00 AM

Event: Help desk suspicious email call

An email gets sent to a group of users across the company. Your email protection tool will recognize this email as a phishing attempt; however, before that happens, a certain number of emails will come through. Only a few users reported the email to the help desk. Unfortunately, a number of users opened the attachment.



Trellix

Escalation and lateral movement

Time: 11:00 AM

Event: Suspicious “Hands-on-Keyboard” activity in the network

The Security Operations Center (SOC) receives some alerts of suspicious “Living off the Land (LotL) activities such as Windows CMD, PowerShell, system admin tools, and red teaming tools/scripts.

Trellix

Data collection and exfiltration

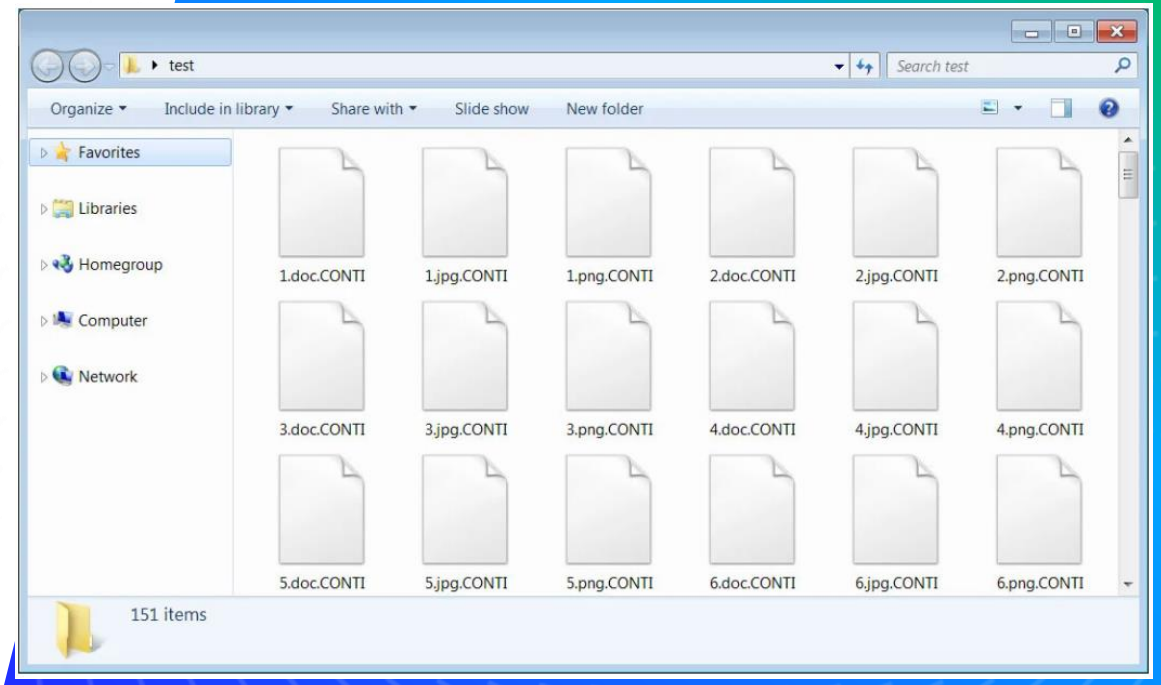
Time: 1:30 PM

Event: Reports of Data Leakage

The attackers just tweeted some passwords to show they mean business

Trellix

Degradation of recovery and system security services



Time: 2:30 PM

Event: Reports of inaccessible files and shares

Some users started to complain about files on the local system and those on remote SMB network shares being inaccessible as they used to be.

Trellix

Ransomware deployment, execution, and encryption

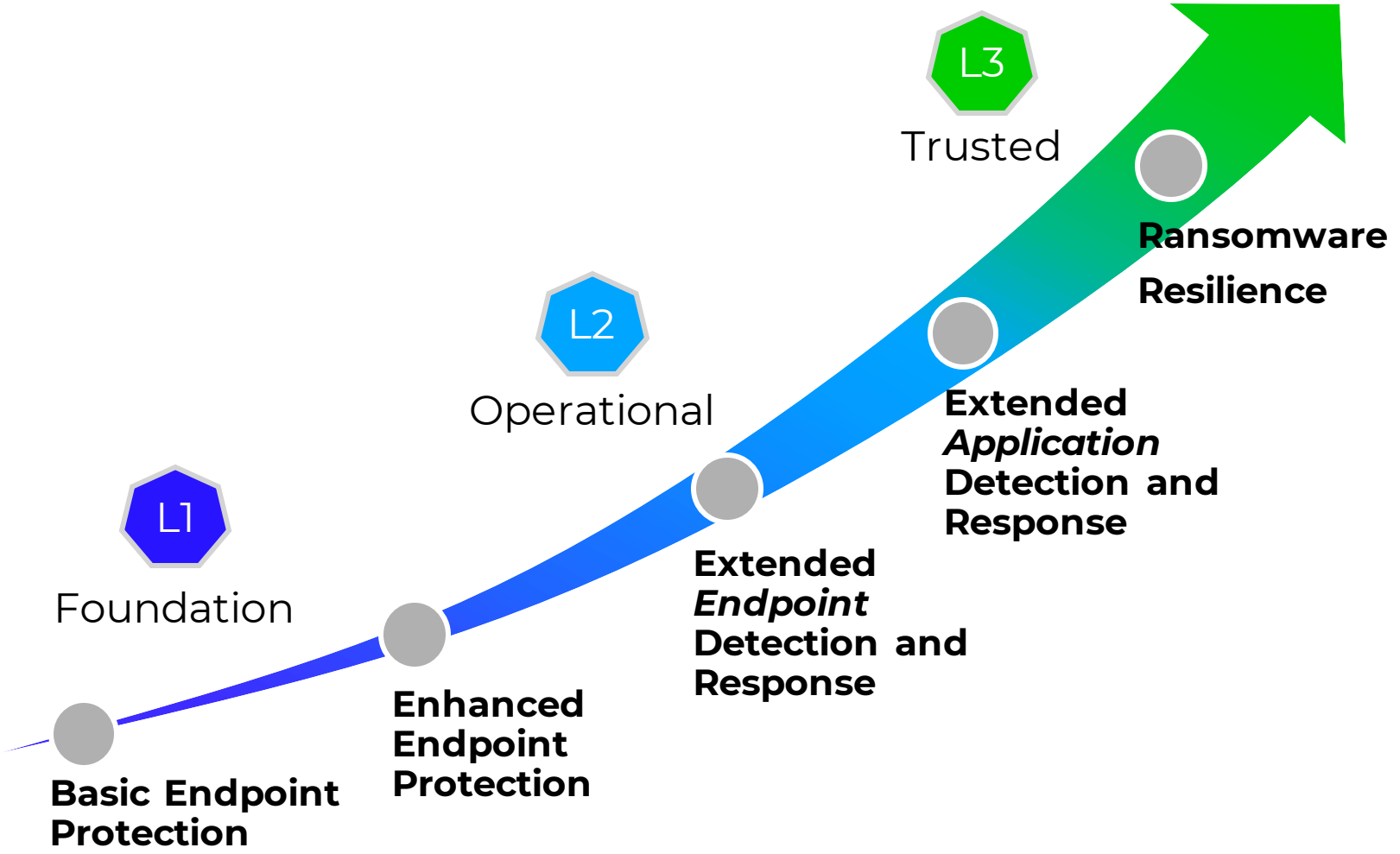
Time: 3:00 PM

Event: Reports of Ransomware Outbreak

The helpdesk and IT department started to receive a high volume of calls and emails about a potential Ransomware attack. The threat actors left a ransom note on each system that was targeted.

Trellix

Ransomware Detection and Response
Customer Outcomes Journey Map



Trellix

Ransomware Solution Reference Architecture

Trellix Endpoint Security

- Proactive Posture Management
- Behavioral Prevention
- Detection and Response Actions
- Rollback Remediation
- Credential Theft Protection
- Forensics
- Hybrid Management

Trellix Collaboration Security

- Malware & Malicious Attachment Protection
- Ransomware Protection
- Business Email Compromise Defense
- Impersonation Attack Protection
- Spear Phishing Defense
- Advanced URL Defense Engine

Trellix Network Security

- Machine Learning and Behavior-based Threat Detection
- Advanced URL & Image Analysis
- Advanced Evasion Technique Detection
- Monitoring, Analysis, & Protection of N/S/E/W
- Industry-Leading Advanced Sandbox

Trellix Data and Cloud Security

- Discovery and Classification
- Endpoint DLP
- Network DLP
- Database Security
- Cloud Posture Assessment
- Cloud Entitlement Management

Trellix Threat Intelligence

- Contextual Intel on Ransomware
- Custom Analysis
- Executive Reporting

Trellix XDR

- Event correlation across all your data sources
- Alert and Risk prioritization
- Threat Intelligence from 1+ billion sensors
- Automated and one-click global responses
- Over 900 native technology integrations
- Pre-built and custom playbooks

Trellix Services

- Emergency Incident Response
- Ransomware Exercises
- Health checks and product optimization

Trellix

Trellix

Thank You!