Idaho's Largest County Takes a Next-Generation Approach to Governing Security

"We have such a broad range of security needs, yet the Palo Alto Networks platform allows me to manage them with simplicity and efficiency. With the types of advanced threats we face today, I'm not sure we could provide the necessary protections without it."

Bret Lopeman | IT security engineer | *Ada County*

INDUSTRY
Government

CHALLENGE
Enable a wide range of network access privileges for a multifaceted public-sector organization while preventing sophisticated cyberthreats from compromising vital network assets and private taxpayer information.

SOLUTION
Palo Alto Networks Next-Generation Security Platform, with granular application- and user-based policy management and comprehensive cyberthreat prevention, across the network and endpoint devices.

SUBSCRIPTIONS
Threat Prevention, URL Filtering (PAN-DB), WildFire, Traps, AutoFocus, Panorama, Premium Support

APPLIANCES
PA-3060 (24), PA-3050 (16), PA-3020 (12)

RESULTS
- Enables an integrated, prevention-based approach to network security and endpoint protection.
- Prevents known and unknown threats from compromising network assets and private information.
- Protects endpoints from malicious exploits, stopping 52 attempts in the first month of deployment.
- Eliminates lost employee productivity by stopping stealthy ransomware, such as Bad Rabbit.
- Simplifies policy management for diverse departmental access requirements.
- Provides centralized event logging and integrated trend analysis to continually refine prevention strategy.

Customer Overview
Ada County, located in southwestern Idaho, is a culturally vibrant and scenic community that comprises six cities: Boise (the county seat), Meridian, Garden City, Eagle, Star and Kuna. With more than 440,000 residents, Ada County is the most populous county in the state. The county government comprises 11 departments and seven elected offices.

Story Summary
The Ada County government in Idaho must ensure secure, unencumbered access to private network services and information, as well as public websites, for a diverse range of departmental needs – from those of county prosecutors and elected officials to law enforcement and records administration. However, the county's previous firewalls followed a traditional port-and-protocol approach to security that could not protect against today's sophisticated cyberthreats. To evolve its network strategy from reactive to proactive, Ada County replaced its legacy firewalls with Palo Alto Networks® Next-Generation Security Platform.

The Palo Alto Networks platform provides a prevention-oriented security model, including granular control to enable application and site access based on user need and role. The Next-Generation Security Platform protects the county's network resources and endpoints with a consistent, global threat intelligence-based security methodology that defends against known and unknown threats. Centralized event monitoring, including integrated trend analysis, uncovers insights that guide ongoing policy refinement as the threat landscape and Ada County's security requirements evolve.

Evolving Network Security to the Next Generation
Public sector organizations, such as county governments, have unique network access requirements compared to private enterprises. For example, in Ada County, a prosecuting attorney trying a drug trafficking case needs access to websites and applications that would be unthinkable in a business setting. In fact, the range of access requirements in Ada County is expansive. Each department – and often, individuals within those departments, whether a county commissioner, sheriff's deputy, treasurer or human resources manager – has its own set of needs and privileges.

"The Palo Alto Networks platform brought us a solid, application-aware environment that we could tie in to people instead of a PC on a desk and [lets us] automatically prevent threats from getting through instead of reacting after the fact."

Bret Lopeman | IT security engineer | *Ada County*

This presented Bret Lopeman, Ada County's IT security engineer, with a daunting challenge, and his previous firewall solution was not up to it. "With our old port-and-protocol approach, you either permit or deny access, and whatever traffic is permitted usually isn't inspected. That just doesn't cut it anymore. The threats have gotten too sophisticated, and the needs of our county government are too diverse."

The situation led Lopeman to adopt a prevention-oriented approach to network security with Palo Alto Networks Next-Generation Security Platform. "Our old technology was all device-based, and required me to manually identify the threats and block them. I'm the only security engineer for 1,800 people and 3,500 devices, so that was almost impossible to do. The Palo Alto Networks platform brought us a solid, application-aware environment that we could tie into people instead of a PC on a desk and [lets us] automatically prevent threats from getting through instead of reacting after the fact."

Granular Control With Application and User Awareness

Ada County deployed Palo Alto Networks Next-Generation Security Platform across multiple sites. A high availability pair of next-generation firewalls secures the internet edge at each of the county's two main facilities. A fifth next-generation firewall protects Ada County's E911 center, while a sixth enables secure access to the county's services by trusted outside agencies, such as local city governments and the FBI.

The county's network is subjected to about 1 million scans per day, primarily from internet bots trying to identify hosts vulnerable to attack. Further, the network gets hit with a targeted cyberattack at least three times a week. Lopeman isn't concerned, however. Threat Prevention, built into the platform alongside WildFire® cloud-based threat analysis service, automatically prevents cyber breaches during all stages of an attack, keeping network assets safe and county personnel productive.

"Nobody can keep up with all the cyber activity that's going on," Lopeman asserts. "That's why having the WildFire service for our network is crucial. I have WildFire look at everything coming inbound or going outbound. It's great because infected files in an email get stopped. If anyone tries to launch something malicious on the internet, they can't. It gives me an extra set of hands to block stuff, even if it's brand-new and unknown to us. So, I feel good about anything people are doing on our network, that it's not going to cause damage."

Individualized Policies Enable Secure Application Access

Lopeman tailors internet and application access based on job function and, when needed, even creates temporary policies for special cases.

"I build different policies for law enforcement, for the courts, for the treasurer – things the average office worker doesn't need. We have deputies and records clerks who don't need to be researching drugs on the web, but our detectives do. We get pretty granular. One time, I created a setup for an individual working on a really bad case, but once the case was closed, that access went away."

Lopeman takes advantage of App-ID™ and User-ID™ technology to further refine application policies and access privileges. For example, the widespread use of social media necessitates access to sites like Twitter® and Facebook® for departments like human resources and commissioners' offices. However, general office workers are not allowed on social media at work.

"App-ID and User-ID enable us to be fairly restrictive about what's allowed on our network and who can talk to it," says Lopeman. "For example, we only allow the apps our websites use to get to our network. We also started defining user groups that are only permitted access to certain areas on our network based on job function. These are the next-generation things we can do using the Palo Alto Networks platform that we could never have done with our old solution."

"The types of threats today are so immediate and difficult to detect, the old signature-based virus protection is not valid whatsoever anymore. We've had such success with the next-generation firewalls, and Traps is so integrated with the rest of the Palo Alto Networks platform - it just makes sense."

Bret Lopeman | IT security engineer | *Ada County*

A New Level of Comfort From Advanced Endpoint Protection

For Ada County, a major advantage of the Next-Generation Security Platform is having advanced endpoint protection as an integral part of a comprehensive, end-to-end security strategy. Like many organizations, Ada County historically relied on traditional antivirus software to protect its endpoint devices. As threat actors became more sophisticated, though, simply getting an alert about malicious software on a PC was not sufficient. By the time Lopeman could respond, the damage would be done.

"Like our network security approach, I wanted prevention for our endpoints instead of reaction," Lopeman says. "The types of threats today are so immediate and difficult to detect, the old signature-based virus protection is not valid whatsoever anymore. We've had such success with the next-generation firewalls, and Traps is so tightly integrated with the rest of the Palo Alto Networks platform – it just makes sense."

Lopeman deployed Traps™ advanced endpoint protection on 2,100 end-user workstations – mostly standard desktop PCs and laptops – as well as 75 virtual desktops used by Ada County's emergency dispatch center. Traps also protects 250 servers, mostly virtual machines, running applications like Microsoft® SQL Server®, Exchange and SharePoint®. As time and resources permit, Lopeman is uninstalling old antivirus software from devices throughout the organization.

"Traps has completely changed our approach to endpoint protection," Lopeman says. "Before Traps, if you got an email attachment, all you could do was scan it. If a zero-day came out, there was no vulnerability control with traditional antivirus. Now, with Traps, it's just set it and forget it. If someone tries to execute a file, it's blocked until WildFire runs the analysis and determines whether it's malicious or benign. The days of someone trying to send you a ZIP file to mess up your PC are over."

According to Lopeman, in its first month of deployment, Traps stopped 52 attempts to launch a process, several containing ransomware. Someone in the county office also tried to launch the new zero-day, Bad Rabbit ransomware, and Traps stopped it. Such attacks would have gotten through the old antivirus software, leaving victims stranded for the better part of a day while support staff re-imaged their PCs. "I feel more comfortable with our endpoint protection now because Traps looks at everything. It takes away a lot of concern."

Insight and Control to Maximize Protection

The Palo Alto Networks platform provides Lopeman with a unified view of activity across the county's network and endpoints through Panorama™ network security management. He also uploads network and endpoint log data up to AutoFocus™ contextual threat intelligence service to analyze activity and uncover trends that help guide changes to his prevention strategy.

"I use AutoFocus as a comparison tool and prevention aid," Lopeman notes. "It allows me to see what kinds of malicious activity other state and local governments are living with. I can look at the alerts and hashes they're getting, and then search for those in my organization and make sure we have the right protections in place."

He adds, "Panorama is where I configure and control every single next-generation firewall I have. It allows me to monitor all my traffic in one place instead of having to connect to different firewalls to look at their logs. Then I can go from that to AutoFocus and do trending, like uncovering a consistent DNS call that needs to be denied. And with one click back to Panorama, I can update my policies to block the DNS and push it out to all my firewalls simultaneously."

As a government entity, Ada County has a responsibility to provide effective county administration and law enforcement, deliver vital public services in a safe online environment, and protect private information for hundreds of thousands of taxpayers. With Palo Alto Networks Next-Generation Security Platform, Lopeman is confident his organization enables the county to meet these demands.

Lopeman concludes, "We have such a broad range of security needs, yet the Palo Alto Networks platform allows me to manage them with simplicity and efficiency. With the types of advanced threats we face today, I'm not sure we could provide the necessary protections without it."