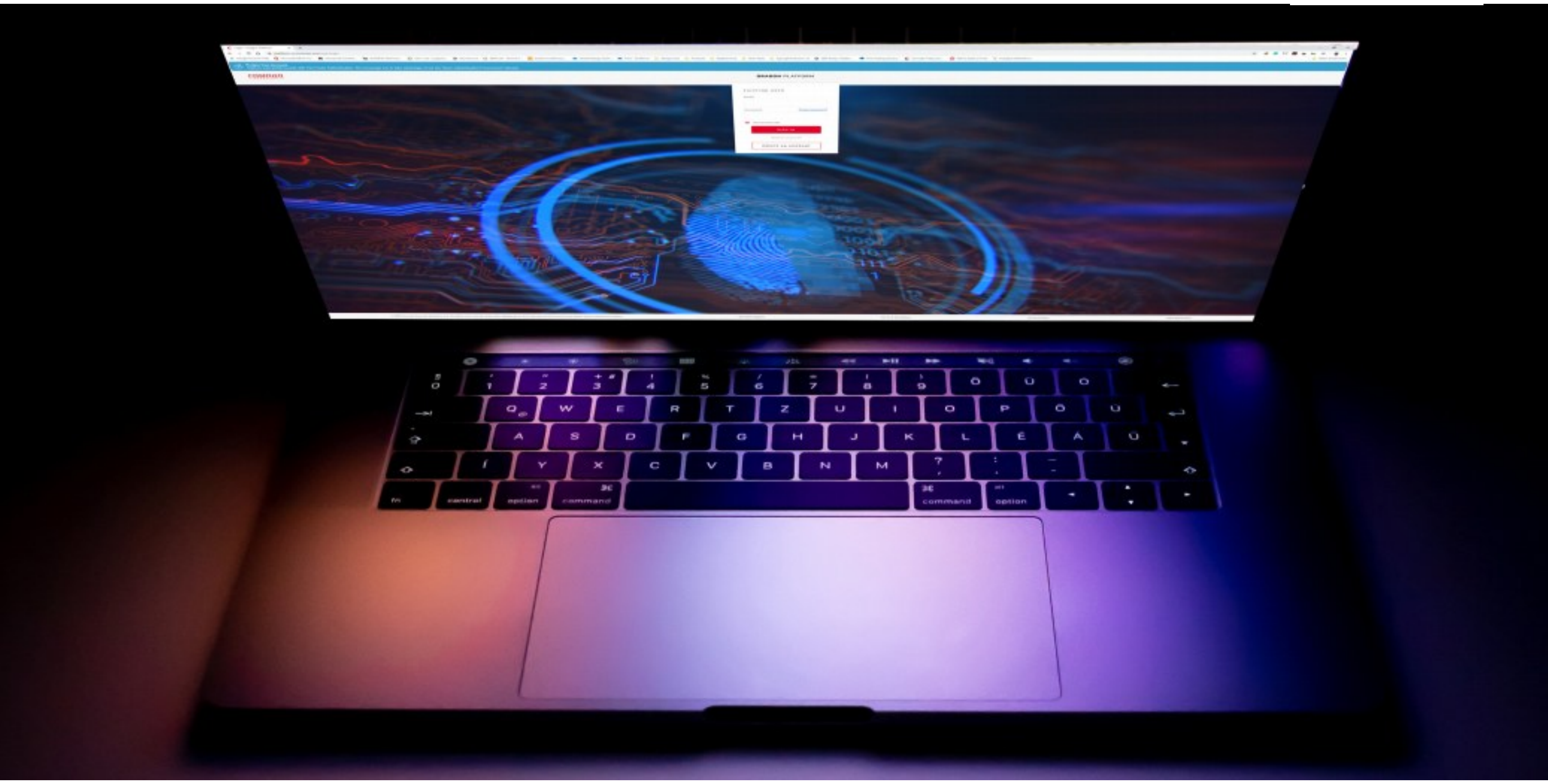
Managed Endpoint Protection



Enterprise Grade Security Against Ransomware, Data Breaches, & Malware

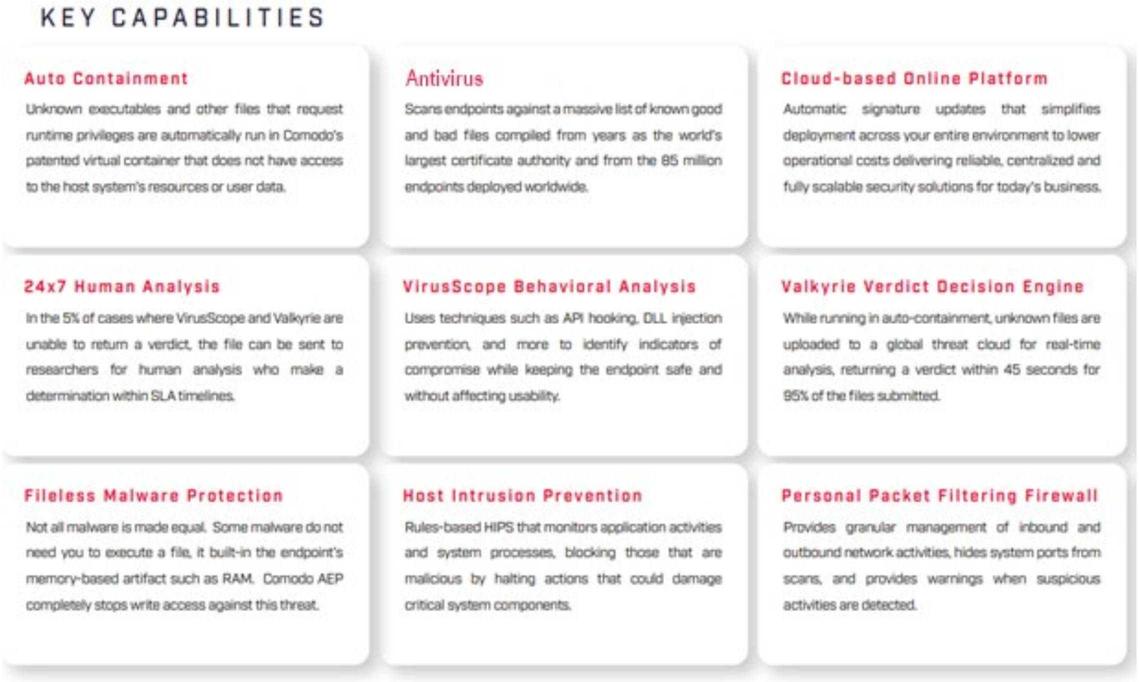
Cybercrime has come a long way from its unsophisticated beginnings as "spray-and-pray" email phishing campaigns against randomly selected targets. Today's sophisticated attackers are after money and power. In 2025, ransomware will attack a business every 10 seconds and damage costs will soar to $20 billion annually. Ransomware in its current state is a nightmare for businesses of all industries and all sizes, who are being successfully breached every day as users click on that one malicious email or URL that slipped through corporate defenses.

Protection for your endpoints starting at $7/month

No business and no user can be considered safe. Having a comprehensive defense-in-depth strategy has never been more critical, and no security posture is complete without technology to protect endpoints. But security controls must not impede employees' ability to do their jobs.

NTELogic has partnered with Xcitium Cybersecurity, one of the oldest and most successful providers of cybersecurity in the world to deliver our Managed Endpoint Protection platform. Utilizing zero trust architecture, Managed Endpoint Protection guards against zero-day threats, known and unknown virus threats, and file-based and fileless malware. Unknown executables and other files that request runtime privileges are automatically run in a virtual container that does not have access to the host system's resources or user data. They run just as well as they would on the host system, making it seamless from the end-user perspective, but they cannot damage or infect the system.

Managed Endpoint Protection



KEY CAPABILITIES

Auto Containment

Unknown executables and other files that request runtime privileges are automatically run in Comodo's patented virtual container that does not have access to the host system's resources or user data.

Antivirus

Scans endpoints against a massive list of known good and bad files compiled from years as the world's largest certificate authority and from the 85 million endpoints deployed worldwide.

Cloud-based Online Platform

Automatic signature updates that simplifies deployment across your entire environment to lower operational costs delivering reliable, centralized and fully scalable security solutions for today's business.

24x7 Human Analysis

In the 5% of cases where VirusScope and Valkyrie are unable to return a verdict, the file can be sent to researchers for human analysis who make a determination within SLA timelines.

VirusScope Behavioral Analysis

Uses techniques such as API hooking, DLL injection prevention, and more to identify indicators of compromise while keeping the endpoint safe and without affecting usability.

Valkyrie Verdict Decision Engine

While running in auto-containment, unknown files are uploaded to a global threat cloud for real-time analysis, returning a verdict within 45 seconds for 95% of the files submitted.

Fileless Malware Protection

Not all malware is made equal. Some malware do not need you to execute a file, it built-in the endpoint's memory-based artifact such as RAM. Comodo AEP completely stops write access against this threat.

Host Intrusion Prevention

Rules-based HIPS that monitors application activities and system processes, blocking those that are malicious by halting actions that could damage critical system components.

Personal Packet Filtering Firewall

Provides granular management of inbound and outbound network activities, hides system ports from scans, and provides warnings when suspicious activities are detected.

Managed Detection and Response

DETECT & FIND

Our Managed Endpoint Protection platform goes beyond traditional endpoint protection by including managed detection and response. Our fully managed security starts with the Xcitium Intrusion Detection System (IDS) via sensors. Security analysts continuously monitor your endpoints and network for malicious activities or policy violations that can lead to intrusions and the attacker's kill-chain.

THREAT HUNTING

Analysts use SEIM and their experience to apply active cyber defense methods. These involve proactively searching client networks to detect threats. Threat hunting does not simply wait for correlation rules to alert. Our proactive threat hunting recognizes that threats can still try to evade in-place security protections.

MANAGED RESPONSE

Managed means maintaining the secure state with the monitoring of endpoints and the collection of logs files. The Response is the alerting and reporting, remediation of events or managing incidents through to resolution, supported with SEIM.

24/7 Security Operations Center

Xcitium security experts search for vulnerabilities, continuously monitor your IT systems for indications of compromise, and contain advanced threats. SOC staff works closely with our team to prioritize and fix security flaws and remediate issues.