
Customer Stories:
AW North Carolina

AT&T Business

# AW North Carolina is driven to malware distraction: AT&T provides the heavy manufacturer with heavy-duty protections

- **Business Needs** - AW North Carolina (AWNC) was in the market for a complete overhaul of its IT infrastructure to be on par with its highly automated production line.
- **Network Solution** - Expanded security solutions protect company digital assets with AT&T multiprotocol label switching (MPLS) between the two AWNC facilities supplies disaster recovery redundancy.
- **Business Value** - Value is not hard to grasp or calculate when a single outage reaching the manufacturing floor can cost AWNC more than a quarter million dollars an hour.
- **Industry Focus** - Automotive systems and parts.
- **Size** - 2,200 employees in two North Carolina facilities.

## AWNC finds the downside of transmissions

In business since 1998, AWNC has grown fast and furious, producing its one millionth Toyota transmission just one-year shy of its first decade in business, and today turning out as many as 700,000 transmissions a year. Headquartered in Durham, North Carolina with a warehouse distribution facility 16 miles away in Creedmoor, AWNC's assembly line operates at maximum capacity around-the-clock, six days a week to keep up with customer demand, shipping automotive components six times per day.

Even a small blip in production can have far-reaching consequences for a business whose products are critical to other busy assembly plants – namely, its customer's. With a perfect record for never missing a customer shipment, AWNC had a culture and a reputation to protect.

## Situation

While the Durham production plant was a marvel of highly automated heavy manufacturing equipment densely fitted onto its one-million square-foot floor, AWNC's IT infrastructure lagged behind in both modernity and functionality. Frequent outages, due to its aging technology, were exacerbated by vulnerabilities to viruses, ransomware and other malware.

John Peterson, general manager of Information Technology for AWNC, led the team that would select the vendor to bring the badly needed IT infrastructure into the future and had short-listed four companies from the original eight under consideration. Before the selection process had been completed, however, an unwanted intruder made itself known: a ransomware attack.

## Solution

In the midst of its department-wide overhaul, a ransomware variant intruded, undetected by the firewall and anti-virus software as it entered into the system. Fortunately, the newly installed firewall did not allow the ransomware locking process to deploy; but the malware did saturate the network, bringing down several key process servers, forcing the company to revert to manual processes to keep orders flowing.

"I have to have something and I have to have something right now," Peterson recalls. "Of all the solutions we had seen and those partners we had the most confidence in, who had the size and scale to do what we knew we needed to do… 'You know what? I'm going to pick the one I'm going to win with.' And I picked AT&T."

AT&T assigned its Incident Response and Forensics team within the first 24 hours of the attack, bringing AWNC's systems back up within 48 hours.

The incident strengthened AWNC's resolve to bring its network security up-to-date as soon as possible, having had near-misses and outages on a nearly monthly basis. "In the summer of 2016, our IT team literally was doing nothing but chasing these attacks, trying to minimize the impact and eradicate them. It was crazy," Peterson says.

## All too common

For an operation as busy as AWNC, one hour of downtime can cost up to $270,000 in potential revenue. If a large percentage of 1,700 people working at any given time are left idle, up to $60,000 in wasted payroll is another unrecoverable expense.

As with many such deployments, the AT&T Cybersecurity Consulting Division started its work with testing and analysis of the AWNC network. The consultants with the AT&T team test a network by trying to breach it. (See sidebar.)

Over just a few weeks, AT&T deployed a number of security solutions designed to help keep AWNC safe. "Having this multilayer, multi-tier approach, which AT&T put into place, has saved us literally from chasing malware from one computer to another just trying to find out where it is," Peterson says. "It just kind of runs away from you and every time you think you caught it, it moves to the next one. That's now stopped."

AWNC was not alone. According to AT&T research conducted in October 2016, 90 percent of companies have experienced a preventable cyberattack.

Just as a vehicle's automatic transmission has extremely complex, precision structures, an AT&T Virtual Private Network (AT&T VPN) provides the transmission mechanism for AWNC digital communications; it also serves as the chassis on which other key components ride. Because the AT&T VPN is private and highly secure, it supplies a protected connection for AWNC employees to transmit data with confidence in the security.

### Testing until it hurts

AT&T Consulting attempts to exploit customer vulnerabilities identified during its testing, once it has obtained permission from the client. Ironically, one vulnerability may uncover still other vulnerabilities to exploit, and AT&T follows this trail to the extent necessary to accomplish the goals of the assessment.

AT&T uses a variety of techniques, depending on the nature of the vulnerabilities. Attackers may exploit a system by using a simple manual request, while others will require specially crafted commands or code.

## Multiple layers of security

AT&T tailors email protection to specific infrastructure and business needs with an AT&T Secure Email Gateway. Just as the AT&T consultants tested the AWNC systems for vulnerabilities, it tries to manipulate its users to uncover weaknesses in the security protocols. (See sidebar next page.) The gateway has the added advantage of requiring no hardware or software to buy, manage, or maintain.

In keeping with its multi-layer approach, AT&T also installed Proofpoint Email Protection to stop malware and non-malware threats such as impostor email (also known as business email compromise, or BEC). Proofpoint provides granular filtering to control bulk "graymail" and other unwanted email.

AT&T linked the Durham and Creedmoor facilities with a multiprotocol label switching (MPLS) network

## Social engineering is anti-social

Social engineering is the practice of obtaining confidential information by the manipulation of legitimate users. AT&T consultants test a customer's security posture and employee adherence to security policies. The assessment provides an objective metric to determine if employees understand and incorporate internal security policies into their daily routine. Social Engineering is not designed to target a specific user, but rather target the corporate culture.

to facilitate redundancy, should a disaster recovery event occur. Now one facility can mimic the other's information technology operations.

"We can push data over to the other location and literally recover within minutes now. Before it took many, many hours – sometimes days – to recover," Peterson says.

## Just in time with the times

AT&T's network-based firewall scans and detects potential threats, and filters out known and suspected attacks in near real-time. AT&T Cloud Web Security Service gateways were added to scan internet traffic for security threats, authenticate users and manage encrypted traffic. Because it is network-based, the AWNC firewall is equal to the ever-changing threats an organization of today faces. Busy organizations that may fail to install patches or upgrades – to their eventual detriment – can operate with confidence, knowing the network is on guard. AT&T Cloud Web Security Service, powered by Blue Coat Systems, helps protect AWNC against viruses and malware and minimizes downtime, while customizing security policies and controls across the network.

"AT&T sees these things happening all over the world and can proactively get these things in place so they're not impacting us," Peterson says. "I wish I could tell you it's getting better; it's actually getting much worse: the number of attacks and the incidence of malware we see is increasing every day. From a manufacturer perspective, we're seeing much more activity than we were a year ago."

The good news, of course, is that the AT&T network and security protections are catching the miscreants. The increased activity Peterson is seeing is via the reports he receives from the AT&T security solutions.

"I've seen a demonstrable difference in the things that are now being caught," Peterson says. It's huge."

## Keeping the wheels turning

With two large plant floors of 1.35 million square feet, AWNC is dependent upon mobility to keep productive. In addition, sales and management teams spend significant time traveling in the U.S., Canada, Mexico and Japan to customer sites. AT&T Enterprise Mobility Management helps the company to manage its more than 450 mobile devices and endpoints to help reduce security risks. Employees have virtually seamless access to their applications without interruption.

The suite of mobile device management (MDM) tools deployed at AWNC includes VMware AirWatch Solutions from AT&T. Working from a single platform,

VMware AirWatch enables AWNC to configure, deploy and manage multiple devices, operating systems, applications, and content from a central console. Most important to addressing security concerns, VMware AirWatch includes an automated compliance engine that allows the company to set and help enforce standards. With its highly efficient integration, VMware AirWatch creates a unified user experience for the entire AWNC team.

## Testing at an accelerated level

AT&T continues to test the network for vulnerabilities, and each successive test escalates the potential pitfalls a network may encounter to make sure they are being addressed.

Peterson welcomes the increasingly rigorous testing: "Then we have very actionable data to bring back to the executive management team to further highlight and enhance our security. AT&T showing us where the holes are and then helping us to fill them. So no, it's not a matter of holding your breath. If you don't do these things, there's holes open in your network that you don't even know were there and it's just a matter of time before somebody else finds that spot."

With AT&T as sentinel, AWNC continues its march into the future. The IT team now has recaptured time it can use to improve company digital assets, such as manufacturing execution systems, enterprise resource planning tools, inventory control software and the like.

So at what cost does peace-of-mind come? "It's $270,000 in revenue an hour. You can talk about cost justification. But until you get to $270,000 an hour … that's what it's worth.