[CASE STUDY]

GREYCORTEX MENDEL

ネットワークの脅威を見逃さない

## DEEP NETWORK VISIBILITY IN ONE SOLUTION

GREYCORTEX's MENDEL is a Network Traffic Analyzer that provides deep network visibility, threat detection, performance monitoring and advanced network traffic analysis for private enterprises, public institutions and other important organizations and industries.

**User's Profile** Hyogo Prefecture

Stretching from the the Seto Inland Sea to the Sea of Japan, Hyogo is a Japanese prefecture blessed with diverse climates and sceneries. From highly internationalized metropolitan areas to rural regions rich in nature, Hyogo is often referred as "A Japan in Miniature" and its strategic position in the Kansai area makes it an important commercial center.
Overseeing the network connecting the prefecture is the System Management Section of the IT Planning Division at the Hyogo Prefecture Government Office, which maintains Hyogo's network, provides for the PC used in the government offices and promotes cybersecurity measures and ICT policies throughout the prefecture.

## DIVERSIFIED CYBER-ATTACKS: A GROWING THREAT

Cyber-attacks targeting specific private companies and public institutions have been increasing significantly in recent years but what is even more concerning is that attacks have also been steadily growing more diversified and specialized. In the past, most cyber-attacks would target large numbers of unspecified victims, whereas recently, targeted threats aiming for money or confidential information are becoming more common.

For example, in the summer of 2018, BEC attacks specifically targeting Japanese companies have been observed for the first time. In the near future, with the development of new technologies, malware that employs artificial intelligence or attacks that exploit vulnerabilities of IoT devices will only escalate. With this rapid specialization of cyber threats, now more than ever it is imperative for Japanese companies to rethink and strengthen their cyber-security strategies.

Kobe Prefecture
Planning Dept.
IT Planning Div.
System Mgt
Section chief
Tsugawa Seiji

Kobe Prefecture
Planning Dept.
IT Planning Div.
System Mgt
Manager
Tanaka Kenichiro

## TRADITIONAL SECURITY SOLUTIONS AT THEIR LIMIT

The most effective approach to contrast these increasingly specialized cyber-threats is a defense in depth strategy. Defense in depth is an approach to cybersecurity in which a series of solutions are layered on different levels (incoming, internal, outgoing traffic) to prevent intrusions to a network. Layering such security solutions does not mean simply deploying them separately on the same network, but to integrate different solutions and manage them to operate synergistically. A layered approach to cybersecurity, if enforced correctly, maximizes the efficiency of each solution: the risk of malware infection decreases effectively, and even when security incidents do occur, they get detected and resolved earlier.

This approach is especially useful for those companies that diversify their security measures depending on subnet or type of device: one all-encompassing security solution cannot fulfill the needs of each different section of the network adequately. Thus, to protect effectively everyday use devices and important operational systems while keeping them separated, a defense in depth strategy that employs complementary security products is, at present, the most effective cybersecurity approach.

"However, even when setting up a defense in depth strategy, there are still many companies that end up not enforcing it correctly. With the rapid increase of cyber threats in recent years, we need a comprehensive security strategy that can provide coverage from multiple angles," Tsugawa explains.

"Companies that adopt a defense in depth security approach tend to assign different managers to each solution, separating the management of endpoint security solutions and network security, for example. As a result, each layer is being managed by

a different staff and often times no one really has a complete picture of what is happening in the network. When analyzing the data obtained from multiple security solutions separately, the risk of overlooking a dangerous threat increases," Tsugawa explains further.

"When deploying a number of different security solutions on the same network, configuration mistakes also become more common. A simple mistake in setting up the network, such as a loop, can create performance issues and even cause the network to shut down. If the person in charge does not have a full picture of the what is going on the network, they will not be able to detect any abnormalities in the PC or the server from which the IP packets are being sent, not to mention isolating the port that caused the loop in the first place. Configuration mistakes like these can be easily spotted and fixed when there is deep visibility of the network," points out Tanaka.

## Expose Every Threat with MENDEL

To maximize the effectiveness of our defense in dept security strategy, at the Hyogo Prefecture Government Office we use GREYCORTEX's cutting edge network traffic analyzer MENDEL. MENDEL uses both machine learning and signatures: it collects traffic data in real time and, by using a combination of algorithms and high-level methods of network behavior analyses, it detects abnormalities on the network.

"GREYCORTEX's MENDEL does not only detect already known malicious codes and traditional cyber-attacks: it also detects the newest types of threats, often overlooked by traditional security solutions. For example, with MENDEL it is possible to detect a malware that has intruded the company network right when it starts spreading through lateral movement and get it marked as abnormal behavior," Tanaka explains.

"That is because MENDEL's detection method is not only based on signatures and deep packet inspection (DPI), it also employs what is called network behavior analysis (NBA). Network behavior analysis differs from traditional signature or rule-based detection methods in how, by using machine learning, it analyzes the behavior of network traffic flows and it compares it to a model of the normal behavior of that network to detect any abnormalities. Network behavior analysis is very useful in detecting zero-day attacks that often get ignored by traditional methods of detection and it does not even need any periodic rule updates. It is by combining all these different detection methods that allows MENDEL to detect threats overlooked by traditional security solutions with high accuracy," Tsugawa concludes.

## Deep Network Visibility with MENDEL

"When it comes to usability, MENDEL's interface was designed to be highly intuitive so that even a beginner could use it effectively. In a few clicks, one can easily navigate through detected security incidents and access highly detailed information on each of them. It is also possible to visualize specific data of every device connected to the network, and even to monitor them without having to register each device beforehand.

Because MENDEL provides deep visibility of the whole network, it is possible to determine if an abnormal behavior has originated from a specific device without having to install anything on any of monitored devices," Tsugawa explains.

"Since all information regarding subnets, devices, services active on each device, their behavior, etc. is visualized, it is possible to use MENDEL not only for threat detection but also for monitoring the network's performance. When abnormalities in performance are detected, like in the case of configuration mistakes (i.e. bottlenecks, loops, etc.), MENDEL promptly sends an alert pinpointing where the problem has originated from. For companies that manage extensive networks, MENDEL is an effective tool for real time network monitoring," Tanaka adds.

Furthermore, MENDEL's deployment process is very simple: only a sensor that collects traffic data, and a collector that analyzes the information collected, are needed. Based on the user's needs, the collector can be either installed on the premise or on the cloud. Deployment itself takes about one hour and it can be done by one person.

"At Hyogo prefecture Government office, we choose the Network Traffic Analyzer MENDEL to strengthen our defense in depth security strategy. By using artificial intelligence and a wide range of network traffic analysis methods, MENDEL detects in real time those threats we cannot detect with other solutions. Furthermore, when considering the current shortage of security resources, MENDEL is also an extremely advantageous security solution for companies that don't have enough security personnel since it can be used effectively even by an unexperienced security manager.
Given its cost-performance ratio, I believe MENDEL is an extremely impressive security solution." Tsugawa highly recommends MENDEL.