

Fairfax County Partners with BlackBerry to Deter Cyberattacks



Local governments are often considered soft targets by threat groups, with a lucrative bounty of data to steal. Their illicit pickings include personal information from mortgage documents, deeds, birth, marriage and death notices, confidential medical records, Social Security numbers, and much more. CISOs are often hamstrung in their attempts to protect sensitive data due to political and budgetary constraints. Sometimes, it's near-impossible to implement a consistent security architecture across a gaggle of semi-independent government agencies.

As a result, local governments are often woefully unprepared to deal with today's increasingly treacherous threat environment. According to a report from BlueVoyant¹, malicious attacks against state and local governments have increased by nearly 50% since 2017.

Against this backdrop is Fairfax County, the 40th most populous county in the United States², where dozens of government organizations provide services to more than a million residents. Over the past decade, the county has been a standout among its peers, experiencing very few security incidents and maintaining an excellent record for business continuity.

Fairfax County

Industry:

County Government

Location:

Fairfax County, Virginia

Products:

CylancePROTECT®,
ThreatZERO®

Deployment:

18,000 Endpoints

Website:

www.fairfaxcounty.gov



Author's Note: The CylancePROTECT solution was formerly known as BlackBerry Protect.

BlackBerry's Cloud-native CylanceOPTICS and CylancePROTECT run on the AWS cloud and provide on-device threat detection and remediation across your organization—in milliseconds. BlackBerry products are available through the AWS Marketplace.

Upgrading a Failing Endpoint Security Infrastructure

Despite these successes, however, Chief Information Security Officer (CISO) Michael Dent was far from satisfied with the status quo in 2014, when he began planning a major endpoint security upgrade. “Our security and network staff couldn’t keep up with the flood of malware infecting our endpoints,” he says today. “We were spending way too much time cleaning and re-imaging employee systems. That’s a major hardship for a small team like ours. We’d been lucky so far. But I knew it was only a matter of time before our signature-based antivirus (AV) failed us entirely. The stakes were too high for us to gamble on a product that repeatedly showed it didn’t work.”

Dent and his team were surprised by what they found when they began evaluating candidate next-gen solutions. “Legacy antivirus companies did a decent job of responding to a malware infection after it compromised one of our test systems,” he says. “But only [CylancePROTECT] was able to prevent the malware from detonating. Plus, the other products relied on the cloud and a massive amount of data collection to work. [CylancePROTECT] didn’t need a cloud or Internet connection, collected only pertinent data, and was generally much easier to manage. After considering our options, we went with BlackBerry Protect.”

Dent engaged a team of [ThreatZERO](#)® experts to help with decommissioning the legacy AV and deploying [CylancePROTECT](#)®. According to Dent, “The implementation was seamless. The ThreatZERO team did an excellent job. They also provided useful suggestions on ways to harden our network and IT infrastructure.”

CylancePROTECT Delivers Return On Security Investment

According to Dent, “We realized a 251% return on investment (ROI) over three years by replacing our legacy AV with [CylancePROTECT].” This included:

- A 99% block rate for zero-day malware and potentially unwanted programs (PUPs). This virtually eliminated the need to re-image endpoints, producing an estimated \$110,000 in annual cost savings.
- A 40% increase in productivity by Dent’s team of 12 full-time IT and security employees, generating \$734,000 in yearly risk-adjusted savings.
- An overall net present value (NPV) of \$5,503,996.

“The results speak for themselves,” says Dent. “Since deploying [CylancePROTECT] seven years ago, we’ve been fortunate to experience very few security incidents caused by malware, ransomware, and zero-day exploits. [CylancePROTECT] secures our endpoints, frees up resources, and provides us with peace of mind. No other vendor can claim to do what [CylancePROTECT] does.”

“We realized a 251% return on investment (ROI) over three years by replacing our legacy AV with [CylancePROTECT].”

– Michael Dent,
Chief Information Security Officer,
Fairfax County

Security Is An Organizational Commitment

Dent is quick to share credit for the improvements in the county's security posture. "None of this would have been possible without the financial, logistical, and moral support of the Fairfax County leadership team," says Dent. "Security is much more than a departmental concern. It's a commitment that flows top down throughout an organization. Fairfax County has been successful because we're all committed to the same goal: delivering quality services to county residents, and protecting the privacy and integrity of their personal data."

Surviving the Pandemic and Securing the New Normal

Flashback to 2020. On March 7, a U.S. Marine assigned to Fort Belvoir became the first resident of Virginia and Fairfax County to test positive for COVID-19. Five days later, on March 12, Virginia Governor Northam issued Executive Order 51³, declaring a state of emergency along with plans for state government employees to begin a phased transition to teleworking⁴. On March 23, the governor ordered⁵ closure of "certain non-essential businesses" and all K-12 schools for the remainder of the academic year. A week after that, on March 30, the governor issued the state's first Stay-at-Home Order⁶.

The impact of these announcements on county and state services was immediate. The Virginia Department of Motor Vehicles closed 75 offices and all mobile units to the public⁷. Residents were encouraged to renew their licenses and vehicle registrations online. The Supreme Court of Virginia suspended all non-essential, non-emergency proceedings in district and circuit courts.

In Fairfax County, Public Schools Superintendent Scott Braband announced plans⁸ to provide elementary school students with laptops and distance learning resources. County government organizations began offering residents "Assistance from a Distance"⁹ to mitigate the effects of department and agency closures.

Throughout the pandemic, Dent and his colleagues worked tirelessly to ensure the continued security and productivity of the county's newly remote workforce.

Today, Fairfax County's shift to a hybrid workforce has become the new normal. According to Dent, "We currently have 10,000 county employees working from home. Going forward, they'll be allowed to work remotely 60% of the time. It's my job to make sure employee systems remain secure, so the machines we provide all run [CylancePROTECT]. Thanks to our partnership with BlackBerry, I'm confident in our continued ability to protect our IT infrastructure and maintain the public trust."

For more information, visit [Cylance Endpoint Security from BlackBerry](#).

"Since deploying [CylancePROTECT] seven years ago, we've been fortunate to experience very few security incidents caused by malware, ransomware, and zero-day exploits. [CylancePROTECT] secures our endpoints, frees up resources, and provides us with peace of mind. No other vendor can claim to do what [CylancePROTECT] does."

– Michael Dent,
Chief Information Security Officer,
Fairfax County

- ¹ BlueVoyant State and Local Government Security Report
- ² World Population Review: US County Populations 2021
- ³ Declaration of State of Emergency Due to Novel Coronavirus (COVID-129)
- ⁴ Governor Northam Declares State of Emergency, Outlines Additional Measures to Combat COVID-19
- ⁵ Governor Northam Orders Statewide Closure of Certain Non-Essential Businesses, K-12 Schools
- ⁶ Governor Northam Issues Statewide Stay at Home Order
- ⁷ CBS 19 News- DMV offices to close until April 2 due to COVID-19 outbreak
- ⁸ Fairfax County closes schools through Apr. 10
- ⁹ Assistance from a Distance During COVID-19

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow [@BlackBerry](https://twitter.com/BlackBerry).

