NTT Security

Technical Insight

Real-Time Malware Detection

Is your organisation protected against the latest advanced threats?

In today's challenging threat environment, organisations are increasingly recognising that their current defences are no longer able to provide the right levels of visibility and protection for the business. To detect and defend against Advanced Persistent Threats (APTs), designed specifically to evade traditional security controls, businesses need new layers of security that provide real-time detection and mitigation of zero-day attacks.

Dealing with advanced threats does not mean that the basic components of information security can be neglected. Perimeter defences, Intrusion Detection and Intrusion Prevention Systems (IDS/IPS), proxies, Distributed Denial of Service (DDoS) prevention and mitigation and Security Information and Event Management (SIEM), still play an important part in managing information security risk. But the nature of today's advanced attacks means that the level of risk organisations face is growing.

The explosion in mobile working and new channels of communication continue to impact the corporate security model. Without additional defences and the right skills and knowledge specifically focused on malware detection, organisations are leaving themselves evermore exposed to the potential loss of intellectual property, sensitive personal data and the availability of critical services. All of these can result in damage to the brand's reputation and the impact on customer trust and financial health of the business. Rather than purely monitoring technology performance, organisations need measures in place that take human behaviour into account and protect end users as well as the infrastructure. Customers that choose our managed Real-Time Malware Detection service benefit from round-the-clock support from our expert team at a predictable cost. Enhanced insight into the wider threat environment helps contextualise business risk, giving you confidence that your critical assets are protected.

Benefits of the Real-Time Malware Detection Service

Enhance resources and reduce complexity

- Maximise investment in existing sandbox technologies
- Ensure the right skilled resources are available to help protect your business 24/7/365
- Stay up-to-date with threats and vulnerabilities without consuming time and resources
- More effective in-house teams – freedom to focus on rapid response to genuine incidents

Improve quality and productivity

- Spotting the needle in the haystack while minimising false positives
- Damage limitation – early detection and containment of threats reduces the risk to your business
- Continuous monitoring and improvement process maintains alignment with any changes in your business needs or risk appetite
- Greater assurance, increased compliance and renewed confidence in ability to protect critical business assets
- View your business risk in context: access to our global threat intelligence network means you benefit from NTT Group's insight into the wider threat environment and how organisations are responding to attacks

The Real-Time Malware Detection Service

Our Real-Time Malware Detection (RTMD) service combines the best of NTT Security's global managed security capabilities with industry-leading sandbox technologies to detect, analyse and rapidly alert our customers to both known and unknown malicious files traversing their networks. Our customers benefit not only from our technical expertise, but also from our continuous monitoring and improvement process and our global perspective on the latest threats and vulnerabilities. This intelligence enables organisations to consistently act more quickly and effectively to isolate and block attacks and ensure critical assets are protected without impacting the business and consuming valuable internal time and resources.

The challenge: getting insight from information

The information generated by the sandboxing technologies can provide valuable insight into potential attacks and incidents which more traditional technologies often fail to detect. By identifying and extracting previously unseen files traversing the customer network, and then executing these within a virtual environment, the system can safely analyse the way the file behaves, generating a security event if the behaviour is considered malicious.

For end users, the challenge of sandboxing technologies is that they generate larger volumes of reporting information than traditional tools. The data can be difficult and time-consuming to analyse, requiring dedicated, skilled security analysts to provide context and judgement and enable the full value of the technology investment to be realised.

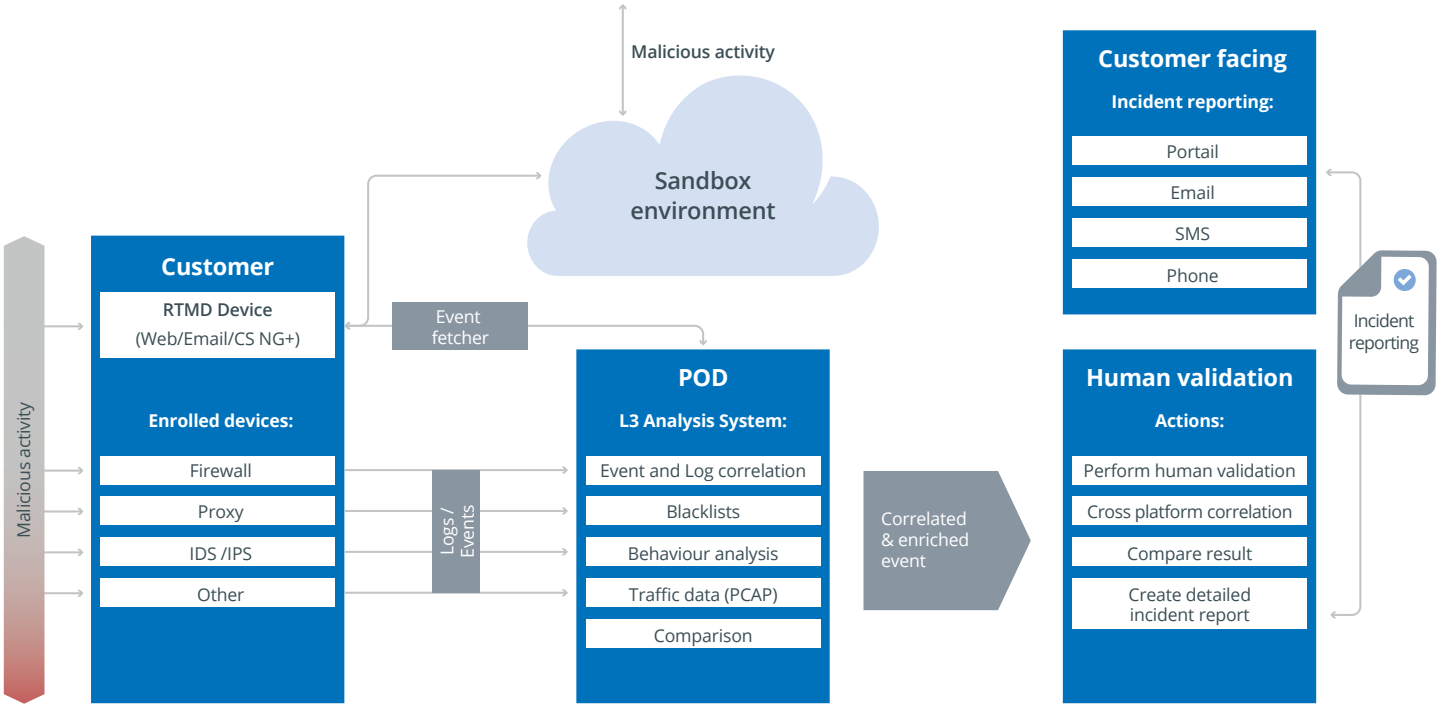
The NTT Security RTMD service addresses this challenge initially by filtering out false positives through advanced automated security event and log correlation rules. Comparison with proprietary NTT Group and third party blacklists, and behavioural analysis including geolocation and domain information, bring context to the process. Remaining events are passed through to the Security Operations Centre (SOC) analysts for further analysis and validation. Finally, detailed incident reports with specific remediation recommendations are created, enabling our customers to focus their energies on genuine incidents, thereby making the best use of limited resources.

Real-Time Malware Detection – the intelligence-led approach

The NTT Security Real-Time Malware Detection (RTMD) service is delivered through a combination of:

- Rapid alerting and 24/7 incident response support
- Round-the-clock telephone and email support and advice
- Clear, pragmatic, actionable incident reports
- A large team of expert, highly-qualified and experienced security analysts
- Industry-leading sandboxing technologies
- Our analysis platform, developed to incorporate NTT Security's experience of monitoring and analysing attacks over the last 20 years
- The NTT Group global threat intelligence network, backed by NTT Communications, and unmatched in the industry

Figure 1: 'Spotting the needle in the haystack' with the RTMD Service



What is included in the RTMD managed service?

- Appliance configuration
- Administration and management of devices
- Global threat enrichment
- 24/7 security event monitoring with advanced correlation and analysis
- 24/7 device availability monitoring
- 24/7 incident reporting

Real-Time Malware Detection – service options

The RTMD service is available to protect both web and email traffic and can be deployed either as a stand-alone service or combined with other next generation firewall services. The following service options are available:

- **RTMD Web/RTMD Email**
  Delivered on dedicated best-of-breed sandbox technology, this option delivers the best possible detection and mitigation of the latest advanced web attacks, threats and trends. These services include options for either NTT Security or customer management of the device.
- **Content Security Next Gen+**
  A more comprehensive service based on next generation firewall technology and its associated sandbox technologies. The full service covers web and email anti-virus protection, URL and application filtering as well as real-time malware detection.

Our customers own the monitoring device and choose whether to locate it on company premises, or at the NTT Security data centre or Security Operations Centre (SOC). Whichever option is taken, you benefit from 24/7 management by our expert team.

NTT Group Security threat intelligence – staying ahead of the threats

The threat landscape is becoming ever more hostile, and threat intelligence needs to draw upon the widest possible range of sources and evolve continually to stay ahead of the game. NTT Group Security threat intelligence, a core component of RTMD, enables our customers to benefit from:

- A large team of research and development staff dedicated exclusively to identifying new threats and continually improving detection logic
- Continual enhancement of the threat intelligence picture by security analysts identifying threats and attacks in other customer environments
- Over 30,000 websites across the world are scanned each day to identify global threat trends
- Constantly updated internal incident databases
- Unpublished blacklists internal to the NTT Group – harder for attackers to detect
- A widespread network of global honeypots, automatically dispersed and configured
- Ability to contribute to and consume vendor-sourced threat intelligence
- Range of global CERT partnerships enabling sharing of newly-discovered vulnerabilities and threats

About NTT Security

NTT Security seamlessly delivers cyber resilience by enabling organisations to build high-performing and effective security and risk management programmes, with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com**

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.