



WFA: Secured

Endpoint Security that combines next-gen antivirus with elite threat hunting and endpoint detection & response (EDR) capabilities, to eliminate blind spots that traditional prevention would miss.

TENEO
OPENING MINDS

Making the case

Successful endpoint attacks are increasing in today's Work From Anywhere environment, the majority of them being unknown or zero day. In-house IT teams suffering this onslaught are increasingly unable to defend against them for two main reasons: 1) traditional antivirus solutions don't provide adequate protection, and 2) organizations lack sufficient time and resources to minimize IT endpoint risk.

They lack the staff required to monitor, hunt, and investigate the sheer volume of data, or that have the expertise and advanced detection and forensic capabilities, and often the issues are just too complex and costly to manage. This results in blind spots across mobile, physical, and virtual endpoints, alert fatigue, where existing staff are chasing too many false positives, and ultimately, prolonged incident dwell times.

Forward-thinking organizations have found a way to achieve more efficient, effective and affordable endpoint protection. Endpoint services that are built on zero trust are protecting their assets 24x7x365 no matter where users or data reside. The results are reduced telemetry, and reduced time to endpoint attack detection and response.

Our WFA: Secured service provides a single agent that combines next-generation antivirus with elite human and AI threat hunting, and endpoint detection and response (EDR) capabilities to eliminate blind spots that traditional prevention would miss.

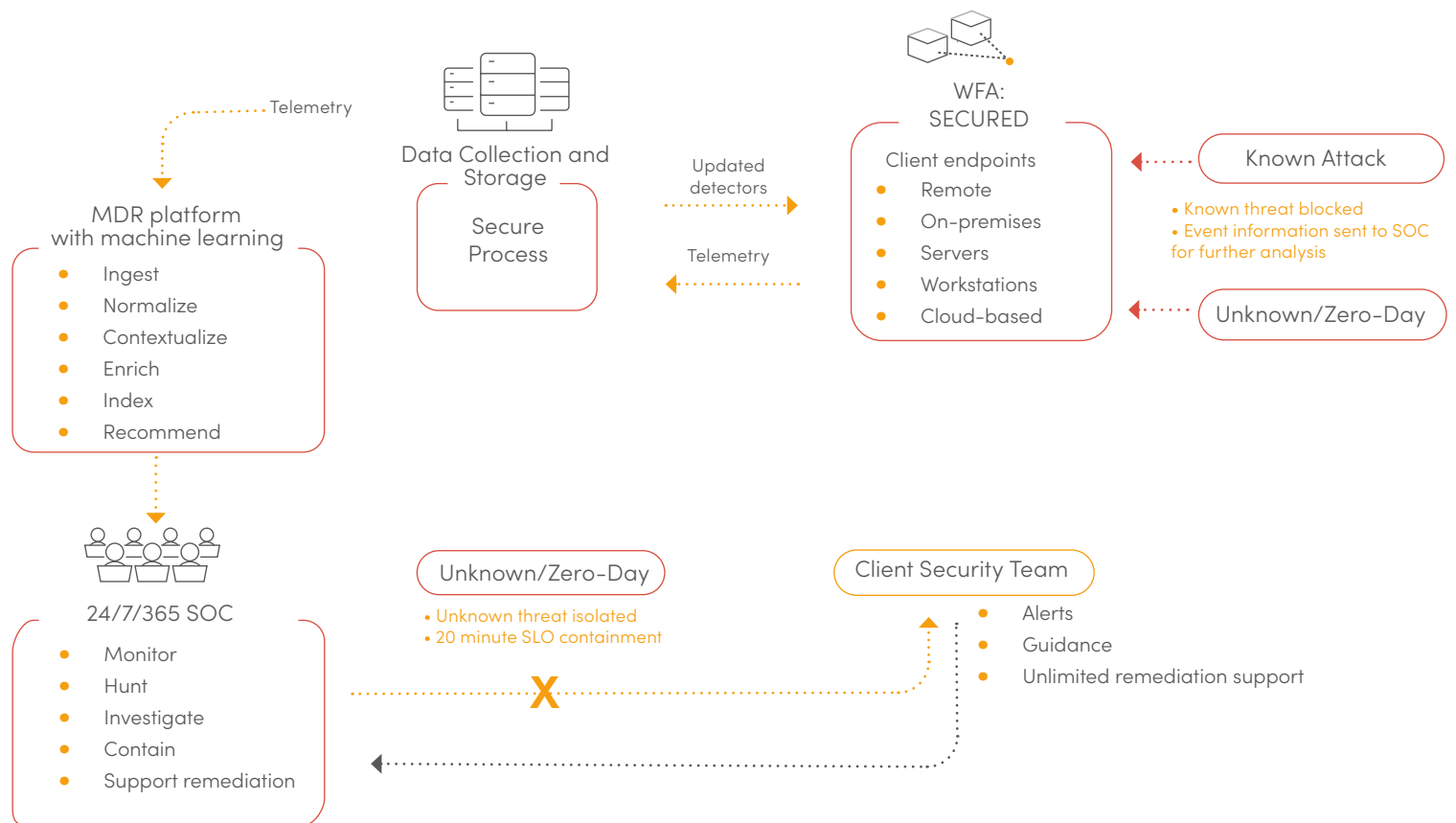
What we detect

- Malware
- Known Attacks
- Suspicious activity
- Lateral movement
- Abnormal behavior
- Fileless Attacks
- Advanced persistent attacks
- Zero-day attacks

Service level summary

✓	Endpoint detection and response
✓	Hands-on expert threat hunters
✓	Automated threat blocking with predictive modeling
✓	Remote managed containment of threat actors
✓	Monthly security insights meeting
✓	24x7 helpdesk

How the service works



Service value

Prevent The Predictable

Identify suspicious behavior using predictive threat modeling to automatically block expected and fileless attacks.

Detect The Elusive

Find threats built to circumvent prevention with a zero-trust approach, leveraging proprietary machine learning and advanced analytics.

Hunt & Isolate Before Disruption

Minimize threat actor dwell time with elite threat hunters that identify, lock down and isolate compromised endpoints on your behalf.

Harden Against Future Attacks

Determine root cause and eradicate threat actor presence across your environment with full incident lifecycle support.



Service outcomes

- Rapid deployment and quick time to value
- Isolation of compromised endpoints, preventing lateral spread
- Optimized and hardened state of endpoint defense
- Reduction in operating expenditure cost and resource demands
- Elimination of physical and virtual endpoint blind spots
- Minimized incident recovery timeframe
- Blocking of known, unknown and fileless attacks
- Improvement in overall security posture
- Detection of elusive attackers and zero-day threats
- Mitigation of potential business disruption
- Satisfaction of compliance requirements

Next steps

Let us help you achieve more efficient, effective and affordable endpoint protection. To find out more, contact us to schedule a meeting at www.teneo.net.

UK
Teneo Ltd
20/21 Theale Lakes
Business Park
Moulden Way Sulhamstead
RG7 4GB

T: +44 118 983 8600
F: +44 118 983 8633

France
Teneo France S.A.S.
71, BD Mission Marchand
92250 La Garenne
Colombes
Paris

T: +33 1 55 51 30 38

USA
Teneo Inc.
44330 Mercure Circle
Suite 260
Dulles
VA 20166

T: +1 703 212 3220
F: +1 703 996 1118

Australia
Teneo Australia Pty Ltd
Level 11, 64 York Street
Sydney
NSW 2000

T: +61 2 8038 5021
F: +61 2 9012 0683