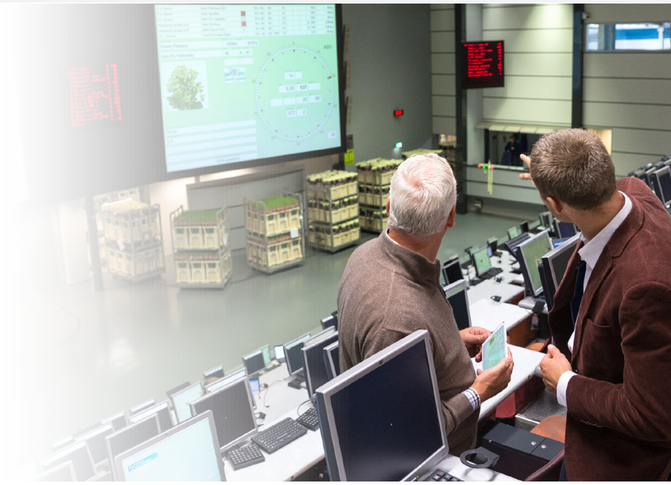
# Cisco Advanced Malware Protection for Meraki MX



## Benefits

- **Gain visibility into threats** inside the network and across multiple branch locations
- **Simplify security management** with a cloud-based network security platform
- **Quickly detect, analyze, and remediate breaches** with deep threat visibility
- **Strengthen network defenses** with global threat intelligence
- **Reduce complexity** by managing security services in the cloud with a single web-based dashboard
- **Reduce costs and save time** with a subscription service that is easy to deploy, easy to manage, and affordable

## Simplified, Cloud-Based Security Management with Advanced Threat Capabilities

Zero-day attacks, advanced persistent threats (APTs), and malware—these are just a few examples of how innovative, persistent, and motivated cybercriminals have become. And as attackers discover new ways to breach your organization, security professionals struggle to deal with those cyber attacks because they lack the visibility, tools, and expertise to coordinate an effective security solution. Attackers take advantage of these gaps in security to evade detection and conceal malicious activity. As attacks become more advanced, so must the security solutions organizations use to protect themselves.

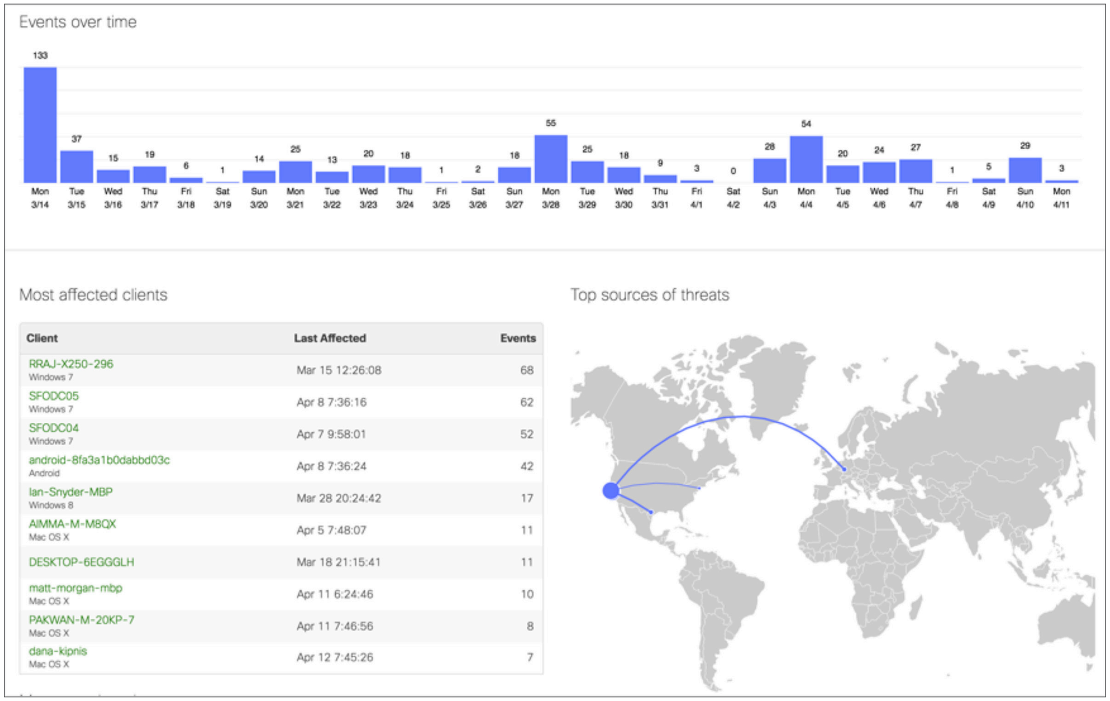
More than ever, organizations need superior visibility, continuous control, and advanced threat protection across their entire network. Cisco® Advanced Malware Protection (AMP) for Meraki MX provides exactly that level of security.

## AMP + Meraki MX: Comprehensive Security

Cisco AMP, together with the Threat Grid for Meraki MX Unified Threat Management (UTM), provides a cloud-based security management platform with advanced threat protection. The solution’s advanced threat capabilities allow organizations to move beyond traditional detection tools and gain visibility into malware threats across all branch locations and remote offices, giving them the ability to quickly detect, contain, and remediate breaches.

## Features

- **Enhanced threat protection:** AMP provides industry-leading threat protection at the network perimeter to help prevent attacks before a breach.
- **Continuous file monitoring:** AMP continues to monitor, analyze, and record file activity to quickly detect malware that evades front-line defenses and to help you scope a compromise and quickly respond.
- **Retrospective alerting:** AMP will notify administrators retroactively of malicious files entering the network, even when those files were not known to be malicious at the time.
- **Advanced malware analysis:** A highly secure environment helps you launch and analyze malware against a large set of behavioral indicators so you can discover previously unknown zero-day threats.
- **Centralized security management:** The solution gives you an all-in-one, cloud-managed network security platform with the ability to manage security, network, and application control across all branches from one central location.
- **Talos threat research:** AMP checks all files entering the network against the global Talos database to determine whether they are malicious.



Events over time

Most affected clients

| Client | Last Affected | Events |
|---|---|---|
| RRAJ-X250-296<br>Windows 7 | Mar 15 12:26:08 | 68 |
| SFODC05<br>Windows 7 | Apr 8 7:36:16 | 62 |
| SFODC04<br>Windows 7 | Apr 7 9:58:01 | 52 |
| android-8fa3a1b0dabbd03c<br>Android | Apr 8 7:36:24 | 42 |
| Ian-Snyder-MBP<br>Windows 8 | Mar 28 20:24:42 | 17 |
| AIMMA-M-M8QX<br>Mac OS X | Apr 5 7:48:07 | 11 |
| DESKTOP-6EGGGLH | Mar 18 21:15:41 | 11 |
| matt-morgan-mbp<br>Mac OS X | Apr 11 6:24:46 | 10 |
| PAKWAN-M-20KP-7<br>Mac OS X | Apr 11 7:46:56 | 8 |
| dana-kipnis<br>Mac OS X | Apr 12 7:45:26 | 7 |

Top sources of threats

Ideal for distributed enterprises and small to medium-sized business, AMP for Meraki provides:

### Deep Visibility into Threats

Today's cyber attacks are stealthy. To protect against them you need solutions that provide visibility into your network's threat landscape, across multiple sites and over time. AMP for Meraki MX goes beyond traditional detection capabilities to capture and analyze file and traffic activity continuously, across your entire network. This gives you increased visibility into what is happening—or has happened—across your network.

### Reduced Time to Detection

Threats can and will get in. When they do, you need to detect them quickly and take action.

With AMP for Meraki, security teams can take advantage of retrospective malware alerts. These alerts will notify customers if a file is found to be malicious after it has already passed through the network perimeter, shortening the time to detection.

## Advanced Sandboxing Capabilities

Threat Grid for the Meraki MX gives you deep visibility into even the most sophisticated malware through advanced sandboxing technology. Security administrators can send unknown files to either a cloud or on-premises sandbox so that the malware can be run safely in a virtual environment and inspected for malicious content. This allows security teams to understand what the malware is doing, what processes it's affecting, and what changes it's making. This capability gives them more accurate, context-rich analytics than ever before.

## Simplified Security Management

The Meraki MX UTM provides an all-in-one, cloud-managed network security platform with the ability to manage security, networking, and application control from one central location. Organizations benefit from the operational efficiency and simplified management of Meraki, while taking advantage of best-in-class threat protection and malware analysis from AMP.

## Next Steps

Talk to a Cisco sales representative or channel partner about how Cisco AMP for Meraki MX can help you defend your organization from advanced cyberattacks.
Learn more at https://meraki.cisco.com/amp.