White Paper

Transportation Management Company Supports Safer, Faster Supply Chains

Transplace deploys Cisco® Cloud Web Security (CWS) Premium for advanced threat protection, web security, and bandwidth optimization across eight Centers of Excellence throughout North America

EXECUTIVE SUMMARY

Company Name: Transplace

Industry: Transportation

Location: Frisco, Texas; eight Centers of Excellence throughout North America

Employees: 1000+

Name: George Abernathy

Job Title: President and Chief Commercial Officer

Company: Transplace

Name: Scott Engel

Job Title: Director of IT Infrastructure

Company: Transplace

Introduction

Transplace is a premier provider of transportation management services and logistics technology to the manufacturing, automotive, retail, chemical, oil and gas, and consumer packaged-goods industries. In addition to providing transportation management, intermodal, brokerage, and international logistics services, Transplace also offers software-as-a-service (SaaS) transportation management system solutions. Headquartered in the greater Dallas, Texas, area, the company has eight Centers of Excellence throughout North America.

Explaining Transplace's view on customer service, George Abernathy, the company's president and chief commercial officer, says, "If you outsource to us completely, your mindset should be comfort, your mindset should be that your goods are safe and secure and that Transplace is acting on your behalf as you would act yourself."

> A couple of the main differentiators with CWS Premium are the threat intelligence of AMP and CTA as well as the ability to drill into the command and control communications.
>
> — Scott Engel

Challenge:

- Protect against advanced threats
- Simplify deployment and management
- Optimize network performance in branch offices

Solution:

- Cisco Cognitive Threat Analytics (CTA) and Advanced Malware Protection (AMP) to protect against zero-day threats already in the network
- Cloud delivered security with centralized management and reporting capability
- Cloud solution eliminates need to backhaul traffic to headquarters

Business Results:

- Identification of threats, command and control activity, and reduced time to remediation (TTR)
- Reduced support and management time
- Optimized bandwidth utilization and roaming users protected

Challenge

Optimize Network Performance in Branch Offices

With a network that spans the continent and a customer base that includes many of the largest shippers in the world, Engel sums up the challenges faced: "We wanted to have better control over the web policies and security being applied to the machines outside of our perimeter, as well as the ability to protect those machines from some of the advanced malware when these machines are located offsite. "

A highly distributed workforce can produce two challenges:

- Remote users need to be protected. In addition to the eight locations in the United States, Canada, and Mexico, there are also employees remotely based.
- Protecting remote employees cannot come at a cost to performance. Machines outside of the perimeter need to be protected in a way that does not overload the expensive WAN used to connect them.

Protect Against Advanced Threats

To protect its sensitive customer data, Transplace needed a solution with high efficacy and protection. Engel explains, "We were looking for something that was more than just IP reputation; we were looking for advanced threat protection from the next solution."

Simplify Deployment and Management

Transplace needed a solution that would complement its existing focus on Lean Six Sigma in terms of management and deployment.

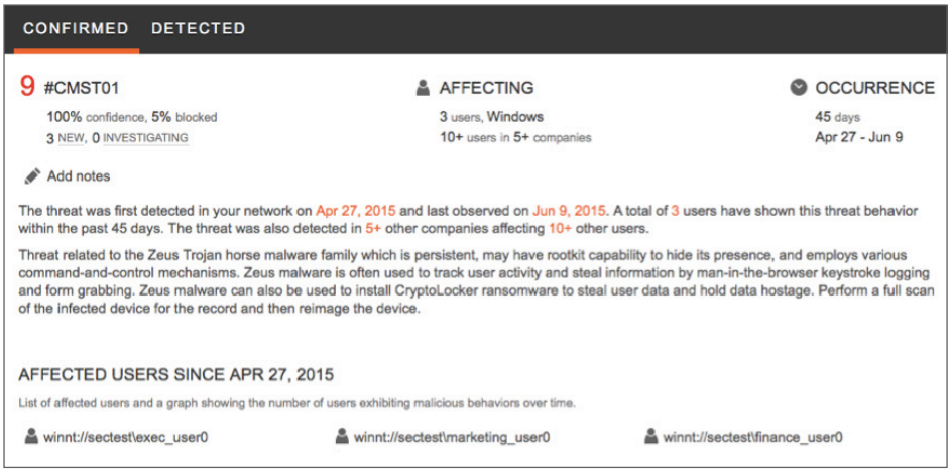
Solution

With CWS Premium, Transplace can identify advanced threats for its remote and branch users, maintain a low level of maintenance and management, and support WAN utilization efforts.

CTA and AMP Defends Against Zero-Day Threats Already in the Network

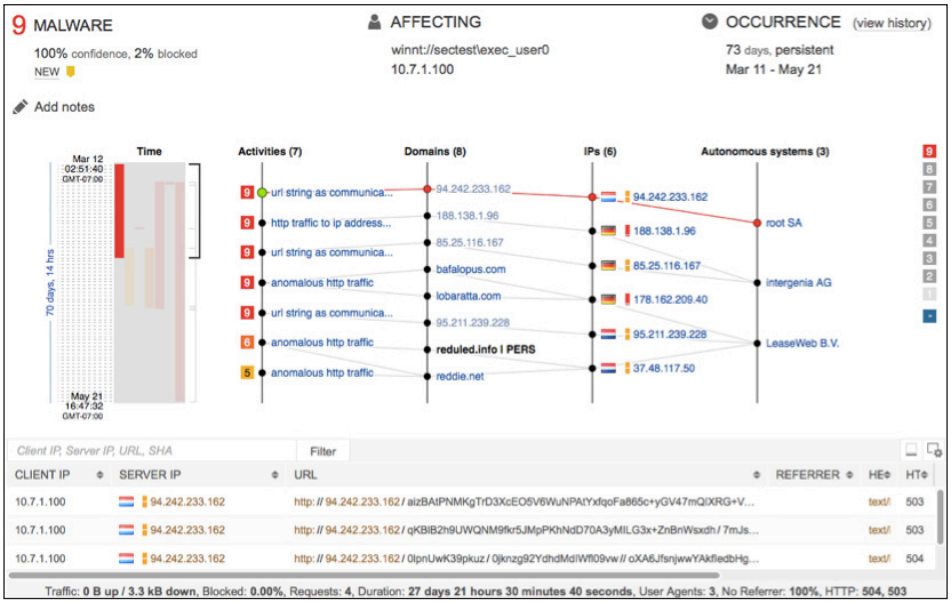
CWS Premium technologies and CTA and AMP work together to protect Transplace from threats that have gotten past other security measures. The technologies give Transplace a threat-level indicator and identification of malicious files, as well as a description of the type of attacks by examining command-and-control traffic. Engel explains, "When CWS detects a threat, it actually gives us a score based on the risk level and the confidence level that the machine is in fact infected." For the command and control activity, "being able to understand how many machines were communicating through that same method helps us understand the level of threat we were dealing with."

Figure 1. Example of Score and List of Affected Users for Identified Threat (Zeus Variant)



> We were getting alerts within CWS Premium that a machine had a high probability of having some form of malware installed. So we tried to remediate and found that our antivirus software wouldn't even start. It would continue to fail to execute.
>
> — Scott Engel

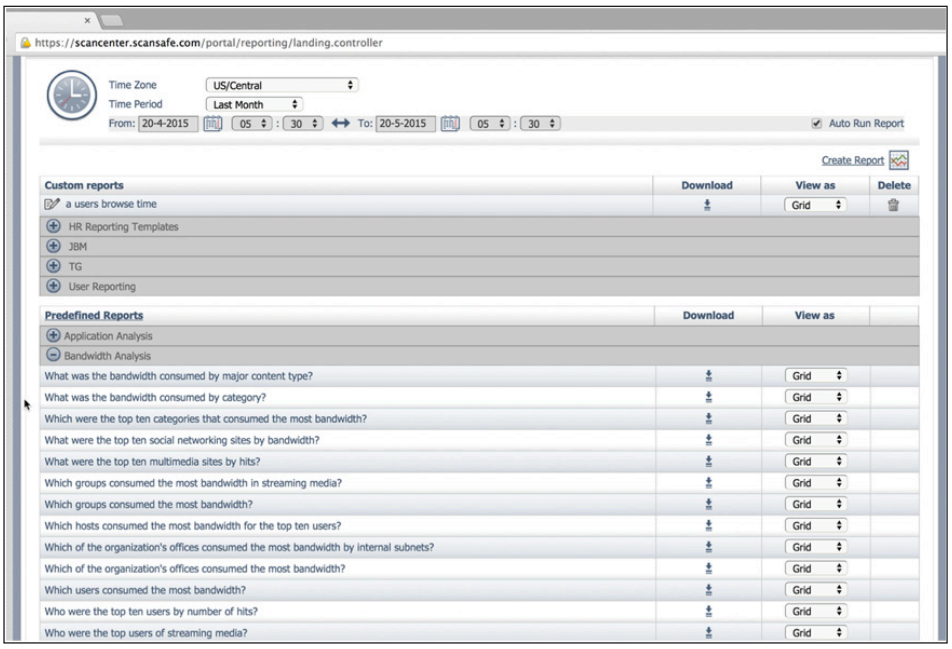
Figure 2. Example: Command-and-Control Activity for One User



Cloud Delivered Security with Centralized Management and Reporting Capability

Another advantage of Cloud Web Security Premium for Transplace is the web-based reporting capabilities. The reporting was needed on the technical team and the Human Resources team to satisfy the need for detailed, technical security reports and also the more basic web usage reports. For example, one of the reports that Transplace uses quite often is the bandwidth utilization report to understand why it might have high utilization on a specific circuit.

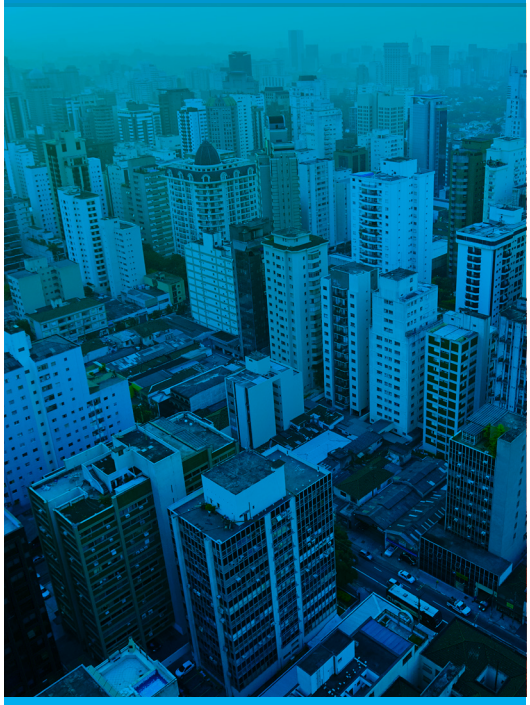
Figure 3. Example: Bandwidth Reports



Security Analysis in the Cloud, Eliminating Need to Backhaul Traffic to Headquarters

Engel states, "One of the requirements was cloud based and that was primarily to protect our offsite assets, as well as to eliminate the need to backhaul that traffic to our central location and through a proxy, so that also provided ease of deployment, ease of configuration with a fully hosted cloud solution."

White Paper



> If you outsource to us completely, your mindset should be comfort, your mindset should be that your goods are safe and secure and that Transplace is acting on your behalf as you would act yourself.
>
> – George Abernathy

Results

Identified Advanced Threats and Command-and-Control Activity and Reduced TTR

Since deploying Cloud Web Security Premium, Engel and his team have identified a Zeus variant, various instances of command-and-control communications back to discovered bad IPs, as well as cases of malware advertising. In the case of the Zeus attack, Engel explains, "We tried to remediate the machine, but our traditional antivirus tools couldn't find anything. When CWS continued to confirm the threat, we reimaged the machine, and we no longer received indications that the machine was still a threat."

Transplace uses Cloud Web Security not only to detect malware and advanced attacks but also to determine a course of action and reduce response time. Engel says, "Because it's able to identify the threat level involved, we don't spend a lot of time trying to run forensics. We simply reimage the machine. So it allows our team to work on the projects that they need to be working on instead of trying to remediate threats."

Reduced Support and Management Time

In terms of reporting, Transplace has gained significant benefits with Cloud Web Security Premium. "One of the efficiencies we have found is that the predefined reports were easy to drill in to using well-known categories that HR may want to be able to see," Engel explains. "Yet we also have the ability to run custom reports that give us more detail around that traffic flow and why bandwidth utilization may be high on a specific network segment."

Optimized Bandwidth Utilization and Roaming Users Protected

From a network utilization perspective, Engel states, "With Cloud Web Security we don't have to backhaul all that traffic into our data center. It can remain offsite, and yet, we still have the capabilities of reporting on that traffic and protecting those assets." Transplace estimates its roaming workforce at about 30 percent. With the cloud solution, Transplace does not have to devote time and resources to updating appliances to support a third of its users or backhauling traffic to protect offsite assets from attacks.

Products and Services

CWS Premium

The CWS Premium License includes CWS Essentials, AMP and CTA.

AMP protects against advanced malware and tracks file disposition over time to see where malicious files travel. CTA scans web traffic for symptoms of infection and addresses threats that bypass perimeter defenses.

For More Information

To find out more about Cisco security solutions, visit http://www.cisco.com/go/cws.

To learn more about CWS, visit Read the CWS Data Sheet.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

C11-734972-01 09/15