CASE STUDY

How Portland, Oregon, Secures Innovative Community Services

Portland, Oregon, is known for its temperate climate, its West Coast lifestyle, and its progressive government. Among the top 30 U.S. cities in terms of size, Portland has long prioritized transparency and information sharing.

To that end, the city government is pioneering a number of leading-edge data management initiatives that are designed to improve its many services for the community. One such program is Smart City PDX, a best-practice framework for data governance projects that emphasizes "equity priorities and privacy principles." Smart City PDX includes open-data big data initiatives such as the Portland Urban Data Lake (PUDL), which brings together information on traffic, transit, utilities, and other aspects of citizen activities to serve as a foundation for data-driven decision making by agencies and entities throughout the region.

"Portland is stretching to be a leader in full transparency with our very large datasets," says Christopher Paidhrin, senior information security officer for the City of Portland. "At the same time, it is vital to keep some elements of those datasets private." Innovation in data sharing is possible only if city leaders and the community have confidence in Portland's cybersecurity posture. That is where Paidhrin comes in.

His information security team is responsible for technology governance, risk, and compliance (GRC) across all the city's divisions and offices. Paidhrin's team sets citywide security standards, monitors cybersecurity risks, keeps city leaders apprised of Portland's security strengths and weaknesses, educates the city's approximately 6,000 employees on cyber hazards, and completes the city's annual cybersecurity review.

"Ultimately, my job is to make sure Portland's technology resources and assets are protected and available," Paidhrin says. "It is a challenging job. My team evaluates no fewer than 30 projects in progress at any time that have a component of cybersecurity, to align with the city's security posture."

Two Years of Due Diligence Reveal Fortinet as the Best Partner

A few years ago, one high-priority project for Paidhrin and his team was to find a new firewall security vendor. The firewall brand that Portland had been using for years had fallen behind the competition technologically. Some of the city's firewalls were reaching end-of-life, and the vendor's extended support was inadequate. "There were some support tickets they were simply not willing to fix," Paidhrin says.

Portland launched a procurement process to find a new firewall vendor. Front and center in the decision was ensuring that the solution of choice would effectively protect the city from cyberattacks, such as distributed denial-of-service (DDoS) attacks, as well as provide next-generation firewall capabilities. Due diligence entailed two years of comprehensive research.

"The fewer devices and vendors you use, the fewer passes through the stack where packets could get sidelined. That is why we are all-in with Fortinet."

– Christopher Paidhrin, Senior Information Security Officer, City of Portland

Details

Customer: City of Portland, Oregon

Industry: Government

Location: Portland, Oregon

Business Impact

- Avoids service disruption with effective and timely protection against ongoing DDoS and other cyberattacks
- Builds confidence among city leaders that innovative city solutions and services remain secure
- Built a zero-trust network framework that manages users to application controls for better governance and control

"Being a public entity, we have a pretty complex rationale for procurement decisions," Paidhrin says. Along with obvious decision factors such as technical capabilities and price, Portland considers 'soft' criteria like how a vendor treats employees; whether it gives back to the community; and how it addresses diversity, equity, and inclusion issues. Paidhrin's team scrutinized all these factors, as well as each vendor's product roadmap.

"Given the cost and pain of moving from one platform to another, we look at relationships with security vendors as long-term, strategic partnerships," he says. "We explored the market and talked with analysts, and we did a deep dive into migration tools. We based our shortlist on a balance of each vendor's long-term financial stability versus growth and market share, along with the pure technological capabilities of each package. When we had narrowed the list of candidates to Fortinet and one other vendor, we brought the finalists' equipment in for three months of real-world benchmarking."

In that testing, he says, "we saw demonstrable throughput value in the FortiGate appliances. We also saw that, for our business use cases, Fortinet's major competitor would be more costly, more complicated, and less aligned to the city's objectives. After two years of research, we decided that Fortinet would be the best partner for the City of Portland and provide the best alignment for the city's next generation of services for our community."

Effective Protection at the Network Edge

Once the decision was made, IT teams began replacing legacy firewalls with FortiGate Next-Generation Firewalls (NGFWs). The onset of the COVID-19 pandemic slowed deployment, but the FortiGate implementation continues today.

"Our edge firewalls—so, those with the highest-risk traffic—have all been migrated," Paidhrin says. "It took us a while to get fully staffed to execute on our migration plan. That was partly because of COVID and partly because we had not fully accounted for some of the higher-level security requirements. The city uses more than 2,000 applications, 600 virtual servers, and hundreds of interfaces and DMZs [demilitarized zones], so the migration has been a major lift. That said, it has gone well. We have been very impressed with Fortinet's migration tools and tech support teams." The city is now transitioning to FortiGates for all its internal network segments. "Traffic in and out of DMZ networks must traverse a firewall in both directions," Paidhrin adds.

He reports that city staff have been impressed with the functionality of the new firewalls. Most of the FortiGates' rules have multiple unified threat management (UTM) features turned on, including intrusion prevention system (IPS) inspections, content filtering, web filtering, and antivirus protection. All these features are updated on zero-day threats by AI/ML-powered FortiGuard Services. These capabilities make it much easier for city staff to respond to DDoS attempts.

Business Impact (contd.)

- Simplifies operations by automating and avoiding manual configurations
- Reduces latency for staff access to cloud-based solutions, and for community access to city resources

Solutions

- FortiGate Next-Generation Firewall
- FortiManager
- FortiAnalyzer
- FortiClient
- FortiAuthenticator

"We saw demonstrable throughput value in the FortiGate appliances. After two years of research, we decided that Fortinet would be the best partner for the City of Portland and provide the best alignment for the city's next generation of services to our community."

– Christopher Paidhrin, Senior Information Security Officer, City of Portland

"Bad actors are constantly attempting to flood our environment with attacks," Paidhrin says. "We have upstream protections through our ISPs, but there have been occasions where we have needed to quickly tune our firewalls because traffic got past the protections of our ISPs. Because we had FortiGates in place, we were able to respond in a timely manner. We knew what we needed to do, and we were able to do it very quickly, thanks to Fortinet."

Turning on new features, and migrating from stand-alone security appliances, has been remarkably efficient. The city previously used a stand-alone web content filtering solution. "In a matter of days, we migrated off the old solution and turned on the features within the FortiGates. The IT team did not receive one related trouble ticket during or after the migration," Paidhrin says.

FortiManager and FortiAnalyzer—which are known collectively as the Fortinet Fabric Management Center—have streamlined management of the firewalls, which are dispersed among many different city bureaus. "The Fabric Management Center is an easy-to-use platform," Paidhrin says. "The tools provide information about firewall activities, which we can use to streamline management and governance of them."

Moving Toward Zero Trust

The city's ultimate goal, according to Paidhrin, is to build a zero-trust network architecture (ZTNA), in which all network activities and resources are allowed or allocated based on the identity of the user requesting them. Most of the Portland infrastructure is in early stages of the journey to ZTNA, but the city's Revenue Division is pioneering a Fortinet-based approach where FortiGate offers the natively integrated ZTNA enforcement to city's 2,000 applications.

"We want to move toward identity-oriented security," Paidhrin says, "because our users today may be accessing resources from a secure device, from a personal device, or even from an unsafe location. We need to be aligning security decisions about whether individuals have the appropriate rights to access information related to their role and not only when they are within the city network or using a city-managed endpoint. Identity access management is at the core of that access model."

Portland's Revenue Division rolled out the FortiClient endpoint protection solution with the specific goal of supporting identity management. When a Revenue Division employee logs onto the network, the FortiClient SSO Mobility Agent automatically provides their username and IP address to FortiAuthenticator, then updates that data anytime the IP address changes. By ensuring that FortiAuthenticator always has the current IP address associated with each employee, FortiClient enables the Revenue Division's cybersecurity team to implement and manage identity-based security policies. Only users with explicit permission to do so can access the division's sensitive data.

This capability has worked without a hitch. "In the many months that the service has been up and running, we have had one service ticket," Paidhrin says. "Even that was not Fortinet's fault; it was related to a configuration issue on an endpoint. Our Revenue Division's IT team is thrilled that user identity management is so seamless."

Portland is now in the process of deciding when to extend these capabilities to the rest of the city. "We're prioritizing our next steps along the path to zero trust that creates secure yet transparent access to city resources for our end users," Paidhrin says. From his perspective, the Fortinet approach makes sense: "The ongoing cost for features and capabilities is excellent with FortiClient, compared with the piecemeal charge, per seat and per feature, from some Fortinet competitors," he says.

Paidhrin sees Fortinet playing a central role in the city's security framework going forward. "Our intent is that the Fortinet platform will be the center of all our cyber and information security services," he says. "When we look to a third party to provide any other service, the first question will be: Does it supplement our Fortinet ecosystem? If not, there will be a higher threshold for selecting that tool versus using a capability offered by Fortinet."

Rather than worrying about putting all the city's security eggs in one basket, "I see GRC and security benefits in consolidating capabilities with one vendor," Paidhrin adds. "That reduces the panes of glass that auditors and security operations teams need to look through and improves our visibility into our security posture and the efficient management of our environment. When faced with a potential cyber threat, time to detect and respond is critical. Consolidated security capabilities on the FortiGates greatly reduces incident response times to address cyber threats.

"My argument has always been: The fewer devices and vendors you use, the fewer passes through the stack where packets could get sidelined or take extra time to investigate," he concludes. "It is desirable to have a cleaner transit for our data, from both a GRC and a security perspective. That is why we are all-in with Fortinet. We are looking to make Fortinet one of a small handful of most-valued partners. By supporting security throughout the City of Portland, Fortinet is helping us maintain secure and reliably accessible services for our community."

June 13, 2022 8:03 AM
1606498-0-0-EN