



AVERTIUM CASE STUDY:

CUSTOMER: THE COURTS

☎ Have questions? Give us a call.
877-707-7997

➤ **www.avertium.com**

📍 **Arizona • Tennessee**



Copyright © 2024 Avertium

CONTENT



| | |
|---|----------|
| About The Customer and Their Cybersecurity Shift | 3 |
| Customer Challenges | 3 |
| How Avertium Helped The Customer | 4 |
| • ASSESS Compliance with a Gap Assessment | 4 |
| • DESIGN the Cybersecurity Infrastructure with the Microsoft Security Suite | 5 |
| • PROTECT continuously 24/7/365 | 5 |
| Engagement Results | 6 |
| • A Proactive Cybersecurity Strategy | 6 |
| • A Responsive Partner | 6 |
| • A Culture of Security | 6 |

ABOUT CUSTOMER AND THEIR CYBERSECURITY SHIFT



In this case study, we have anonymized our customer in order to better protect their critical legal infrastructure. They will instead be referred to as "The Courts". A state judicial branch, or court plays a vital role in legal matters large and small, hearing everything from capital offenses and felonies to traffic offenses and land title disputes. In this specific case, The Courts see nearly 900,000 court cases annually across 120 counties, but the court system has responsibilities that extend beyond offering justice to the citizens it serves – including protecting sensitive data related to the court cases being processed.

In 2021, The Courts' Information Security Architect (ISA), whom we will refer to as "John", transitioned from the private sector to the public sector. As the new ISA, he quickly noticed that the absence of a cybersecurity infrastructure, coupled with a largely reactive approach to cybersecurity, posed serious risks. John identified an opportunity to enhance The Court's cybersecurity posture – which led to a significant shift in the organization's cybersecurity priorities.

CUSTOMER CHALLENGES



John's challenges with the The Courts's cybersecurity infrastructure fell into three buckets: 1) Need for program roadmap, 2) Getting buy-in from internal stakeholders, and 3) Fully utilizing the court system's existing Microsoft investment.



Need for program roadmap: In a previous private-sector role, The Courts' had to adhere to FDIC guidelines; this provided a great starting point for their prior organization's cybersecurity strategy. But in the case of The Courts' court system, there were no regulatory mandates that provided a frame of reference. Without that provided directionality, the court system had to work from the ground up to implement a cybersecurity strategy. The absence of a regulatory framework, coupled with the size and scale of the court system (120 counties, 250+ internal apps, 3,500 workstations), made it hard to understand or measure the efficacy of the existing cybersecurity program in any meaningful way.



Getting buy-in from internal stakeholders: Like many cybersecurity leaders, John had to garner support from internal stakeholders within the court system. Government entities typically require more approval in order to make any major changes; as a result, they move much more carefully, especially when undertaking projects like a security overhaul. To justify this investment and to move the process along more quickly, John spent time educating The Courts about "the why" and "the how" behind his cybersecurity recommendations.



Fully utilizing the court system's existing Microsoft investment: The Courts, operating in 120 counties, manages 250+ internal apps, all under a Microsoft-centric approach with a G5 license which includes all of the Defender suite (Defender for Endpoint, Defender for Cloud Apps, Defender for O365, and Defender for Identity) protects its 3,500 workstations. Microsoft Sentinel was later added as a new SIEM to take advantage of the integrations that exist within the court's environment. Because The Courts lacked subject matter experts who could work within each tool AND see how they connected to the bigger picture, the team needed to rely on a Microsoft Partner for guidance to tie all of their Microsoft tools together by implementing Sentinel and ultimately drive toward better security outcomes.

While Avertium had been helping The Courts with security log management since 2020, it wasn't until John began looking for vendors to help tackle these challenges that they realized Avertium could partner with them as a security advocate, security expert, and strategic consultant.

“Avertium is able to bring an expert perspective while maintaining a personal touch.”

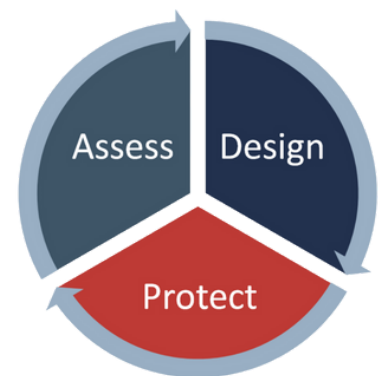
– Information Security Architect, The Courts

HOW AVERTIUM HELPED THE CUSTOMER

After presenting substantial data and reasoning to justify the investment in security, John needed a security solution that delivered the value he had been promising to stakeholders and bolstered his claims around why it was so necessary.

John appreciated the personal touch Avertium brought to The Courts' security measures and how the Avertium team applied industry expertise.

The promises and pleas for stronger security John had been making for months came to fruition in front of his (and his teams') eyes. Using its Assess-Design-Protect Approach, Avertium delivered measurable value from the start:



ASSESS Compliance with a Gap Assessment

The Avertium team began with a gap assessment of The Courts' entire infrastructure. Because a governance committee had yet to be established, Avertium was essentially working from scratch. Initially, The Courts tried to implement NIST across their environment but quickly encountered internal resistance when stakeholders realized that NIST wouldn't meet all of the court system's security requirements. So Avertium pivoted – working with The Courts was about finding a solution that worked for their unique environment, not forcing a specific cybersecurity framework.

Ultimately, Avertium helped The Courts adopt CIS IG1. It was more flexible and intuitive for even the non-technical teams. In the end, Avertium created a more unified governance framework and deployed CIS IG1 across all 120 counties.

Moving towards a unified front flipped a switch for The Courts' leadership. The CIO, CTO, Tech Officer, Application Officer, and more members of the leadership team shifted their adoption strategies once they began to see the benefits this new structure was bringing to the team. They had finally uncovered a solution that just made sense for their organization's unique context.



DESIGN the Cybersecurity Infrastructure with the Microsoft Security Suite

To build a long-lasting security strategy, The Courts needed a solid foundation of security tools. Like many businesses, they turned to the Microsoft suite – but without subject matter experts in-house, they found it challenging to get the most out of Microsoft’s security suite.

For The Courts, a new tech stack meant a new SIEM. Cybersecurity teams know SIEM migration is hard enough – but when the team isn’t familiar with the new tool, that layers on an even more difficult set of challenges. Avertium guided the courts through their migration to Microsoft Sentinel, even accelerating the timeline to a rapid 40 days (less than the average 60 days).

The SIEM migration was just the beginning. Avertium was able to walk John’s team through the nitty-gritty details of each tool and connect its configuration to a bigger-picture cybersecurity strategy, offering a practical roadmap alongside its deep bench of Microsoft security experts to guide the court system through the process. With Avertium’s help, The Courts developed a thorough understanding and security strategy through the following Microsoft tools:

-  **Microsoft 365 GCC G5**
-  **Microsoft Defender for Identity**
-  **Microsoft Azure**
-  **Microsoft Defender for Cloud**
-  **Microsoft Sentinel**
-  **Microsoft Defender for Endpoint**
-  **Microsoft Entra ID**

**PROTECT continuously 24/7/365**

One of the things John appreciates most about Avertium is that the team always has his back, whether that means helping him think through how to sell security initiatives to internal stakeholders or diligently manage, optimize, and monitor the court system’s SIEM and EDR 24/7/365 through Managed Sentinel.

“I feel like I have a whole team in my corner now.”

“Avertium is always available to help. With other partners, I always felt like just another cog in the wheel. Avertium answers the call no matter what. If I don’t know an answer to a question I’m being asked, all I have to do is shoot Avertium a message and that question gets answered. Beyond that, they’re always offering me ideas on how to take our cybersecurity strategy to the next level. I feel like I have a whole team in my corner now.”

– Information Security Architect, The Courts



ENGAGEMENT RESULTS



A Proactive Cybersecurity Strategy

Just a few months into their security journey, The Courts' system has already noticed a considerable improvement in its preparedness. Before, The Courts' system's cybersecurity strategy was more reactive, requiring the team to wait for an incident to strike before they were able to mobilize. Now, they are ahead of incidents, subscribing to Avertium's flash notices and proactively addressing any risks in their network.

In the event that a threat does slip through the cracks, John now has visibility and confidence that the court system's cybersecurity infrastructure will enable security teams to respond quickly and effectively. Today, The Courts is ready for whatever is next, no matter what "next" may be.



A Responsive Partner

As John worked to build out The courts' security strategy, he needed more than a provider – he needed a partner. And that is exactly what Avertium was. With Avertium, John felt like more than a customer. When he called, Avertium answered.

"Avertium is always looking for opportunities to improve the service they were providing [The Courts], and bringing ideas to us to take the courts to the next level. With other providers, it would be the other way around...but because Avertium truly understood [The Courts'] needs and unique environment, Avertium is able to bring an expert perspective while maintaining a personal touch." – Information Security Architect, The Courts



A Culture of Security

One of John's greatest hurdles from the beginning was merely convincing their team that advancing their security was worth their time (and budget). Rome wasn't built in a day, and the same goes for a strategic security roadmap (especially in an industry with lots of hoops to jump through). Avertium helped John not only build a realistic security roadmap but also advocate for his security vision to non-technical stakeholders.

Though the road to security can be a long one, the results Avertium demonstrated in just the early stages of their partnership have been substantial. Avertium helped John champion the move towards a compliance and security-first culture, shifting the mindset across the courts to prioritize their cybersecurity measures. The Courts adoption of a compliance framework and Microsoft suite demonstrate more than just a few changes to their immediate protection: They are proof of a holistic and prioritized security culture, changing the way The Courts operate on a day-to-day level.

"Unwavering support and expertise."

"Avertium's Solutions Architects, have been invaluable in navigating the day-to-day challenges. Working with them feels like I have two dedicated experts in my corner, providing unwavering support and expertise."

– Information Security Architect, The Courts




Level up your
cybersecurity posture
and contact an Avertium
expert today >

ABOUT AVERTIUM

Avertium is a cyber fusion company with a programmatic approach to measurable cyber maturity outcomes. Organizations turn to Avertium for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and Threat Intelligence, Avertium delivers a more comprehensive approach to cybersecurity.

That's why over 1,200 mid-market and enterprise-level organizations across 15 industries turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. **Show no weakness.®**

 Have questions? Give us a call.
877-707-7997

 www.avertium.com

 Arizona • Tennessee



Copyright © 2024 Avertium