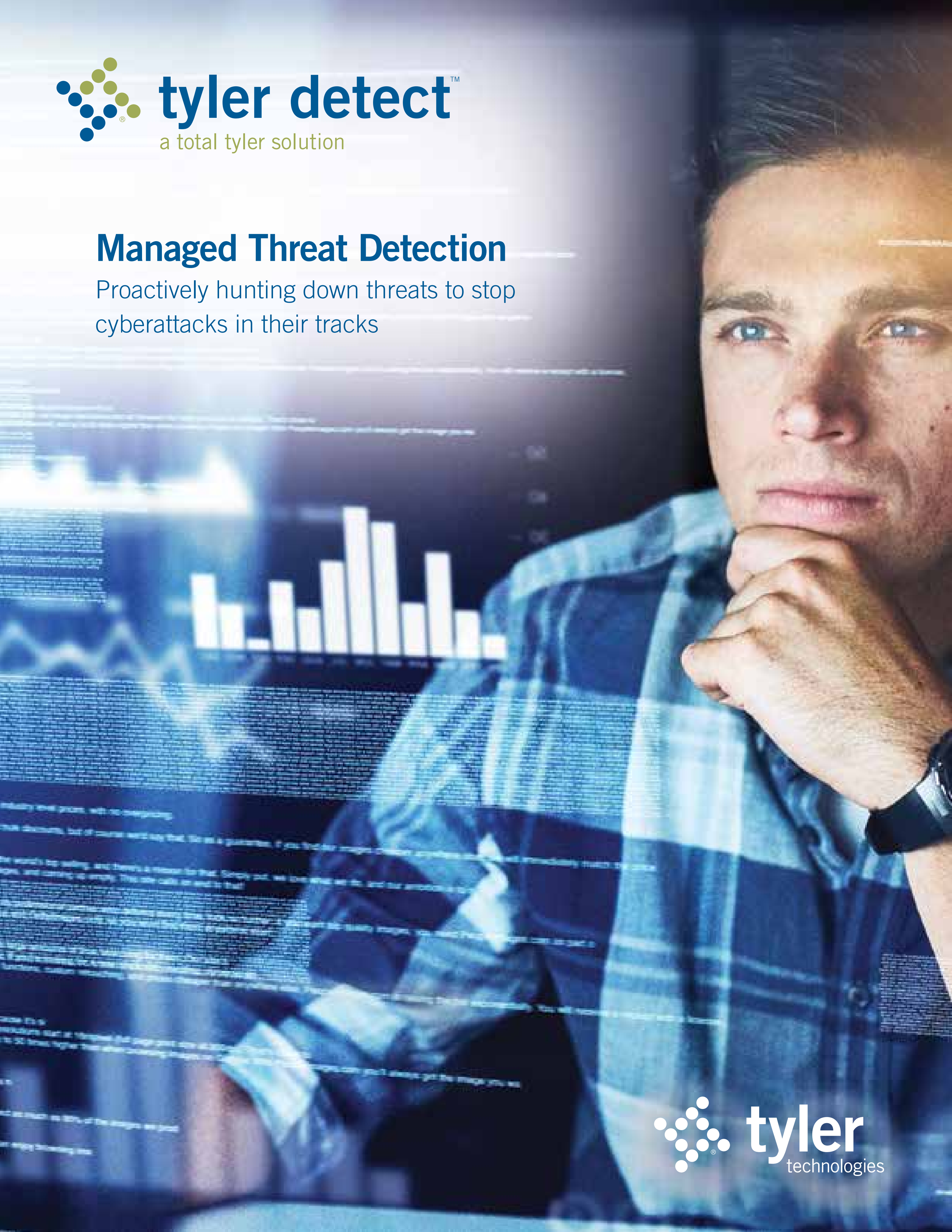
tyler detect™
a total tyler solution

Managed Threat Detection

Proactively hunting down threats to stop cyberattacks in their tracks



tyler technologies

"There is absolutely no way for a CIO or technology director to be aware of what is going on in their environment without a tool like Tyler Detect. Knowing that I have security experts monitoring my traffic 24/7 for any deviant behavior gives me and the County's management team peace of mind."

— **Aaron Kostyu**
Director of Technology for
Lowndes County, Georgia

Take a Proactive Stance Against Cybercriminals

Local governments and school districts are falling victim to cyberattacks with alarming frequency and devastating consequences. It's no surprise considering the wealth of personal information saved on your networks. Data on citizens, students, and employees is all at risk of being compromised or held hostage.

Cybercriminals are extremely adept at obtaining access to networks undetected with hazardous effects. We see it in the headlines every day. As the number of successful cyberattacks continues to soar, it's time to take a proactive stance to detect them.

Automated controls will fail. You can't simply sit back and wait for an alert to let you know you've been breached. Continuous analysis of your network traffic is essential to quickly detect and contain threats.

Tyler Detect allows you to overcome the day-to-day demands of threat hunting, whether you have gaps in technology, manpower, or expertise.

With Tyler Detect:

Your network is under surveillance 24/7	Threats are hunted down by highly trained cybersecurity analysts
Incidents are found and confirmed for you	You are contacted within minutes of a threat

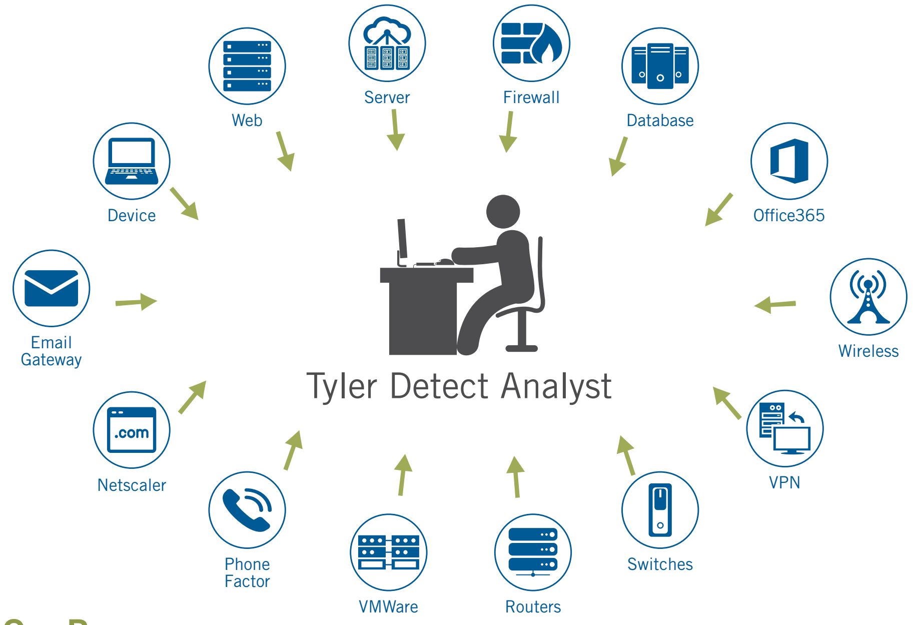
Tyler Detect: Security Analyst as a Service

Tyler Detect is a subscription service that combines automated tools with real-time human analysis and the latest threat intelligence to quickly and accurately detect threats across your entire environment, including endpoints. We confirm an incident and deliver remediation recommendations within minutes, 24/7.

Holistic View of Network

We monitor your entire network, including endpoints, and hunt for indicators that you have been compromised.

Tyler Detect analyzes logs generated by network devices including Firewalls, VPNs, Web Servers, Authentication Servers and Devices, Windows Application Servers, SQL Databases, Routers/Switches along with a host of other interconnected systems.



Our Process

1 Query
- Query network devices every 15 minutes
- Transmit new activity to our SOC

2 Investigate
- Investigate anomalies
- Confirm malicious activity

3 Alert
- Alert you to risky behavior by email
- Alert you to active threats by phone call

"Detecting cyber threats is a full-time job, and we just didn't have the resources to dedicate to it. The task is time consuming. There is a huge amount of data that needs to be sifted through. Plus, attacks don't always happen during normal business hours. With Tyler Detect, I feel like I have a team working around the clock to uncover all those things I didn't know before."

— **Mike Caffrey**
IT Executive, East Tennessee Governments

> **“Tyler Detect’s methodology is very unique in this marketplace and because of that, I believe their service sets them apart from competitors and has already shown value to our City.”**
>
> — **Paul Fraser**
> Director of Information Technology, Auburn, Maine

What Sets Us Apart

Our Methodology

Our focus is not to find known malicious activity. Automated systems like your firewall, anti-virus software, and even intrusion detection systems, are an important line of defense against known threats. They catch the easy stuff. But what you don’t know can harm you!

Hackers have access to all the same tools—and they test their malicious code to make sure it can get through these defenses. That’s where Tyler Detect comes in. We look at what has been allowed in, and alert you to any potential risky or malicious activity.

This means you can stop an incident before it becomes a breach.

Our Thoroughness

The Tyler Detect team is 100% focused on security and brings that expertise to your network. We develop familiarity with your environment. By learning what traffic is expected and allowed, we develop a baseline of your network behavior over time. This allows us to minimize false positives and detect indicators of compromise quickly and accurately.

With insight to your entire network, including endpoints, we examine behavioral attributes and place an activity in the appropriate context.

We identify sophisticated and zero-day threats, even those mimicking normal behavior.

Our Intelligence

Tyler Detect analysts are highly trained threat hunters. They detect advance threats by examining behavioral attributes of network users and placing activity in the appropriate context.

They couple this intelligence with an awareness and understanding of the latest developments in the external threat environment. This skill requires regular and consistent attention and allows them to stay in tune with the latest cyberattack vectors that can impact your organization.

You can stop cybercriminals in their tracks with Tyler Detect.

What You Get

Real-Time Alerts

If you are actively at risk, we contact you immediately.

- Unique and suspicious activity is identified and confirmed
- Detailed notifications of what occurred are sent immediately
- Request authorizations are available to disable infected Windows machines to mitigate suspicious activity

Daily Report

Every day, our analysts prepare a summary of your network traffic.

- Daily reports consist of critical log data for a 24-hour period
- Secure and documented audit trail for compliance
- Summarized monthly reports that auditors love

Secure Online Portal

Get insight into all your network traffic online 24/7.

- Search and filter your report data
- Access dashboards with system health statistics
- Review up-to-date threat intelligence

> **“Tyler Detect solved all our cybersecurity problems. Their analysts have the expertise to translate our network activity and make it meaningful and actionable for us.”**
>
> — **Craig Bowser**
> Information Technology Division, State College, Pennsylvania

"The Tyler Detect team are all very knowledgeable, professional, and persistent in tracking us down to address potential issues as soon as possible. That's why they have a stellar track record. It gives me peace of mind knowing that we have Tyler Detect as part of our proactive, IT Security portfolio."

— **Laurie Gagner**
Information Technology
Director, Sunrise, Florida

Success Stories

Ransomware

At 1:39 a.m., our 24/7 Security Operations Center (SOC) received an endpoint alert detailing a new persistence mechanism detected on a critical server. After researching the event, the persistence mechanism was determined to be an exact match to known WannaCry Ransomware infection indicators of compromise. At 1:51 a.m., the SOC escalated the alert to the Tyler Detect senior analyst on duty for verification and notification to the client. The server was taken off-line before any files were encrypted.

In another instance, one of our clients had a user unknowingly download ransomware during a session and did not notice their files being encrypted. Tyler Detect analysts identified the new persistence mechanism within minutes and notified our clients. They contained the incident to the user's local machine before it encrypted the shared folders.

Office 365 Account Takeover

A Tyler Detect analyst initially identified a brute force attack being perpetrated against our client's network. They went to the log files to investigate. At that time, no suspicious logins were found.

Still, the Tyler Detect analyst followed up with the client to review the findings. They let them know to keep a sharp eye out for any suspicious login activity while they worked to get two-factor authentication set up.

Weeks later, while reviewing the logs, the Tyler Detect analyst identified that one of their police detectives was logging in from Nigeria. Of course, the detective wasn't really in Nigeria. But his account had been compromised and taken over by a criminal who was!

Tyler notified the client so they could stop the attack before any damage was done.

Trojan

At one municipal client, Tyler Detect discovered a machine had been infected with a Trojan, which is a type of malware that tricks users into downloading by posing as a legitimate application. Many Trojans act as a backdoor, connecting to a command and control (C2) server that gives an attacker unauthorized access to the compromised computer.

Upon further investigation, they found that a computer was potentially compromised through the download of a fake antivirus software. The Trojan was removed before any harm was done.

Fileless Malware

Fileless malware is a popular cyberattack vector because it's difficult to detect. It's doesn't need an executable file (.exe) like other malware does. Instead it operates using legitimate programs, typically a common scripting language, like PowerShell, for malicious purposes.

A malicious encoded script can be decoded by PowerShell, and then reach out to a command and control server, without writing any files to the local hard drive. Without a payload file to infect a system, antivirus software applications can't generate a signature definition based on the malware's characteristics or detect the compromise, and it gets by undetected.

Malware must survive when you reboot your device, which is called persistence. By identifying suspicious and unique persistence mechanisms on devices, Tyler Detect identified numerous fileless malware attacks, allowing our clients to stop an attack before any damage is done.

What Tyler Detect Identifies

Malware

Zero-Day Exploits

Ransomware

Suspicious Activity

Compliance Violations

Errant Administrative Activity

Explore our services at tylertech.com/cybersecurity

About Tyler Cybersecurity

Information security has always been a top priority at Tyler. Tyler has taken that focus to the next level by offering Tyler Cybersecurity, products and services supported by a team of experts dedicated to protecting their clients since 2002. By partnering with Tyler Cybersecurity, our clients realistically and cost-effectively protect their information assets while maintaining a balance of productivity and operational effectiveness.

Tyler Technologies (NYSE: TYL) provides software and services to transform communities. Tyler's solutions connect data and processes across disparate systems, allowing clients to gain actionable insights for solving problems. We are proud to deliver effective cybersecurity solutions to help protect our communities.

Tyler was also named to Forbes' "Best Midsize Employers" list in 2018 and recognized twice on its "Most Innovative Growth Companies" list. More information about Tyler Technologies, headquartered in Plano, Texas, can be found at tylertech.com.

800.772.2260 | info@tylertech.com | tylertech.com

tyler technologies

Empowering people who serve the public®