CUSTOMER SUCCESS STORY

# Telecom Giant Uses VMware NSX Advanced Threat Analyzer to Protect Against Threats

High availability is essential to the success of telecommunications providers. The growing set of cyberthreats from organized crime and hostile nation-states has put telecommunications providers at continual risk of network downtime or failure. Providers are required to deliver emergency 911 services or face potential investigation and penalties by the Federal Communications Commission (FCC) for any interruption.

Telecommunications networks are high-value targets. Physical infrastructure attacks can enable attackers to commit fraud, access billing systems and divert financial assets. For example, criminals use telecom infrastructure to enable SIM cards for use on their own infrastructure, as well as for enabling traffic in other countries for which compensation is never received by the provider. Cyberthieves can also attack the networks that connect the physical transmission infrastructure and other network devices. The risks include private branch exchange (PBX) hacking, subscription fraud and voice phishing. In short, once an attacker is inside the network, the potential for fraud, financial loss and data theft is almost endless.

To protect its corporate networks, one of the largest U.S. telecommunications carriers had deployed both antivirus and email security appliances. The email and antivirus technologies were not enough to protect its networks and failed with regularity, resulting in increasing penetration of its networks by cyberthreats. At the same time, the growing volume of alert traffic continued to overwhelm its security operations center (SOC) team. The SOC team was spending too much time on threats that were not severe enough to merit attention and not receiving alerts for some truly dangerous threats that were penetrating its defenses.

This telecommunications carrier determined that it urgently needed to find better security controls for the detection of sophisticated network-based threats. It needed technology to better detect and identify sophisticated threats, and provide the latest threat intelligence information on advanced threats that could be integrated with its cyberdefense efforts in real time.

## COMPANY

Operates one of the largest wireless telecommunications networks in the United States, serving millions of customers

## INDUSTRY

Telecommunications

## CHALLENGE

- Existing security solutions failed to identify and stop attacks
- Small security staff was overwhelmed with unresolved investigations and endpoint cleanup and redeployment
- High volume of false positives and extraneous alerts wasted limited staff resources

## VMWARE FOOTPRINT

VMware NSX® Advanced Threat Analyzer™

## RESULTS

- Dramatically reduced the number of successful system compromises
- Decreased the number of investigations launched
- Accelerated threat detection and response

vmware®

## The solution

The telecommunications provider decided to deploy VMware NSX Advanced Threat Analyzer to protect against malicious URLs, binaries and artifacts. The VMware team completely integrated and deployed NSX Advanced Threat Analyzer within an hour. This installation was managed remotely and over the course of a single night.

NSX Advanced Threat Analyzer, powered by machine learning and expert systems, interacts with suspect malware and creates a detailed inventory of every malicious behavior engineered into the code. It delivers the detailed information the organization needs to respond faster to evasive threats. This automated the visualization of the malware, the severity and the type of intrinsic malicious behaviors identified, indications of compromise and their alignment with MITRE ATT&CK, and associated network traffic. This empowered the telecom's analysts to make better and faster decisions, as well as to focus their energy on the most dangerous threats.

"The corporate security team loves NSX Advanced Threat Analyzer because it catches stuff that two of our other security solutions miss. When I was looking for a sandbox utility, I performed a side-by-side comparison between NSX Advanced Threat Analyzer and those other tools. NSX Advanced Threat Analyzer outperformed both of them by a large margin," said a member of the provider's SOC team.

---

"We begin every instance of malware analysis by sending the file to NSX Advanced Threat Analyzer. If we see something interesting, we then dig in as deep as we can."

SOC TEAM MEMBER
TELECOMMUNICATIONS PROVIDER

---

## The results

NSX Advanced Threat Analyzer immediately provided improved detection of network-based threats. As a natural evolution, the telecommunications provider decided to expand its deployment to monitor web traffic. NSX Advanced Threat Analyzer was then able to correlate both the web and network threat data, allowing it to map out the entire attack footprint and improve efficiency. The solution lowered the number of end-user systems infected via email and, most importantly, substantially reduced the amount of time spent by the SOC team on spurious alerts. This enabled the SOC team to focus on the true high-priority alerts. These integrated views of indicators of compromise (IoCs) regularly save hours per day for their incident response team.

"NSX Advanced Threat Analyzer not only detected this new threat, but it also extracted the threat, despite the threat being encrypted. This allowed me to look at the detailed report right away," said a member of the SOC team.

The time saved in incident response had another positive effect: It enabled the security team time to focus on other tasks to improve the organization's digital security posture. For instance, the security team began running a script that uses NSX Advanced Threat Analyzer APIs to distribute IoCs generated from the analysis of email attachments. The team then pushed the IoCs to a threat stream feed designed to associate severity and confidence information with IoCs. Matches with the threat stream feed triggered responses that updated the firewalls in the enterprise network to block these malicious IPs. This highly automated workflow, along with other security-minded processes, helped decrease the number of investigations overall.

"I love the flexibility with integrations of NSX Advanced Threat Analyzer, and the fact that we can use an NSX Advanced Threat Analyzer API to customize our tools on the network. I'm continually impressed by how NSX Advanced Threat Analyzer goes above and beyond other tools in the same area of focus," an SOC team member said.

## Summary

VMware NSX Advanced Threat Analyzer detects the advanced malware that is engineered to defeat advanced or next-generation enterprise security tools, such as traditional sandboxes, firewalls and intrusion prevention. NSX Advanced Threat Analyzer delivers complete visibility into advanced malware, enabling your security team to respond rapidly to malicious activity before it results in a damaging data breach.