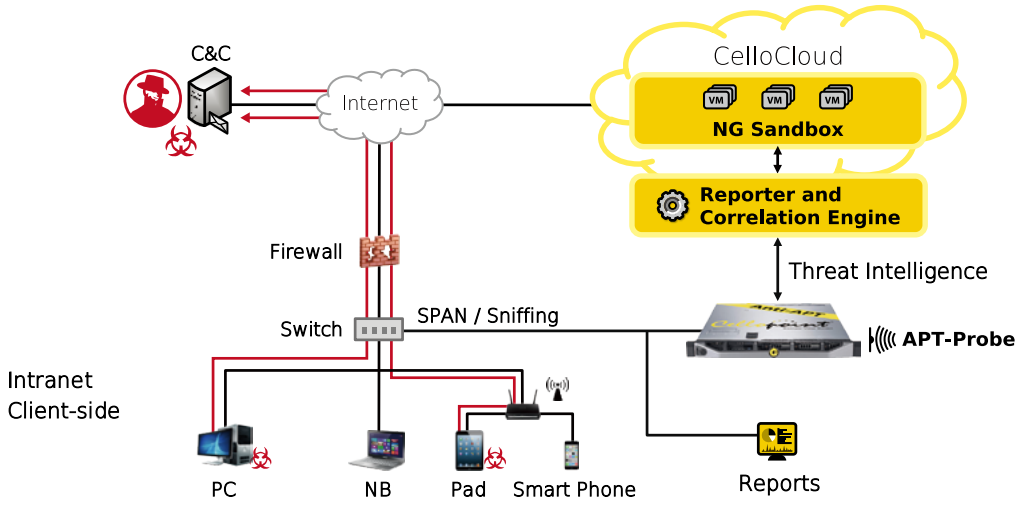
APT-Probe for Malware Protection

APT-Probe is a platform that detects advanced malware and protects your system against Advanced Persistent Threats, Zero Day Attacks, and Evasive Malware. Avoid hackers from getting access to your information and business value and secure your IT infrastructure with the industry-leading malware protection.

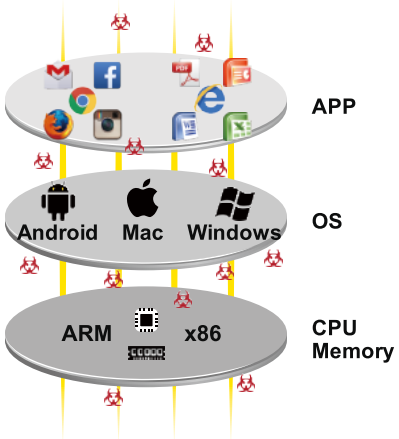


Detect & Stop Advanced Malware

By monitoring network traffic in either sniffing or SPAN/Mirror mode, APT-Probe provides real-time detection and is able to discover C&C servers. CelloCloud updates its Threat Intelligence Database (TID) every 10 to 15 minutes, detecting and stopping malicious IP address, domains, URLs, objects with zero-day exploits, IRC protocol and botnets. All these threats can be blocked using TCP Reset or DNS response format and analyze them using packet sniffers.

Next-Generation Sandbox

The NG Sandbox in the CelloCloud, in collaboration with APT-Probe, provides deep analysis and real-time protection. With high level of visibility into malware behaviors, NG Sandbox can effectively induce threats into an operating system simulation environment, such as x86- and ARM-infrastructure (CPU/Memory/Disk/ Mouse/Keyboard etc.), and software (such as Windows, Android OS, and APK files etc.)



Features

- NG Sandbox with high level of visibility
- Detect threats in x86 server infrastructure and Windows system
- Multi-vectors analyze web and files
- Intuitive threat analysis reports
- Autocorrelation analysis
- Seamless integration with IPS/Firewall/SIEM
- Supports ICAP and proxy server

Cellopoint®
Secure Your Email

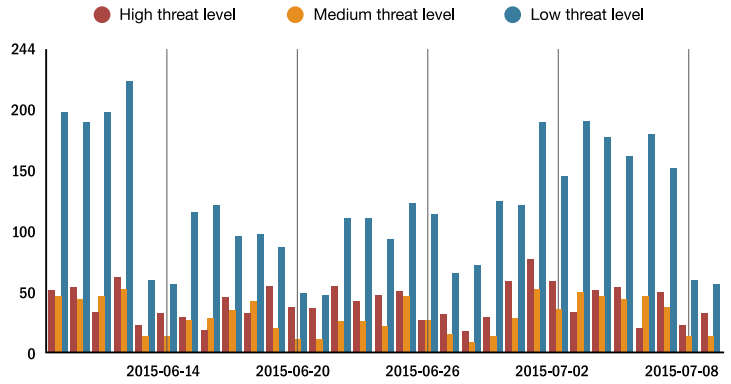
Intelligent Management Center

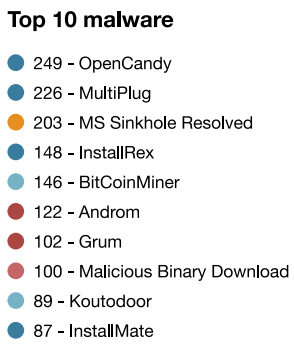
Correlation Engine

The reporter collects all the threats detected by NG-Sandbox, APT-Probe, or TID in CelloCloud. Reporter correlates threat events into incident views to know when to take action. Based on the level, threats are given scores from 0 to 100. The highest are from 100 to 70, those in medium level from 69 to 30 and the less risky get scores under 30. The administrator decides how to respond in a reliable and intuitive way.

Dashboards and Reports

After analysis, APT-Probe generates comprehensive reports. These charts include category of malicious behaviors, screenshots of NG Sandbox in simulation environment, system call and library functions, modified machine code or system files, external connections and other derived sub-programs. The administrator gets firsthand reports about the infection and manages them accordingly.





Specifications

APT-Probe Model	250	500	1000	2500	5000	10000
Business Size	Small	SMB	Midsize	Mid to Large	Large	ISP
Active Users	50~250	250~500	500~1,000	1,000~2,500	2,500 ~ 5K	5K ~ 20K
Performance	20 Mbps	50 Mbps	100 Mbps	250 Mbps	500 Mbps	1000 Mbps
Monitor Port GbE	1	1	2	2	4	4
Deploy Mode	SPAN / Sniffing					
IPv4 / IPv6	Supports both					
Detection files HTTP / FTP	Download as EXE, Android APK, PDF, XPF, DOC, XLS, RTF, DLL, ZIP					
Sandbox Analysis	Exports as PDF, XML, JSON, RTF format					
Management Port GbE	1					
Form Factor	1U Rack-Mount					
Hardware / RAID	Support SAS					
Warranty Updates	1 year					

Cellopoint®
Secure Your Email