CASE STUDY

Multisite College Achieves Security and Resiliency in Oracle Cloud Infrastructure

St. Petersburg College is a public college headquartered in St. Petersburg, Florida. It boasts an annual enrollment of about 31,000 students with 11 different campuses and centers located in St. Petersburg, Seminole, Pinellas Park, Largo, Clearwater, and Tarpon Springs. These campuses are in coastal cities in central Florida.

Business Continuity in the Cloud

Since St. Petersburg College is based in hurricane-prone Florida, business continuity is a major concern. Reliance on on-premises infrastructure means that a storm could take down systems storing the college's student records and administrative data. As a result, when given the opportunity, Chief Technology Officer David Creamer decided to move St. Petersburg College's enterprise resource planning (ERP) system to the cloud.

When choosing a cloud service provider (CSP), Oracle was the logical choice for St. Petersburg College. One of the main driving factors in this choice was a heavy reliance on PeopleSoft, an Oracle application. "Deploying PeopleSoft in the Oracle Cloud was an intuitive and cost-effective choice," Creamer explains.

A key decision factor involved the ability to easily and quickly build out the features the college needed in its cloud deployment. Oracle offered prebuilt shapes (a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance), based off Oracle and PeopleSoft standards. This enabled the team to easily define their cloud deployment. Oracle's automation capabilities also allowed the college's PeopleSoft team to make more efficient use of their time. These two factors assured Creamer that his team had made the right choice in picking Oracle as their CSP. "Oracle Cloud [Infrastructure] made it easy to port our production environment to the cloud, and its built-in automation is saving my team valuable time," Creamer says.

Securing the Cloud with Fortinet

After choosing Oracle as the platform to host the college's ERP, Creamer and his team embarked on a search for a firewall solution to secure the new cloud deployment. While security solutions based upon access control lists (ACLs) were readily available, they did not meet the college's security needs. As an educational institute, St. Petersburg College must maintain a very permissive "bring-your-own-device" (BYOD) policy, meaning the network contains many untrusted and potentially infected devices that generate traffic that must be monitored.

St. Petersburg College SPC

"With Oracle and Fortinet, St. Petersburg College's OCI network is more resilient, secure, and much easier to manage."

– *David Creamer, CTO, St. Petersburg College*

Details

Customer: St. Petersburg College

Industry: Education

Location: St. Petersburg, Florida

Business Impact

- Ensure 99.9% application availability in disaster-prone region
- Saved $12,000 annually by testing applications in Oracle Cloud
- Improved analytics enable five-year log retention that supports "default deny" firewall policies
- Reduced time to resolve service tickets from multiple days to one day

Integration with the Oracle Cloud Infrastructure (OCI) was one of the main selection criteria for a firewall provider. Fortinet differentiated itself by offering turnkey integration with OCI. "Fortinet is also the leading independent software vendor (ISV) security provider for Oracle Cloud," Creamer adds. This, along with the fact that Fortinet impressed the team in a previous evaluation, convinced Creamer to invite Fortinet to work with his team on a proof of concept (POC).

During the POC, St. Petersburg College, Fortinet, and Oracle worked together to identify and correct a minor software bug, setting the tone for the organizations' future relationship. "There was no finger-pointing, just a focus on finding and fixing the problem," recalls Creamer. Throughout the POC, Fortinet went above and beyond, providing demo licenses, helping to set up the firewall, and conveying additional knowledge to ensure the team had what they needed to make an informed decision.

Solutions

- FortiGate VM
- FortiAnalyzer VM
- FortiADC VM
- FortiCare

"The FortiADC controller decreased our network latency and provides us with full visibility into the traffic flowing through our load balancer. With full log access, we can quickly get to the bottom of any issues we experience."

– *Bernie Enlow, Network Design and Security Engineer, St. Petersburg College*

Enterprise-level Cloud-based NGFW Protection

With untrusted devices both inside and outside the network, the security team needed full network traffic visibility and protection at Layers 4-7. Additionally, protecting faculty and student devices required an integrated intrusion prevention system (IPS) that could identify and block threats before they enter the network. Finally, the team wanted full connection logging to support incident response, enabling them to respond to external requests for historical data regarding connections from their network.

As network latency and performance were key concerns for St. Petersburg College, the security solution could not increase latency or degrade performance. The St. Petersburg College networking team also needed the capability to segment the college's network into multiple zones for its websites, applications, databases, and administration. FortiGate next-generation firewalls (NGFWs) offer integrated intent-based segmentation, which allows the team to isolate these zones with zero-trust access control policies driven by the needs of the business.

Based on these requirements and their POC experience, Creamer and his team decided to deploy FortiGate VM virtualized NGFWs in OCI.

Achieving Network Visibility with FortiADC

After selecting and deploying their FortiGate NGFWs, Creamer and his team realized that their existing load-balancing solution was not capable of meeting the needs of the college. While their existing load balancer was capable of handling the volume of traffic that the college experienced, it did not provide any logging capabilities. When troubleshooting a network issue, Bernie Enlow, network design and security engineer at St. Petersburg College, often had little or no data to work with.

Based on his experiences with the earlier POC, Enlow spoke with the Fortinet team and opted for the VM form factor of the FortiADC application delivery controller. In addition to the logging and performance features, Enlow appreciated the cloud-native VM form factor, which made it easy to deploy in the OCI environment. "The FortiADC controller decreased our network latency and provides us with full visibility into the traffic flowing through our load balancer," says Enlow. "With full log access, we can quickly get to the bottom of any issues we experience."

Increased Agility in the Cloud

While business continuity was a major driver behind St. Petersburg College's shift to the cloud, they rapidly discovered that the switch also dramatically decreased operational costs due to newfound efficiencies in the DevOps testing environment.

The college operates a highly customized environment, meaning that every time an update or change is applied, it must be comprehensively tested. Most of this testing is handled in a DevOps environment that mirrors the production network. However, the team is frequently asked to test new features that require a completely new testing environment. In the past, this meant spinning up a testbed on-premises, which could take weeks.

By moving its deployment to OCI, Creamer and his team were able to set up a simulation of the organization's highly customized PeopleSoft environment in a few hours. With prebuilt shapes for Oracle applications and preconfigured Terraform templates for FortiGate NGFWs, the team configured the environment to their exact needs with minimal effort. Enlow notes, "In the secure Oracle Cloud [Infrastructure], we save over 20 staff hours every time we spin up a test environment." With around 12 such environments needed each year, the new test environment saves the college work days for other tasks. This translates to around $12,000 in annual productivity gains. In addition, these templates reduce misconfigurations in the cloud, a potential source of firewall breaches.

The use of cloud-based test environments also allowed the St. Petersburg College team to use their time for testing more efficiently, as they no longer need to wait until off-hours to spin up a new environment or to wait until physical appliances are ordered, delivered, and deployed. Moving to OCI enabled the team to more rapidly test and deploy network upgrades and new features, such as support for mobile devices for class scheduling.

> *"In the secure Oracle Cloud [Infrastructure], we save over 20 staff hours every time we need to spin up a test environment."*
>
> – *Bernie Enlow, Network Design and Security Engineer, St. Petersburg College*

Meeting Log Management Policy Requirements

St. Petersburg College takes a strict security approach to external content. The organization's network firewall operates on a "default deny" policy, where any suspicious content is blocked automatically at the network boundary. If, after further investigation, the detection is determined to be a false positive, then an exception is added for the specific user that requested it.

Accomplishing this requires the ability to access and analyze security logs for some time after an event occurs. The college has chosen to retain logs for over five years, which also allows them to respond to requests for information from external organizations regarding traffic that originated from the college's network. In the event of a breach, this log storage policy will also enable the security team to perform forensic investigation.

After its move to the cloud, the college needed a log management solution capable of meeting its retention policy. The FortiAnalyzer logging and reporting solution meets this need and integrates with more than 250 third-party products via the Fortinet Security Fabric. This solution consolidates log collection into a single tool and interface, which Creamer says has been a huge asset. "My team simply would not be able to gather and analyze log data in the same way without the FortiAnalyzer user interface," he notes.

Now, the team is able to rapidly inspect alerts on a daily basis, manage exceptions to their security policies, and quickly generate reports based upon collected data. These capabilities reduce the log analysis time and allow the team to generate reports more quickly than their previous solution.

Responsive, Effective Support Services

As it supports the round-the-clock activity of students and faculty, the St. Petersburg College network does not keep normal business hours. For this reason, Creamer and his team opted for an extended support contract with FortiCare support services to ensure they had help when they needed it.

"The FortiCare team provides some of the best technical support that I have ever experienced," Enlow says. "When we encounter a problem, we immediately get on a WebEx or Zoom meeting. The Fortinet support specialists know their stuff. There is no more waiting around for three days just to get a support contact, who then has no idea what I am talking about—as happens with other providers." With FortiCare support, the St. Petersburg College team is able to work out a trouble ticket from start to finish in one sitting, allowing them to get services back online and perform updates quickly.

Creamer's decision to move to the cloud was designed to ensure that St. Petersburg College's systems would be functional no matter what was thrown at them. With Oracle Cloud secured by Fortinet solutions and supported by FortiCare services, he has reached his goal. "With Oracle and Fortinet, St. Petersburg College's OCI network is more resilient, secure, and much easier to manage," says Creamer.

March 19, 2020 9:30 AM

569585-0-0-EN

D:\Fortinet\Case Study\St Petersburg\cs-FA-multisite-college-achieves-security-and-resiliency-352020\cs-FA-multisite-college-achieves-security-and-resiliency-352020