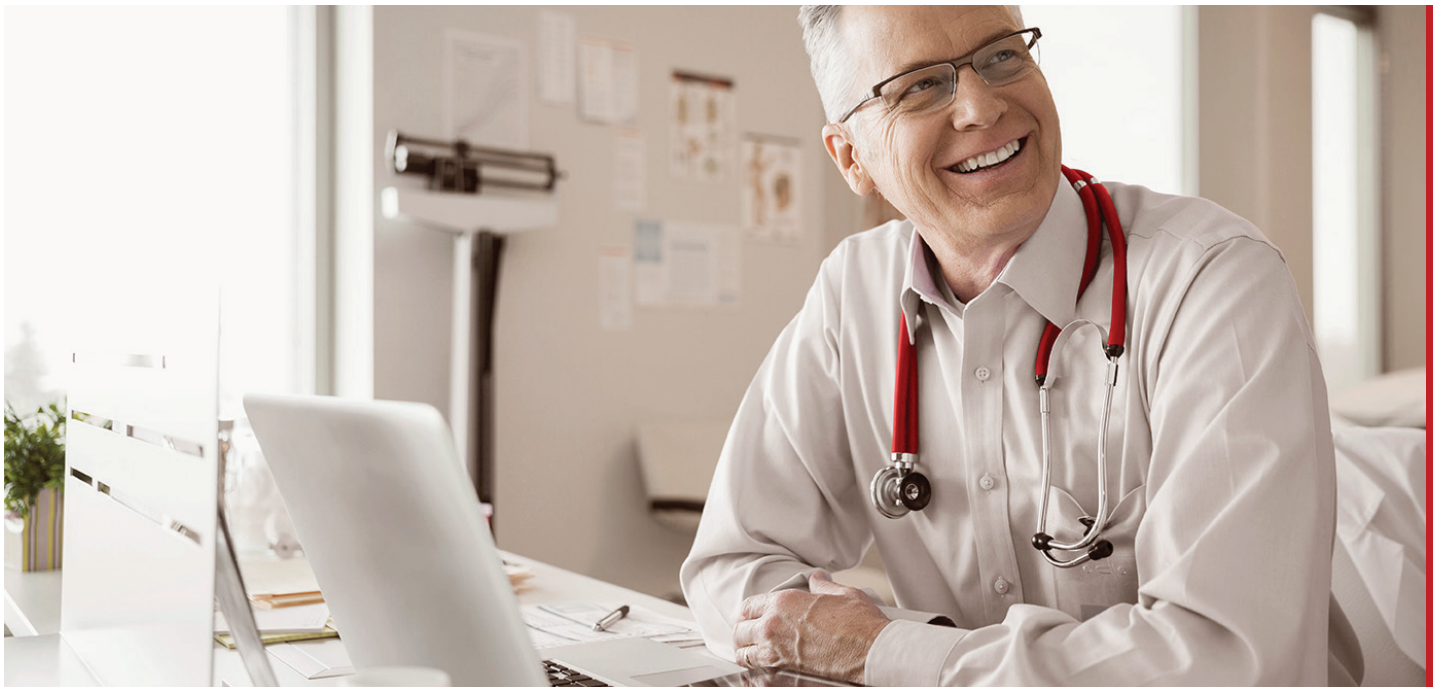
CASE STUDY

British Acute Healthcare Provider Builds Adaptable Security Infrastructure

Small team bolsters security amidst continuously changing requirements, environment, and threat landscape



County Durham and Darlington NHS Foundation Trust

Customer profile
Acute NHS care provider in Northeastern England

Industry
Healthcare

IT environment
6,000 endpoints across two acute hospitals, six community hospitals, and 70 locations

By building an adaptable security infrastructure based on the McAfee® integrated security platform, this small information security team dramatically improved its ability to defend its organization, staff, and patients, despite an environment of continual change.

The United Kingdom's National Health Service (NHS) foundation trusts are healthcare providers that together cover the country geographically to deliver healthcare services for all inhabitants. One of the largest integrated care providers in England, the County Durham and Darlington NHS Foundation Trust serves a population of more than 650,000 in Northern England through its two acute hospitals, six community hospitals, and 80 community sites. As the ICT Technical Security Manager for the Trust, Tony McGivern never stops working to ensure that the Trust can deliver its critical services 24/7 and that its staff and patients can be confident their information is safe.

Constant Change Demands Robust, Adaptable Security

Since McGivern began working at the Trust in information security eight years ago, he and a minimal security team have often had to deal with industry and institutional changes that affect information security, but these days dealing with change is their modus operandi. For instance, the Trust is currently preparing to move entirely to electronic patient records. In addition, because of the impending NHS England sustainability and transformation plans, which are intended to provide patient services when and where they are needed, regardless of which local service providers are nearby, the Trust must be able to securely exchange more information with other healthcare organizations. If that's not all, the Trust can be called upon at any time to add new healthcare services that introduce additional systems into the environment. And, of course, there is always the latest cyberthreat looming in the background. "Ultimately, all these changes and potential changes, from both inside and outside the organization, demand a higher level of security, with greater visibility, control, and adaptability," explains McGivern. "For instance, in the future, with increased exchange of information with other healthcare organizations, we need to be even better at knowing exactly what is entering and exiting our network, and blocking anything that shouldn't enter or depart and ensuring it is secure at all times of transfer."

Zero-Day Attack Prompts Return to McAfee

Ten years ago, County Durham and Darlington NHS Foundation Trust decided to try an alternate antivirus solution. However, shortly thereafter a zero-day attack caused significant impact across the organization. An available McAfee license enabled the Trust to submit one of the zero-day infected files to McAfee. "McAfee staff were absolutely fantastic in helping us eradicate the virus," recalls McGivern. "After that, the Trust switched back to McAfee endpoint protection and has been a very happy customer ever since."

After assessing the ever-morphing, always challenging global threat landscape, the Trust decided to invest further in McAfee solutions and take advantage of the McAfee integrated security ecosystem, the McAfee ePolicy Orchestrator® (McAfee ePO™) central console, and the open source Open Data Exchange Layer (OpenDXL), which connects security components to automate integration and enable real-time data exchange. "An ecosystem in which security systems share threat information in real time and learn and adapt

Challenges

- Enable uninterrupted patient services and protect patient data
- Protect against cyberthreats and vulnerabilities, including zero-day threats
- Efficiently adapt to ongoing and future changes in complex environments
- Meet the above challenges with minimal resources and operational overhead

in the process improves our defenses tremendously," says McGivern. "And the McAfee ePO central console makes it possible for minimal human resources to manage the entire security environment."

WannaCry Ransomware Thwarted by New Defenses

To strengthen endpoint protection, the Trust enhanced its existing McAfee Complete Endpoint Threat Protection suite by upgrading approximately 6,000 endpoints to McAfee Endpoint Security, migrating all rules for the McAfee VirusScan® Enterprise software to the McAfee Endpoint Security Threat Prevention module and rules for McAfee SiteAdvisor® to the McAfee Endpoint Security Web Content module. "McAfee Endpoint Security gave us a greater level of protection and flexibility, and in a smaller package," notes McGivern. "We have a lot more confidence in our endpoint protection now."

McGivern had already been testing McAfee Endpoint Security on a few hundred nodes when the WannaCry ransomware hit. Urgency to block the ransomware fast tracked approvals, enabling McGivern's team to immediately deploy McAfee Endpoint Security across the enterprise. Within a week, all nodes were protected by McAfee Endpoint Security and were sharing information across the DXL with other McAfee solutions in the Trust's environment. While the WannaCry malware created chaos at many other organizations or caused them to disconnect internal and external services out of fear, the County Durham and Darlington NHS Foundation Trust kept up and running, business as usual, with no interruption in patient services.

Fortifying Web Protection and Reducing Help Desk Calls by 80%

To improve web protection, including more flexible filtering and stronger website categorization capabilities, the Trust replaced its existing web gateway appliance with McAfee Web Gateway, one of McGivern's favorite investments. According to McGivern, a vulnerability assessment of web traffic found that during the two weeks prior to installation of McAfee Web Gateway, 2,500 outbound connections to known indicators of compromise (IoCs) occurred, compared to zero in the two weeks following implementation. The McAfee appliance was also cost effective compared to the solution it replaced.

The security team has also benefited greatly from more granular controls within McAfee Web Gateway, including the ability to customize the message that is displayed when a web page is prevented from loading. Before implementing McAfee Web Gateway, the user would see the same generic message when a web page was blocked, regardless of whether it was blocked because the site was not safe, against corporate policy, or some other reason. Now the user sees a message explaining why that page is blocked. If necessary, users can request a site re-categorization. McGivern estimates that this feature alone has reduced calls to the help desk by 80%.

"Although we can't point to specific metrics, I feel like McAfee Web Gateway pays for itself tenfold," says McGivern. He also mentions that as patient records become completely digital, he expects that McAfee Web Gateway, along with McAfee Network Data Loss Prevention, will yield significant return on investment.

McAfee Solutions

- McAfee® Complete Endpoint Threat Protection
- McAfee Endpoint Security
- McAfee Endpoint Threat Defense and Response
- McAfee Device Control
- McAfee Web Gateway
- McAfee Advanced Threat Defense
- McAfee Threat Intelligence Exchange
- McAfee SIEM: McAfee Advanced Correlation Engine, McAfee Enterprise Log Manager, McAfee Enterprise Security Manager, McAfee Event Receiver, McAfee Global Threat Intelligence for SIEM
- McAfee Data Loss Prevetion Endpoint (McAfee DLP Endpoint)
- McAfee ePolicy Orchestrator

Widespread Visibility Across the Enterprise with McAfee SIEM

According to McGivern, the Trust added McAfee Enterprise Security Manager and other components of the McAfee SIEM solution primarily to expand visibility across the enterprise, enabling better control and increased ability to meet future compliance requirements. "We wanted to be able to tie everything we could into a SIEM—firewalls, gateways, IPS, and so on, as well as physical security such as video cameras and door access devices—so we could monitor everything in one place," he says. "We did just that with the McAfee SIEM. As a result, we have an infinitely better handle on what is going on in our environment."

The McAfee SIEM proved extremely useful to McGivern during the weekend of the WannaCry outbreak: "Since the SIEM and McAfee ePO console are integrated, I basically looked at the McAfee ePO console on my laptop, reporting to management every few hours from my kitchen table. Without leaving home, I could tell whether, when, and where the ransomware had entered our environment and verify that it was blocked each time. My counterparts in neighboring healthcare organizations, on the other hand, struggled to gain the same visibility in their own organizations."

With the McAfee SIEM, out-of-the-box correlation rules handle most of the security team's needs. It is also easy to customize reports. McGivern cites aspects of user access—who has access to which systems, when access occurred, what was accessed, and so on—as a common focus of customized reports. One report that McGivern runs frequently shows all remote access to the Trust's systems. "With the remote access report, we can tell if any of our suppliers has accessed information during nonstandard hours, and, if so, require justification," cites McGivern as an example of how the report strengthens security.

Saving Time When Investigating Potential Threats and Speeding Time to Resolution

Because of the impending England NHS sustainability and transformation plan and the subsequent need to exchange more information with other healthcare organizations, the Trust decided to augment threat detection with a McAfee Advanced Threat Defense sandboxing appliance. "We need to ensure that all of the additional incoming traffic is legitimate," notes McGivern. Now, when McAfee Web Gateway or McAfee Endpoint Security encounters an unknown, potentially malicious file, the file is sent immediately to McAfee Advanced Threat Defense, which uses static and dynamic analysis and sophisticated machine learning to detect threats that use evasion techniques.

"McAfee Advanced Threat Defense saves time investigating potential threats and dramatically accelerates time to resolution," claims McGivern. "For instance, just today out of the 327 files McAfee Advanced Threat Defense received, it detected 42 malicious files. McAfee Web Gateway blocked them all, and McAfee Advanced Threat Defense confirmed that they were indeed malicious. Without McAfee Advanced Threat Defense, we would have had to investigate many of the questionable files manually."

Results

- Assisted in defending the organization against the recent WannaCry ransomware attack
- Provides adaptable, extensible threat defense infrastructure
- Saves administrative time and reduces incident response time
- Reduced help desk calls by 80%
- Increases visibility into threats and compliance efforts

The Trust is currently piloting McAfee Endpoint Threat Defense and Response and its McAfee Active Response capability on a subset of high-risk endpoints. McGivern expects the endpoint detection and response (EDR) technologies will be especially important when new services are added. "If the new service introduces hundreds of new machines, we can't reimage them all from scratch," explains McGivern. "We need to be able to quickly pinpoint exactly where a bad file resides and take action immediately."

To prevent leakage of sensitive data in outgoing traffic, the Trust has relied on McAfee Device Control and McAfee Endpoint Encryption for many years. It has also recently added McAfee DLP Endpoint in anticipation of electronic patient records and the sustainability and transformation plan.

Praise from Board of Directors

The County Durham and Darlington NHS Foundation Trust's board of directors has been very pleased with the increased level of protection that the integrated McAfee solutions have provided, especially after the Trust escaped unscathed from the WannaCry ransomware attacks and was able to keep the board and upper management continuously apprised of the status of the Trust's environment, providing reliable information as needed. "We received ardent praise from our board after the WannaCry attack," recalls McGivern.

"I have been very impressed with both the range of products that McAfee provides and the knowledge and expertise of McAfee Professional Services," continues McGivern. "Change is a fact of life in our industry. With McAfee, we have a high level of confidence and assurance that our information security infrastructure can and will adapt to meet our ever-changing security challenges."

"We received ardent praise from our Board after the WannaCry attack… Change is a fact of life in our industry. With McAfee, we have a high level of confidence and assurance that our information security infrastructure can and will adapt to meet our ever-changing security challenges."

—Tony McGivern, Security Manager, County Durham and Darlington NHS Foundation Trust

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com