FireEye
SECURITY REIMAGINED

Maricopa County delivers secure services to its residents

The 4th largest county in the US entrusts FireEye to protect its data

CUSTOMER STORY

SECURITY REIMAGINED

CUSTOMER PROFILE

With over 4 million residents, Maricopa County is the most heavily populated in Arizona and the fourth largest county in the United States. Located in the south-central part of Arizona, the county has witnessed a rapid expansion in population over the last 10 years.

The Maricopa County Office of Enterprise Technology (OET) is tasked with providing a full suite of technology solutions to county departments, equipping them with the capabilities necessary to deliver exceptional customer-oriented services to the County's citizens, residents, employees, and elected officials.

"FireEye is a fantastic strategic partner for Maricopa County. We've been able to achieve things that apart we would not have been able to do."

– **David L. Stevens**, chief information officer for Maricopa County

One of the biggest trends in the public sector is the exponentially escalating increase in the public's expectations: Daily use of smart phones, tablets, social media and the web has brought unprecedented levels of convenience and expediency. David L. Stevens, chief information officer for Maricopa County, commented, "In this age of pervasive technology, our citizens and employees expect the same capabilities and service in their interactions with our county."

BUSINESS CHALLENGE

However, as a backdrop to the rising expectations, a core component of the charter for the Maricopa County Office of Enterprise Technology (OET) is to ensure the data security of the county's almost 60 departments. "The team's collective talent and effort fall short if we cannot deliver our portfolio of services securely; the threat of cyber attacks is one of the most significant risks we have to consider," remarked Stevens.

Michael Echols, chief information security officer for Maricopa County, elaborated, "The diversity of data we handle means that we have to comply with a wide range of federal and industry regulations, including HIPAA, PCI, CJIS, and NIST-related mandates. With web and email-based attacks representing such a significant source of potential risk, we created a strategy specifically to identify, manage, and mitigate the risk of cyber threats."

Having defined the desired approach, Echols and his team performed an extensive analysis of solutions capable of fulfilling the requirements. He stated, "We found several companies that had solutions in the appropriate areas but we also wanted to see demonstration of sustained leadership in the advanced tools market, and we really wanted a company that we could build a longer-term partnership with.

"I knew about FireEye before we started our research but wasn't aware it had the technologies that could deliver what we needed. Our concept and the FireEye model were an excellent match."

The County's FireEye account team was asked to conduct a proof of concept to demonstrate the capabilities of the FireEye® Email Threat Prevention (EX Series) Platform. Echols commented, "We immediately saw results and of special note was the absence of false-positives,

> "FireEye has reduced our malware liability significantly, very significantly."
>
> – **Michael Echols**, chief information security officer for Maricopa County

which is typically what is experienced with products that purport to be more thorough in detection capabilities. This really piqued our interest and culminated in the decision to go with FireEye as our partner of choice.

"Another significant benefit is the ability to respond to phishing attacks from malicious emails with malware payloads, etc. We found that the EX platform detected payloads that were not identified in our mail gateway. The solution was configured with auto mitigation, resulting in the phishing campaigns launched and detected by the EX, not ever reaching their target. This enabled us to identify and respond to threats in real-time without requiring any manual intervention."

The County supplemented its EX Series Platform with the FireEye® Network Threat Prevention (NX) Platform, the FireEye® Host Prevention Platform (HX) and FireEye® Central Management (CM Series). "We use the FireEye forensics capability all the time, especially in demonstrating what an individual piece of malware is capable of doing," described Echols. "We're able to observe behaviors and note trends, and also categorize malware components. From this we're then able to tune our process-based solutions to further mitigate against subsequent attacks and contain the lateral spread of malware.

"I am a constant user of the CM Series console: It gives me a dashboard view of everything that's occurring across the whole environment in real-time. Our FireEye platforms are configured inline and are deployed at every egress-point enabling me to see exactly what's going on. I'm also immediately made aware of any potential email-based threats as they occur."

He continued, "I have visibility into zero-day attacks and can see what's been detonated – I'm aware if the attack is something that's never been seen before, or if it's a reoccurrence of a previously detected event. The FireEye console gives me a unified view of everything. If we do witness something happening that warrants closer scrutiny we can triage any system and do on-the-spot forensics right from our offices without the need to go out and visit each desktop."

More recently, the county added to its layered defense architecture with the integration of a FireEye Threat Analytics Platform (TAP) into its diverse environment. The platform utilizes threat intelligence, expert rules and advanced security data analytics to interrogate complex event data streams. Echols commented, "The Threat Analytics Platform will allow us to prioritize and focus our response efforts on the alerts that really matter to the county."

Despite the dramatically elevated levels of protection, users are unaware of the presence of the FireEye platforms: "No one knows they're there except for the IT team members who manage the devices," affirmed Echols, "but FireEye has reduced our malware liability significantly, very significantly."

Stevens summarized, "I like to tell people that we have a lot of vendors but we have very few strategic partners. FireEye is a fantastic strategic partner for Maricopa County. We've been able to achieve things that apart we would not have been able to do."

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**