CITY OF WILLIAMSBURG

CASE STUDY

Williamsburg Protects Its 17th-Century Heritage from 21st-Century Cyberthreats with Enterprise-Scale Prevention, Detection, and Response

"Before, we were doing detection and response through a security information and event management system, but we had to piece together information from multiple sources. It took a ton of time to do it effectively. The beauty of Cortex XDR is that all the security information is together in one spot where we can get a complete view. It allows us to block out the noise so we can focus on actual issues."

Mark Barham | Director of IT | *City of Williamsburg*

INDUSTRY
Local Government

CHALLENGE
Prevent malware, ransomware, and other cyberthreats from breaching the city network and exposing private citizen data or disrupting city services

ANSWER
Palo Alto Networks Next-Generation Firewalls and Cortex XDR for comprehensive cybersecurity with intelligent detection and response from the network core to all endpoints citywide

SUBSCRIPTIONS
Threat Prevention, URL Filtering (PAN-DB), WildFire, Traps, Cortex XDR, Cortex Data Lake

APPLIANCES
PA-3020 (1), PA-200 (2)

RESULTS
- Automatically blocks tens of thousands of potentially malicious files
- Provides realtime protection against ransomware and zero-day attacks
- Improves speed and efficiency in prioritizing and responding to security alerts
- Enables consolidated visibility into security events regardless of origin
- Frees up more time for IT to focus on strategic cybersecurity and municipal projects

Customer Overview
The historic city of Williamsburg, Virginia, needed to protect its infrastructure from modern cyberattacks that could expose private citizen data, disrupt critical city services, and damage its reputation as a tourist destination. To address this need, the city deployed Palo Alto Networks Next-Generation Firewalls and Cortex XDR™, providing a hardline cyber defense for its network perimeter and endpoints, with intelligent detection and response to streamline security operations. As the Next-Generation Firewalls automatically block tens of thousands of potentially malicious files each day, Cortex XDR keeps a vigilant eye on all security events across the network and endpoints, surfacing the most urgent and relevant alerts for further investigation. This enables the IT team to act on and resolve security issues more quickly, freeing up more time for them to focus on projects important to improving city services while enjoying peace of mind that the infrastructure is protected against data breaches.

Protecting Living History Against Modern Cyberthreats
Williamsburg, founded as the capital of the Colony of Virginia in 1699 and later playing a key part in the American Revolution, is a city steeped in American history. In fact, its role in history is replayed daily in the streets of Colonial Williamsburg, the historic district, as the daily bustle of a modern city plays out all around in businesses, schools, civic centers, and residential communities. Like any city, Williamsburg provides a wide range of public services, including police, firefighters and other first responders, water and wastewater processing, public works, transportation, and parks. In today's digital world, even a city centered on 17th-century life must be vigilant against the risk of 21st-century cyberthreats.

Cities large and small have discovered that a security breach can be devastating. Private citizen data may be exposed. For a historical destination like Williamsburg, a breach could tarnish the city's reputation and hurt tourism. Under the worst circumstances, a deep-reaching cyberattack on city infrastructure could bring down critical municipal services altogether.

Williamsburg's director of IT, Mark Barham, is determined to prevent any of these scenarios from happening in his city. "If there was a breach that shut down our servers, we'd have issues dispatching and responding to 911 calls, it would disrupt water distribution, every municipal service would be affected. I don't ever want to have an event like that occur and say, 'if we had only done this one thing, we would have been good.'"

That's why Barham relies on Palo Alto Networks for comprehensive cybersecurity protection from the network core to endpoints across the city, all under constant watch through the intelligent security operations of Cortex XDR.

Strong Defense at the Network Core and Endpoints
As a central line of cyber defense, Barham deployed a Palo Alto Networks PA-3020 Next-Generation Firewall in the city's data center to inspect all traffic flowing between its network and the internet. Smaller PA-200 Next-Generation Firewalls are deployed at remote sites, such as the city's water treatment facility. Leveraging Palo Alto Networks services including Threat Prevention, URL Filtering, and WildFire® malware analysis, the Next-Generation Firewalls automatically block tens of thousands of potentially malicious data packets every day.

Understanding that sophisticated attackers are continuously finding more ways into networks, Barham took a fresh look at

> "Malware, ransomware, phishing—it's all a fact of life these days. Up to now, there's been a lot of concern not only about how we detect these types of threats, but how we respond to them. With Cortex XDR, I sleep a lot better. We have a much better understanding of what's out there, much better visibility into what's hitting us, and much better ways to isolate the threats and secure our enterprise."
>
> **Mark Barham** | Director of IT | *City of Williamsburg*

endpoint protection. "For a long time, we were a Trend Micro customer," says Barham, "but it's signature-based and not much good against zero-day attacks. We were looking for an approach that didn't use signature files."

Talking with other municipalities, Barham learned that Palo Alto Networks has a strong reputation with Traps™ endpoint protection. Unlike traditional signature-based approaches, Traps uses machine learning and artificial intelligence in combination with cloud-delivered WildFire malware analysis, drawing from the industry's largest global threat intelligence community to automatically detect and respond to sophisticated attacks, including zero-day threats. So, Barham started a pilot. Then, the question was how to tie together security events from both the endpoints and network firewalls.

"We were feeding information into a security information and event management system, but it was disjointed," says Barham. "Palo Alto Networks told us about Cortex XDR, and seeing how all security events go into a single data lake and Cortex XDR stitches everything together in one place for us, we were pretty much sold after the first demo."

Surfacing Security Alerts That Matter Most

Today, the City of Williamsburg has endpoint protection (now part of Cortex XDR) on hundreds of endpoints—250 devices, including laptops, workstations, and servers. The vast majority of cyberattacks are stopped automatically at the point of entry, while all security events from the endpoints and Next-Generation Firewalls are aggregated in Cortex™ Data Lake. Using machine learning, Cortex XDR then surfaces the most important alerts for further investigation.

Barham reports that the Palo Alto Networks technology is doing its job at the network perimeter and on the endpoints. "Using WildFire and the AI techniques from Palo Alto Networks, we haven't had any types of breaches," he affirms. "The way we use Cortex XDR is to see what's happening on the network and endpoints, and investigate anything that truly warrants our attention."

The city doesn't have a security operations center (SOC) or a dedicated security team on staff, so each member of the small IT team has multiple duties, whether that's network management, system and application analysis, or database administration. Therefore, any security alert that comes in takes time away from other important IT tasks.

Barham explains, "Before, we were doing detection and response through a security information and event management system, but we had to piece together information from multiple sources. It took a ton of time to do it effectively. The beauty of Cortex XDR is that all the security information is together in one spot where we can get a complete view. It allows us to block out the noise so we can focus on actual issues."

He adds, "We're able to do more in Cortex XDR than a security information and event management system because everything is right there. It has intelligence and context to understand where an issue occurred, what actually happened, who was affected, so we can act on what we really need to. I don't have to concern myself with things that don't matter. With Cortex XDR, we're able to be a whole lot more efficient and spend significantly less time on detection and response."

Added Intelligence to Accelerate Detection and Response

One of the common alerts Barham and his team respond to is when users attempt to install software. This has proven important for both sanctioned and unsanctioned software. Upon being alerted, someone from IT will immediately contact the user and determine if the software installation is authorized. If so, IT simply creates a rule in Cortex XDR, which then allows the installation to proceed with no further notifications. Conversely, if the software installation is questionable, IT can determine whether the software is trusted and otherwise advise the end user on IT policies.

"With Cortex XDR, we get notifications instantly and are able act on them much quicker than in the past," Barham says. "For valid software installations, it allows the end users and vendors to be more efficient in getting done what they need to. If it's questionable activity, it helps us ensure that whatever ends up on our network is valid as well as educate end users about the ramifications of risky behavior like installing unsanctioned software."

Having the intelligence and automation to accelerate detection and response with Cortex XDR brings much-needed peace of mind to Barham and the entire Williamsburg IT team. They can sleep at night knowing Palo Alto Networks is preventing malicious packets and files from getting through the security barriers set up on the network and endpoints. During the day, the team can work more efficiently, stay focused on the projects most important to the city, and act promptly on legitimate security alerts when necessary.

Barham concludes, "Malware, ransomware, phishing—it's all a fact of life these days. Up to now, there's been a lot of concern not only about how we detect these types of threats, but how we respond to them. With Cortex XDR, I sleep a lot better. We have a much better understanding of what's out there, much better visibility into what's hitting us, and much better ways to isolate the threats and secure our enterprise. That gives us time back in our day to spend on the business of running technology for a municipality. We can do that with confidence that we have the security we need."