As one of the world’s largest insurance brokerage and consulting firms, USI Insurance Services works with a wide array of businesses and individuals, specializing in the delivery of property and casualty insurance, employee benefits, personal risk, and program and retirement solutions.

USI has been on a dramatic growth trajectory ever since its founding in 1994. In less than 30 years, it has ballooned from 40 employees generating $6.5 million in annual revenue to more than 9,000 associates and more than $2 billion in revenue. “We have experienced hypergrowth,” explains Senior Network Engineer Joe Mogelinski. “I have been with USI for about six years, and the company has doubled in size since I started.”

This hypergrowth has resulted in a corporate wide-area network (WAN) that spans the United States. Mogelinski’s team of three network engineers is responsible for network and security management, with assistance from about 25 regional IT operations professionals. A group of analysts set security policy and monitor security events, “but they are not the ones deploying the technology,” Mogelinski says. “For the three of us to manage networking and security in 182 offices from coast to coast, it is imperative that we minimize complexity.”

**Eye-Opening Deployment of Data Center Firewalls**

As an insurance brokerage and consulting firm, USI handles highly sensitive information, most of which resides in the company’s two data centers. And until recently, all communication to and from the 182 offices was backhauled to the data centers. Thus, the top cybersecurity priority for Mogelinski and his team has long been securing the network edge.

That is why, when the headend firewalls in the data centers needed a refresh a couple of years ago, the team evaluated multiple options to be sure they were using the best possible technology. USI’s security analysts had relied on the FortiSIEM security information and event management solution for several years. Still, most of the company’s networking and security infrastructure—including the data center firewalls—was standardized on another industry leader. USI considered FortiGate Next-Generation Firewalls (NGFWs), the legacy edge-security solution, and another competitor.

“We had a bake-off among the three heavy hitters from the Network Firewall Analyst Report,” Mogelinski says. “We weighed all the pros and cons. A huge negative for the legacy firewalls was that they were very difficult to manage and maintain. As a result of our analysis, we ended up replacing our legacy firewalls with FortiGates, and we introduced FortiManager and FortiAnalyzer to manage them. Once we deployed the Fortinet solutions, we fell in love.”

**CASE STUDY**

**Insurance Broker Ensures WAN Security Plus Higher Performance, Less Downtime, and Streamlined Management**

As one of the world’s largest insurance brokerage and consulting firms, USI Insurance Services works with a wide array of businesses and individuals, specializing in the delivery of property and casualty insurance, employee benefits, personal risk, and program and retirement solutions.

“We had a bake-off among the three heavy hitters from the Network Firewall Analyst Report. We weighed all the pros and cons. We ended up replacing our legacy firewalls with FortiGates, and once we deployed the Fortinet solutions, we fell in love.”

– Joe Mogelinski, Senior Network Engineer, USI Insurance Services

**Details**

**Customer:** USI Insurance Services  
**Industry:** Insurance  
**Headquarters:** Valhalla, New York  
**Number of Secure SD-WAN Locations:** 182

**Business Impact**

- WAN downtime cut in half: From around 40 outages per year to fewer than 20
- Internet connectivity up to 10x faster from office locations
- Network engineering team can focus on more value-added activities due to networking and security solutions’ ease of management
USI engaged FortiCare Professional Services to help with the implementation and to bring Mogelinski and his team up to speed. “We quickly got good at managing them,” he says. “Right away, we were very happy with the firewalls’ ease of management and performance.” They also liked the Fortinet licensing model.

“Fortinet offers the hardware as it is,” Mogelinski says. “You can plug into any of the interfaces and expect to get whatever throughput the datasheet says. Unlike some of Fortinet’s competitors, which require you to buy additional licensing for the firewalls to reach their full capability, you do not have to have a second tier of licensing to reach the FortiGates’ published speeds.”

All in all, this first experience with FortiGates “opened our eyes,” Mogelinski adds. “We said, ‘If we are getting this much out of these devices, in this segment of the network, what happens if we add Fortinet solutions in other places?’”

**Nationwide Rip and Replace**

A couple of years later, Mogelinski had the chance to answer that question, as the firewalls and software-defined WAN (SD-WAN) throughout USI’s many offices needed a refresh. The complexity of the legacy infrastructure put a perpetual strain on the network engineering group. They liked the idea of consolidating SD-WAN networking and security in a single device at each location.

Plus, Mogelinski asserts: “We already knew how well the FortiGates were securing the headends. We implicitly trusted that technology to protect our offices as well. We were somewhat invested in the legacy product, but we decided to switch to Fortinet and start fresh. We did a proof of concept for Fortinet Secure SD-WAN, and everybody at USI agreed that transitioning the entire WAN infrastructure to FortiGates was a no-brainer.”

The rollout itself proved the wisdom of that decision. USI standardized on a single firewall model with a cable modem and multiprotocol label switching (MPLS) connectivity. Mogelinski and his team built a tool to customize the firewalls’ configuration. “Once we finished our proof of concept, we had a ‘golden template,’” he says. “We used the configuration generator tool to plug in variables that differed from site to site, like IP address. Then the tool would generate a configuration for the firewall in the form of two files that we saved to a USB drive.”

USI engaged a Fortinet technical account manager (TAM) for a year to support the rollout. “He hopped in right away and reviewed our SD-WAN design and configurations,” Mogelinski says. “Within an hour, he was rattling off best practices that we had not included in the plan. He quickly became like part of our team. In fact, he was so helpful that we just renewed the TAM agreement for five more years.”

Once deployment got underway, the SD-WAN project proceeded very quickly. When a firewall arrived at a USI office, an operations staff member would fly or drive there with the appropriate USB stick. “They would plug the USB stick into the new firewall, power it on, and in less than 10 minutes, the FortiGate was functional,” Mogelinski says. “The on-site folks would log off. The operations team member would literally move three cables from the old firewall to the FortiGate, and that was it. The process was seamless, and the downtime was well under five minutes per site.”

Within two months, all the company’s sites had been converted to FortiGate. “It is incredible, when you pick the right technology, how quickly and easily you can make it work,” Mogelinski adds.
CASE STUDY | Insurance Broker Ensures WAN Security Plus Higher Performance, Less Downtime, and Streamlined Management

Securing Direct-to-Internet Connections

Every office has one SD-WAN tunnel to each of the company’s two data centers via the cable modem, and one tunnel to each data center via MPLS, for a total of four exit points from each office to the WAN. This redundancy reduced downtime from an average of around 40 outages per year in the past to fewer than 20 this year. “We have effectively cut our outages in half,” Mogelinski says. “The proof is in the pudding that Fortinet Secure SD-WAN does what it is supposed to do.”

At the same time, USI introduced direct-to-internet connectivity with the FortiGates to accelerate performance of applications such as cloud-based videoconferencing. “To achieve secure, direct-to-internet connectivity, the other vendors we considered would have required us to put a proxy in front of each firewall,” Mogelinski says. “We would have ended up managing multiple devices in each office. Fortinet stood out because it is a security company: The SD-WAN is both the router and the firewall.”

This new approach dramatically accelerated internet connectivity from USI’s office locations. Mogelinski’s team ran before-and-after speed tests, which demonstrated that internet applications and resources are up to 10 times faster. No longer backhauling internet traffic to the data centers does raise the potential for new attack vectors. Still, Mogelinski has a high degree of confidence in the security of the branch firewalls, which are supported by the FortiGuard artificial intelligence (AI)-powered Security Services Enterprise Bundle. “We have antivirus and outbreak prevention, intrusion prevention, and anti-malware capabilities,” he says. “Even with the direct-to-internet connections, our traffic is more secure.”

Much Easier to Manage at 40% Lower Cost

Perhaps most important for the lean network engineering team, management of the dispersed infrastructure is streamlined. They use FortiManager for large-scale firewall updates and FortiAnalyzer to investigate security events. Mogelinski says the resulting time savings are “huge.” “With FortiManager, we can centrally manage our firewalls,” he explains. “If our security analysts come to us and say, ‘We need you to change this rule on all the office firewalls to prevent users from doing XYZ,’ we can accommodate that request in 60 seconds with a FortiManager push.”

By contrast, with USI’s legacy WAN, “We would have to manage each rule change on a per-site basis,” he says. “We would either need to push the change to each firewall one at a time or write a custom script. Nobody here has the time to log in to 182 devices individually to make a simple change, so we generally relied on homegrown scripting. That meant a rule change we can now push in 60 seconds might have taken us hours in the old environment.”

And if a security incident should occur, Mogelinski and his team can use FortiAnalyzer to understand what happened. Supported by FortiGuard Labs threat intelligence, FortiAnalyzer consolidates logs from all USI’s firewalls. “Now that we have introduced direct internet access, we need to monitor device behavior more closely,” Mogelinski says. “If there is an issue or we have concerns, we can easily see everything that a particular device has done within a time interval we dictate. We can see what traffic was permitted, what was denied, and why.”

The staff time savings of the Fortinet infrastructure are complemented by its drastic cost savings. “From a support perspective, we are achieving around $1 million a year in savings, which is a 30% to 40% decrease in costs,” Mogelinski says. “And the Fortinet hardware was 40% cheaper than our legacy firewalls right out of the gate.”

Now, USI is in the process of deploying FortiSwitch network switches in each office and is evaluating both FortiNAC network access control and FortiAP access points. Mogelinski expects that expanding Fortinet’s presence in the USI infrastructure will enhance the benefits they have already achieved. “We want to standardize as much as possible,” he concludes. “When you deploy FortiSwitches behind a FortiGate, for example, you can tie them into the Fortinet Security Fabric. Ultimately, Fortinet provides an end-to-end security posture that can recognize indicators of compromise and then prevent attacks.”