JBG SMITH

Real Estate Investment Firm Builds Comprehensive Defense Against External Cyberthreats and Internal Security Risks

JBG SMITH™ owns and manages millions of square feet of real estate, providing people in and around Washington, D.C., with inspiring places to live, work and shop. When JBG SMITH merged with another firm, it inherited network security point products that did not blend well with its legacy systems. To solve this problem and gain a more comprehensive approach to security, JBG SMITH moved to Palo Alto Networks® Security Operating Platform.

The Palo Alto Networks platform provides JBG SMITH with complete, integrated security and consistent policy enforcement across the enterprise network as well as to endpoints, on and off the network, and to the Microsoft® Azure® cloud. Alongside greater visibility into its network traffic, the firm gained intelligent control to enable trusted applications while preventing malicious content and targeted exploits from compromising business assets or productivity.

> “It’s really all about security. The Palo Alto Networks platform gives us protection at every layer. It’s not just edge, not just endpoint; it is top to bottom.”
>
> **David Shanker** | vice president of Information Technology | *JBG SMITH*

INDUSTRY

Real Estate

CHALLENGE

Achieve comprehensive security to enable critical business applications while preventing external threats and internal human error from compromising assets, both on and off the network.

ANSWER

Palo Alto Networks Security Operating Platform provides end-to-end security from the data center to the network edge, to local and remote endpoints, and out to the Microsoft Azure cloud.

SUBSCRIPTIONS

Threat Prevention, URL Filtering (PAN-DB), WildFire, GlobalProtect, Traps, AutoFocus, Panorama, Aperture

APPLIANCES

PA-3060 (2), PA-3020 (2), PA-850 (4), VM-300 (2)

RESULTS

- Achieves end-to-end security for network assets, endpoints and cloud applications.
- Enables key business applications while ensuring strong network security.
- Provides peace of mind that known and unknown threats will be automatically stopped.
- Mitigates risk of end users introducing ransomware or exfiltrating proprietary data.
- Ensures consistent policy enforcement while saving administration time.

Customer Overview

JBG SMITH is an S&P 400 company that owns, operates, invests in and/or develops assets concentrated in leading urban infill submarkets in and around Washington, DC. The company’s mixed-use operating portfolio comprises nearly 20 million square feet of high-quality office, multifamily and retail assets, 98% of which are Metro-served. Their emphasis on placemaking drives synergies across the portfolio and creates amenity-rich, walkable neighborhoods. JBG SMITH’s future development pipeline includes over 17.6 million square feet of potential development density. For additional information on JBG SMITH, please visit www.jbgsmith.com.

Consolidating Security Following a Merger

JBG SMITH has been part of the communities in and around Washington, D.C., for more than 50 years. More than just a building management firm and real estate investment trust, or REIT, JBG SMITH uses its creative resources to shape inspiring, engaging places for people to work and live. This requires an extensive IT infrastructure spanning standard office services, such as email and document management, as well as REIT-specific applications and an array of building automation and control systems.

For David Shanker, JBG SMITH’s vice president of Information Technology, priority one is protecting these business-critical assets from external bad actors and internal human error that could inadvertently unleash cyberthreats. Running a Cisco® shop from top to bottom, Shanker and his team had long relied on Cisco ASA firewalls with SecureX® administration and AnyConnect® VPN, along with WebSense for content filtering and Microsoft antivirus for endpoint protection. However, when the firm merged with another REIT, doubling its size virtually overnight, a major challenge emerged.

In the merger, the IT team inherited a second data center, along with additional network and security infrastructure that included Cisco FirePOWER®. However, there was no central management – traffic was routed for inspection to another data center outside the merged enterprise – and FirePOWER turned out to be especially problematic.

Shanker explains, “I didn’t want to continue with WebSense because it’s expensive and built on a legacy architecture that doesn’t support our cloud strategy. So, we decided to give FirePOWER a try. But on our ASA firewalls, FirePOWER brought everything to a crawl. It wouldn’t work with our REIT-specific applications. We had to disable services to get them to work. Our engineers did not want to deal with the situation at all and urged me to find a new solution.”

> "With Palo Alto Networks Traps running in conjunction with our next-generation firewalls, if an end user does something foolish on their computer, on or off our network, we apply policy to it and prevent the threat from detonating."
>
> **David Shanker** | vice president of Information Technology | *JBG SMITH*

He says the goal was to find a comprehensive offering. "Whatever we chose had to have intrusion prevention, content filtering, remote access, unified management, and be able to move easily to and from the cloud. We looked at several different vendors, but what really stood out with Palo Alto Networks was the integrated platform approach and how everything is centrally managed with Panorama. The way it all works together is leaps and bounds above what we had been tolerating up to then."

Greater Visibility and Intelligence With a Platform Approach

Shanker and his team replaced JBG SMITH's legacy security infrastructure with Palo Alto Networks Security Operating Platform, including next-generation firewalls, cloud-delivered security services and Traps™ advanced endpoint protection. Next-generation firewalls are deployed at the internet edge and in the data centers to inspect traffic across the company's software-defined wide area network. The firewalls also provide segmentation between building automation systems – which control heating, air conditioning, power, water and other critical building systems – and the property management offices.

The most immediate impact was a dramatic improvement in visibility. Shanker notes, "Before, we had no idea what people were doing in the field or what kind of traffic was rolling into our corporate office. With SecureX, unless there's a validated breach attempt, you simply don't know what's on the network. Now, the Palo Alto Networks platform lets us see exactly what's going on. If the network is slow one day, we can see who's using up all the bandwidth and address it."

The Palo Alto Networks platform also brought more intelligence to intrusion prevention and content filtering. For example, JBG SMITH runs a highly customized Oracle® application that creates some irregular behavior in web browsers. FirePOWER completely shut down the application, and despite their best efforts, the IT team could not get around it. By contrast, URL Filtering on the Palo Alto Networks platform identified the suspicious behavior and allowed IT to easily create an exception for this known, trusted application.

Similarly, Shanker points out that using Threat Prevention in conjunction with WildFire® cloud-based threat analysis service provides the intelligence to automatically stop cyberthreats of all types without relying on human decision-making. "With just a couple check boxes, we were able to block a full boat of potential threats. WildFire brings that extra peace of mind that someone is always looking out for you, taking a deeper look and stopping things before they get into your network. Before, SecureX would let traffic pass and alert us after the fact if there was something malicious, which we'd then have to manually address. We had to take a more preventive approach and eliminate the human element wherever possible."

Prevention-Based Endpoint Protection

Recognizing that traditional signature-based antivirus software is no longer adequate protection against today's sophisticated threats, Shanker also deployed Palo Alto Networks advanced endpoint protection offering, Traps. Traps now protects 1,100 end-user devices and more than 250 servers with a unique multi-method prevention approach that automatically blocks known and unknown threats.

Shanker remarks, "We were looking for the widest range of protection we could get, including preventing an employee from launching an executable that locks up their computer with ransomware. With Traps running in conjunction with our Palo Alto Networks next-generation firewalls, if an end user does something foolish on their computer, on or off our network, we apply policy to it and prevent the threat from detonating."

Traps automatically sends suspicious files to WildFire, where they are detonated and analyzed in a secure cloud environment to prevent even highly evasive zero-day attacks from causing trouble. WildFire then automatically shares the threat intelligence it gleans from this detonation across the entire Palo Alto Networks Security Operating Platform – firewalls, endpoints and all other elements.

"Signature-based antivirus is no longer effective," Shanker asserts. "With our antivirus, we got a lot of false positives, and it picked up things that were useless or outdated. We needed more intelligence to address endpoint protection holistically and proactively. A next-gen product like Traps was the answer."

He adds, "With WildFire, Traps isn't looking at things in a vacuum. The WildFire cloud gives us the scale to reference potential threats against what many other companies are seeing, which eliminates the false positives. And it's automatic, again removing the uncertainties of human intervention."

> “You have bad actors on the internet who are really good at getting through even the strongest security. The Palo Alto Networks next-generation firewalls are the first line of defense, but exploits can still get in through the endpoints. That’s why it’s important to have that extra layer of protection with Traps.”

David Shanker | vice president of Information Technology | *JBG SMITH*

Securing Assets on and off the Network

One of Shanker’s primary objectives is to protect JBG SMITH’s data whether users are on or off the enterprise network. The Palo Alto Networks platform enables him to achieve this by providing tightly integrated, end-to-end security that extends from the data center to the edge and out to local and remote endpoints.

“You have bad actors on the internet who are really good at getting through even the strongest security,” Shanker notes. “The next-generation firewalls are the first line of defense, but exploits can still get in through the endpoints. That’s why it’s important to have that extra layer of protection with Traps.”

Shanker extends this blanket of protection to remote users through GlobalProtect™ network security for endpoints, which enables enforcement of security policies regardless of where remote users connect to JBG SMITH’s network – at home or while traveling.

“We have to provide security on the go,” says Shanker. “We can’t rely on someone to turn on protection, like with AnyConnect. GlobalProtect is always on, it’s easy, and it’s part of a complete integrated platform, so our security is consistent on and off the network.”

Centralized Management Saves Time, Improves Consistency

Panorama™ network security management ties everything together for Shanker and his team by providing central control of the enterprise’s entire security landscape. This is a major improvement over their old way of managing security.

“We were constantly chasing after our ASA firewalls in terms of management,” Shanker recalls. “There could be a rule applied here but not there. Someplace else, an object might be missing, or the syntax on an inspection set was slightly different on one of the devices. We’re a small IT shop, so having a product like Panorama saves us a lot of time. We can just drop it on our network and go, with confidence that our policies are applied consistently across all devices.”

Shanker adds that visibility and insight are also much better with Panorama. “We can see what’s happening on our network. In the past, we often couldn’t get accurate or complete information. Now, if someone asks a question, we can hand them a nice, little report.”

AutoFocus™ contextual threat intelligence service will enhance this capability even further. While an issue requiring AutoFocus has yet to arise, Shanker expects it to provide invaluable intelligence. “We wanted AutoFocus so we’d have a way to quickly analyze attacks to understand what happened, how it happened and what we can do about strengthening our prevention tactics.”

Extending Comprehensive Security to the Cloud

As JBG SMITH continues to evolve its network infrastructure by moving select workloads to Microsoft Azure, Shanker has begun shoring up security in the cloud with the Palo Alto Networks platform. “Virtualized next-generation firewalls will enable us to secure our assets in Azure the same way we secure the rest of our network,” he notes.

Shanker’s cloud strategy also includes moving more applications to software-as-a-service, or SaaS, delivery. The company already uses Microsoft Office 365® and will soon move its entire document management system to SharePoint® online. The Aperture™ SaaS security service provides the full visibility, control and reporting Shanker needs to ensure JBG SMITH’s SaaS applications are fully secured.

Shanker has put a lot of trust in Palo Alto Networks to secure JBG SMITH’s network, and the reason is simple: “It’s really all about security. The Palo Alto Networks platform gives us protection at every layer. It’s not just edge, not just endpoint; it is top to bottom.”

The company behind the platform also makes a big difference. “When I need something, the phone gets answered. When I have a request, it gets done. We all have a job to do, so having that intelligent, responsive support we get from Palo Alto Networks lets me and my team focus more time on turning around projects that help JBG SMITH improve the business.