MANAGED ADVANCED MALWARE PROTECTION SERVICE (MAMPS)

DETECT AND DEFEAT A NEW GENERATION OF LETHAL ZERO-DAY AND APT ATTACKS

Today's hacker is focused on stealing money, intellectual property, identities, state secrets and more. Their weapon of choice is advanced zero-day and APT malware that's often undetectable by signature-based defences. But now there is a way to stop these attacks in their tracks. Managed Advanced Malware Protection Service (mAMPS) is a new, advanced managed security service that protects your organisation through innovative, signature-less detection and prevention.

- Defeat known as well as unknown, zero-day threats with advanced security for today's evolving threat environment
- Achieve greater command and control with outstanding network visibility and the power to set more granular policies
- Deploy protection quickly, easily and more effectively
- Enjoy greater peace of mind through our managed security services featuring on-staff information security experts and powerful predictive analytics

THE BEST DEFENCE IS A GREAT OFFENCE

Our innovative new mAMPs delivers the security intelligence and protection you need. Fully managed and flexible, it allows you to choose between end-point/network-based protection and even a hybrid deployment for maximum protection. Our multi-pronged approach combines adaptive correlation, heuristics-based analytics and advanced malware look-up for detecting even the most well disguised threats.

KEY BENEFITS

- Real-time network visibility—thanks to user-friendly console and customised reports
- Aggressive early detection quarantines resident malware—through recursive, scheduled and on-demand scanning of network files
- Actionable threat intelligence—by observing malware behaviour through real time, virtualised analysis
- Multi-threat detection—our full-featured, dynamic virtual analytics can rapidly identify and protect against blended, advanced attacks
- Proactive threat research—our unique malware intelligence sharing component delivers advanced alerts of emerging threats
- System integration support—fast, trouble-free incorporation of Advanced Persistent Threat components into your network environment
- Reduced Total Cost of Ownership—our Managed Advanced Persistent Threat protection service requires no investment in expensive in-house security staff.

KEY FEATURES

- File reputation—via advanced analytics and collective intelligence
- File analysis and sandboxing—we execute, analyse and test malware behaviour in a secure environment
- Retrospective detection—sounds alerts when file disposition changes after extended analysis
- Compromise detection—correlates and prioritises possible active breaches
- Tracks file trajectory/propagation in your environment—continuously over time
- Outbreak control—quickly takes command of suspicious files or outbreaks
- Virtual analysis—accurately identifies zero-day attacks, creates real-time protections and captures dynamic callback destinations
- Identify and block blended attacks—defend against advanced, blended attacks via Web, spear-phishing emails and zero-day exploits
- Managed AMP support—choose from network AMPS, end point AMPS or combined network and end point AMPS.

Trust us with protecting your network—and safely extend your reach virtually anywhere. As owner/operator of one of the world's largest and most advanced networking and communications infrastructures, our more than 700,000 kilometres of subsea and terrestrial fibre, 400+ PoPs and 44 data centres offer unparalleled worldwide support.

"Modern cybercriminals usually have clear business objectives... They know what information...or what outcomes they want... (and they) spend significant time researching their targets...and planning their objectives strategically."

—CISCO 2014 ANNUAL SECURITY REPORT

"There are two kinds of big companies...those who've been hacked... and those who don't know they've been hacked."

—JAMES COMEY, DIRECTOR OF THE FBI

Companies that deployed security intelligence systems... enjoyed an ROI of 23%.

— PONEMON INSTITUTE

For more information, visit us at www.tatacommunications.com.