Lumen® Managed Endpoint Detection and Response Service

A holistic real-time endpoint threat detection and response service to help preempt, detect and nullify ransomware and other malware attacks jeopardizing your organizations' cyber landscape and data.

Today's workforce is more mobile, with employees accessing corporate networks through multiple endpoint devices. However, endpoint devices are increasingly susceptible to zero-day exploits, file-less malware, ransomware, and other Advanced Persistent Threats (APT). Furthermore, compromised endpoints act as gateways to high-value organizational assets and information.

Benefits

- Defuse, disarm, and remediate cyber threats like ransomware in real-time
- Plug cybersecurity loopholes by securing endpoint gateways against Advanced Persistent Threats endangering organizational systems and data
- Lumen's 24/7 SOC proactively creates policy-based rules using Advanced Threat Intelligence feeds and Behavioral Analytics engines
- Automated threat remediation to restore impacted endpoints quickly to preinfection states
- Lumen's SOC performs post remediation threat hunting to verify remnants of the attack have been removed from your corporate environment
- Eliminate alert fatigue burdening IT operations

Global ransomware damage costs are predicted to hit $20 billion in 2021, up from $11.5 billion in 2019. Cybersecurity Ventures expects that businesses will fall victim to a ransomware attack every 11 seconds by 2021, up from every 14 seconds in 2019

source: Cybersecurity ventures

ATPs can take on many forms. Browser-based malware and social engineering/phishing attacks are common — both of which are directed at users and their predictable behaviors.

Once an initial foothold has occurred within the corporate environment, the malware often attempts to propagate across the organization, or the attacker uses the compromised device to gain access to company systems and data.

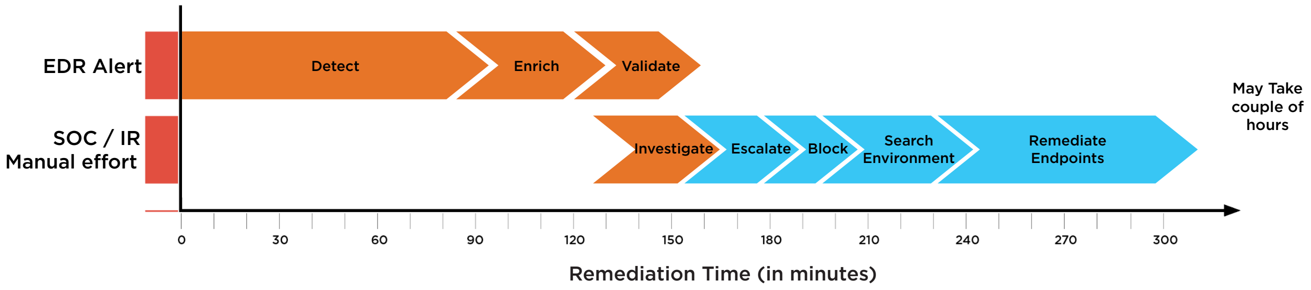
IT Security teams generally do not have the tools to detect, protect or mitigate against these undetected threats, leaving their organizations vulnerable to the devastating consequences of ransomware and other malware attacks.

While organizations may deploy endpoint protection software such as Antivirus, or other types of Endpoint Protection, these solutions often cannot detect and remediate against emerging cybersecurity threats and high-speed attacks.

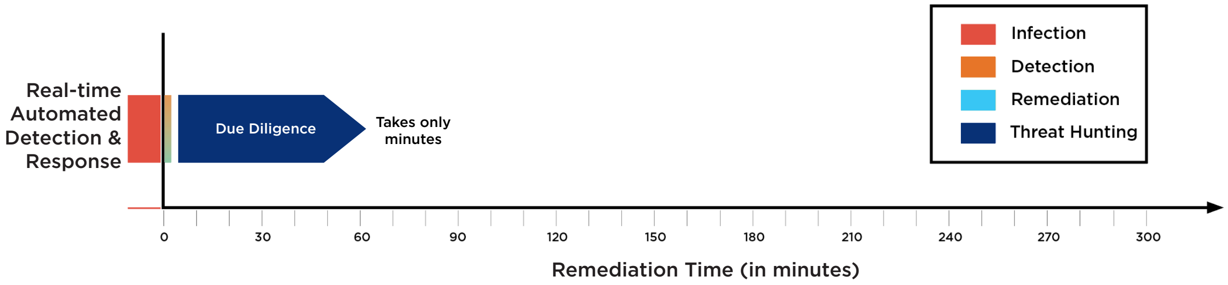
Lumen's Managed Endpoint Detection and Response service provides a layered defense to help mitigate against ransomware, malware and other Advanced Persistent Threats that endanger corporate endpoints.

Using Advanced Threat Intelligence and behavioral analytics, Lumen's 24/7 Security Operations Centre (SOC) enables automated real-time threat detection and remediation of impacted endpoints to pre-infection states.

Traditional EDR setup with Manual SOC efforts for remediation



The Lumen MEDR Service



Technical features and capabilities

- Discover and control rogue devices (e.g., unprotected or unmanaged devices) and IoT devices
- Track malicious and potentially compromise-able applications
- Offline protection to safeguard endpoints in disconnected states
- Access control for USB devices
- Log history analysis
- Contextual-based incident response leveraging incident classification and attack targets (e.g., endpoint groups)
- Preserve memory snapshots of in-memory attacks for memory-based threat hunting
- Conforms to MITRE ATT&CK® framework

Why choose Lumen?

Lumen believes it is essential to see more of the entire network/user activities, to help enterprises stop more cybersecurity attacks, including Advanced Persistent Threats. We have one of the largest and most deeply peered IP backbones in the world, giving us expansive, near-real-time visibility into the threat landscape. Plus, through our continued investment in Black Lotus Labs, we have harnessed the power of our global visibility to disrupt malicious actors. Leveraging Lumen Connected Security solutions eases the burden of having to develop and manage incident response and remediation in-house.

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.