# Kettering Health Prescribes Cyber Observer for Healthy IT Security Environment

## A major roll-out and COVID-related challenges stalled cyber hygiene

Known for brand recognition scores that consistently chart 20% above average, Kettering Health was steadily embracing layered defenses and aligning with NIST security controls to protect a distributed, hybrid network supporting 13 medical centers, over 120 outpatient locations, and more than 30,000 users when an aggressive rollout of the EPIC Electronic Health Records system fully consumed all IT resources.

With the IT team focused on implementing EPIC, cyber hygiene activities stalled. The resulting configuration drift was worsened by the COVID-19 pandemic as IT staff, again pivoting from routine maintenance, labored to address the new security challenges presented by a mobile and remote workforce of first responders.

“Tool misconfiguration frequently opens the door to attack, especially as telework surges,” explains Michael Berry, Director of Information Security and CISO at Kettering Health. “Because attackers are constantly on the lookout to exploit vulnerabilities, our goal is to ensure that our security tools are providing the best possible protection.”

## Complexity and scarce resources made cyber hygiene hard to reestablish

Standing in the way of ensuring IT security was in peak condition was limited visibility into the status of the security tools. Manual, ad-hoc analysis using open source and freeware technologies was time-consuming and delivered suboptimal insight into the security posture of the enterprise.

Also impeding the effort to keep the cyber hygiene ‘house in order’ was an overwhelmed IT network team with no time to dedicate to cyber hygiene.


**CUSTOMER:**
Kettering Health

**INDUSTRY:**
Health care

**ORGANIZATION SIZE:**
1,800 physicians
14,000+ employees

**LOCATION:**
130+ medical centers and outpatient facilities in Ohio

**SUMMARY:**
Top-performing health system network gains real-time visibility into the state of network security tools and transforms cyber hygiene processes to ensure IT security provides a strong defense against cyber threats.

Further, with a diverse toolset, the knowledge required to maintain the tools increased. The need to maintain business continuity while protecting against new cyberthreats made it impossible to research what needed to be done, let alone make the changes to update the configurations. Beyond lacking the time to stay up-to-date on product features, system upgrades, and industry security controls, with everything seemingly equally urgent, the tool custodians didn't know where to start in remediating misconfigurations.

**Kettering moved to continuous monitoring with Cyber Observer**

To maintain a strong security posture, Kettering Health selected Cyber Observer for its ability to continuously monitor the IT security infrastructure and provide actionable insights and recommendations to ensure cyber hygiene, achieve compliance with regulatory frameworks, and fully optimize tool configurations across the security ecosystem. Equally important was the platform's ability to prioritize based on critical security controls and business impact.

**How Cyber Observer helped reestablish cyber hygiene**

"The proper configuration of security tools plays a vital role in mitigating vulnerabilities," continues Berry. "Cyber Observer gives us the ability to be proactive and look for misconfigurations rather than wait for an incident. The simple dashboard provides instant insight into the state of the systems, potential misconfigurations, and policy failures – all mapped to critical security controls. Diagnostics, for example, that would normally require a network architect to drill down several levels are viewable at a glance on a single screen. Rather than spending time doing a root cause analysis, we can now quickly evaluate a situation and take immediate action. Not only that, Cyber Observer's simple dashboard is also invaluable in reporting to the Board on the status of information security and our progress in aligning with the NIST Cybersecurity Framework."

> "I've never seen a tool that visually delivers as much diagnostic information on system technologies—and in a manner that is very easy to see and understand—as Cyber Observer.
>
> We have immediate visibility into the state of network tools and potential misconfigurations and know what action to take."
>
> **Michael Berry**
> Director of Information Security and CISO, Kettering Health

"Cyber Observer increases our ability to correctly deploy and leverage a tool's full capability while lowering the required knowledge capital," explains Berry. "As a small shop with a tight budget, we can't afford to simply rip and replace technologies. Because Cyber Observer guides us in what to do to get the biggest bang for the buck, we can take a phased approach to making new investments. Cyber Observer also tells you when there is a deviation from established thresholds and baselines and how to remediate it. Busy analysts can focus on high priority projects instead of attempting to stay up-to-date on system upgrades and security trends."

**Outcome: The Merlin Difference**

"We like to get the most out of everything that we invest in. We are more than pleased with our partnership with Merlin and how easily the partnership came together," concludes Berry. "The Merlin team is not only great to work with, but are open to suggestions for enhancements. They go above and beyond to incorporate new features and are always willing to help. Being able to pick up the phone and say, "We are having issues, can you please take a look and help," is usually unheard of – but not with Merlin. The ease of those conversations and the assistance is greatly appreciated."

**Merlin Ventures**, a strategic partner of Cyber Observer, helps visionary companies rapidly scale to deliver disruptive solutions for today's most critical cybersecurity challenges. Partnering with Merlin has helped Cyber Observer penetrate new markets and increase its presence in North America.