MANDIANT®

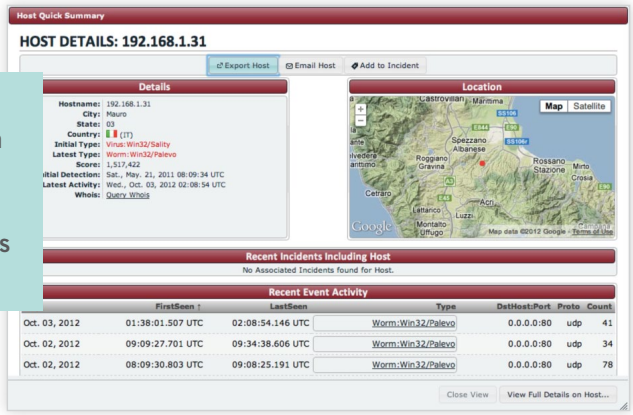
Mandiant Cloud Alert™

Get real-time visibility into malicious communications on your network without installing any hardware or software – and with no false positives.

Millions of computers become unwitting participants in cyber-criminal activities every day. When organizations are compromised, their computing resources can be used to steal login credentials, log keystrokes, steal data, conduct cyber espionage against other organizations, and participate in distributed denial of service (DDoS) attacks or spam campaigns. Mandiant Cloud Alert draws on proprietary intelligence to provide you with a granular view into the state of your network and the context you need to remediate.

Mandiant Cloud Alert Dashboard

Mandiant Cloud Alert provides subscribers with real-time visibility when malicious traffic exits your network and beacons to known bad domains.



PRODUCT OVERVIEW

Mandiant Cloud Alert is a subscription-based service that helps organizations monitor the health of their network by confirming active command and control activity between their network IPs and known nefarious domains.

See Active Compromise on Your Network
View your network's status updated in real-time when one of your monitored IP addresses is attempting to communicate with a known bad domain.

Obtain Context About the Incident
Access specific intelligence on the incident, including the malware used to create the command and control activity, exact timestamps, destination host, and more.

Confirm that Your Preventive Controls are Working
Validate whether your existing security systems and policies are effective.

Monitor How Your Organization Is Trending Over Time
Watch how compromise activity changes over time to understand the impact of new security measures, and how sub-organizations compare.

Track Incidents in Your Network
Assist your remediation efforts by managing and tracking incidents in your network.

HIGHLIGHTS

Mandiant Cloud Alert is the only solution that can effectively evaluate your environment for malicious communications without the need to deploy any hardware or software.

- **Zero False Positives**
  Mandiant Cloud Alert only reports known compromises so you don't spend time investigating false positives.
- **No Appliances or Agents**
  Passive monitoring and reporting requires no hardware, software or agent installation.
- **Find Unknown Malware**
  Mandiant Cloud Alert catches and identifies new samples that your antivirus misses.
- **Actionable Intelligence**
  Detailed information on active compromise provides context for what you're seeing and how to remediate the problem.
- **Tracks More Than Botnets**
  Mandiant Cloud Alert tracks modern malicious networks in addition to traditional botnet activity.

Mandiant Cloud Alert™

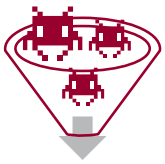
Get real-time visibility into malicious communications on your network without installing any hardware or software – and with no false positives.

HOW IT WORKS

Mandiant Cloud Alert determines if an organization's network is compromised by malicious actors. Mandiant's proprietary cloud intelligence network tracks millions of compromised IPs using thousands of active command and control channels. When Mandiant Cloud Alert detects that your assets are participating in unwanted behavior it provides an early warning so that you can initiate appropriate mitigation activities.

Source & Identify Undetected Malware

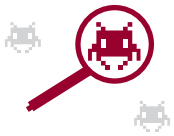
Mandiant gathers and pre-processes large volumes of malware daily, identifying new samples undetected by antivirus.



New Undetected Malware

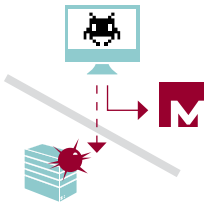
Analyze Malware for New C2 Information

Command and control (C2) information is extracted in Mandiant's proprietary sandbox.



Monitor Command & Control Channels

Strategically selected C2 domains are redirected into Mandiant's monitoring environment.

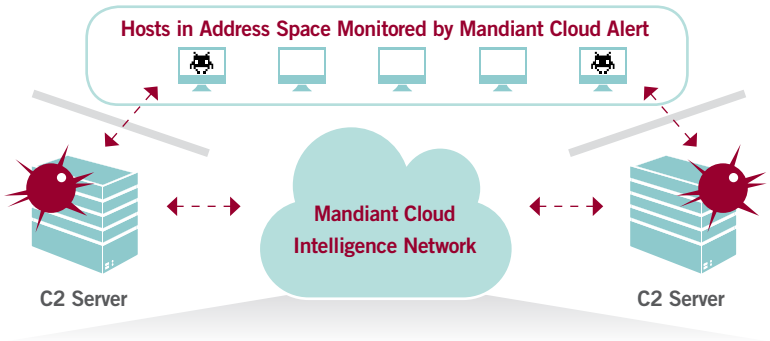


Alert Client to Malicious Communications

Mandiant Cloud Alert provides detailed data and context for each C2 connection originating from your network.

WHAT YOU GET

Mandiant Cloud Alert provides you with the information required to understand the frequency, severity, and context of your network compromise, including:



- Real-time confirmation of malicious activity on your network.
- Identification of malware family associated with the attack.
- Aggregate infection rate across your network.
- Time of command and control communication, including historical data.
- Port and protocol used for communication.

CASE STUDY

Situation: A large global management consultancy suspected they were compromised and required a tool that would provide them the means of conducting network assessments and information to perform remediation.

Action: With Mandiant Cloud Alert, the customer was able to easily identify compromised IPs and conduct successful remediation of the infected systems.

Results:

- Clear intelligence on their global network infrastructure enabled the customer to proactively identify gaps in protection.
- Ongoing analysis and metrics ensured that personnel and assets were directed to the critical issues, mitigating further damage.
- Mandiant was able to provide ongoing intelligence in the form of malware statistics, analysis and trending.

MANDIANT®

Mandiant's products and services protect the world's most valuable data every day from targeted attacks. Our unique combination of intelligence, experience and technology equip organizations to detect, respond and contain attackers before they reach their objective.

TEL +1 (703) 683-3141 TOLL FREE (800) 647-7020 WASHINGTON NEW YORK LOS ANGELES SAN FRANCISCO WWW.MANDIANT.COM