nDiscovery™

a total tyler solution

Managed Threat Detection

Discover a better way to detect threats in the vast cyber universe.

tyler technologies

Manage Threat Detection with nDiscovery

Tyler Technologies' nDiscovery™ provides advanced threat detection, incident response support, and compliance reporting across your entire environment — all without the need to invest in costly hardware devices or dedicated resources.

Whether you're a small government agency or an enterprise organization, nDiscovery will:

Save you time, because the research and confirmation of potential malicious activity is off your plate. No need to juggle competing priorities.

Save you money, because you no longer need to invest in training, development, or headcount for security expertise.

Let you know when you've been breached and exactly what to do about it.

Why nDiscovery?

According to a recent Ponemon Institute report*, 63 percent of organizations experienced at least one cyberattack in the past 12 months — and getting malware attacks under control continues to plague companies across all sectors. Tyler's nDiscovery solution offers all the features you need to overcome the challenges and confidently defend your network.

Advanced Threat Detections

61 percent of organizations do not rate their ability to detect a cyberattack as highly effective. This is in part because advanced threat detection cannot happen by algorithm alone. nDiscovery combines human expertise with the latest threat intelligence and advanced data analytics to quickly and accurately detect threats across your entire environment.

Incident Response & Forensic Support

65 percent of organizations report a shortage of skilled personnel on their incident response teams. During an incident, you need to know how it happened, the extent of the damage, and how to correct it. With nDiscovery, we have immediate access to forensic-quality data to determine exactly what's going on — and tell you what to do about it.

Regulatory Compliance & Reporting

Analyzing audit logs is an integral part of complying with a number of IT security compliance standards, but the process is extremely time consuming. nDiscovery keeps you in compliance, and provides daily and monthly reports that auditors love.

Confirmation in Real-Time

The average time to detect an advanced cyberattack is 170 days, and the longer it takes to identify and contain data breaches, the more it costs your organization. With security events streamed in real time, nDiscovery validates the breadth of an incident and delivers remediation recommendations within minutes.

Dedicated Support from Cybersecurity Experts

55 percent of companies lack the in-house expertise to detect threats. Precious time is wasted because many malware alerts investigated are false positives. We're 100 percent focused on security and bring that expertise to your team, so you can focus on your core disciplines. We develop familiarity with your environment and provide support and guidance with security findings.

Simple & Light Deployment

Other solutions require you to invest in costly hardware devices, software applications, or dedicated resources. We don't. Set-up is straightforward and we're there to assist you every step of the way.

* *The State of Malware Detection & Prevention, Ponemon Institute© Research Report, March 2016*

“nDiscovery has helped us take control of our network and be proactive instead of reactive to issues. I trust [the team] to help us keep our assets as safe as possible.”

—Lisa Roy,
Chief Technology Officer,
Maine Maritime Academy

What nDiscovery Analyzes

Traditional thinking of maintaining adequate controls on critical network devices is no longer enough to stop incidents or breaches from happening. nDiscovery analyzes logs generated by network devices, firewall traffic, Windows® endpoints, along with a host of other interconnected systems to get a holistic picture of your environment to detect threats, regardless of the entry point of the attacker.

Analyzing allowed activity is an important part of our methodology because it is not always approved. Whether an unintentional oversight or a targeted attempt to leverage protected information, risk exposures are often introduced via allowed activity or an authorized connection from a third-party. nDiscovery reviews and reports on all administrative activity, so that you can be sure that they are legitimate … and approved.

- Firewall
- Windows Endpoints
- Windows Servers
- Web Servers
- Microsoft SQL Servers
- FTP Servers
- Linux Servers
- Switches
- VMWare
- VPN Servers
- Routers
- Email Gateways
- Phone Factors
- Wireless Access Points
- Netscalers

What nDiscovery Detects

- Malware
- Zero-Day Exploits
- Ransomware
- Insider Threats
- Compliance Violations
- Errant Administrative Activity

How nDiscovery Works

With Tyler's nDiscovery, your network is under surveillance 24/7 and our team of cybersecurity experts hunt down potential threats for you every day. Incidents are found and confirmed for you — and you receive remediation recommendations within minutes.

Contextual & Behavior Analysis

With insight to your entire network, including all Windows endpoints, we examine behavioral attributes and place an activity in the appropriate context. This allows us to detect sophisticated and zero-day threats, even those mimicking normal behavior.

Current Threat Intelligence

With the dynamic pace of change in the external threat environment, keeping up-to-date is an on-going and time-consuming responsibility. Our security analysts are constantly combing the latest threat intelligence from a collection of public and private data repositories.

Data Aggregation & Advanced Analytics

Intelligence gained from working with a broad spectrum of industries allows us to detect new threats before automated tools even know they exist — and with heightened awareness by our cybersecurity experts compared to your internal team.

Business-Specific Context & Security Intel

Not every environment is the same. By developing a baseline of your network behavior over time, we minimize false positives and detect indicators of compromise quickly and accurately.

The nDiscovery Team

Most solutions that detect network threats are completely automated, so no one is actually watching what's happening. nDiscovery is entirely different. We have real security professionals hunting for threats every day.

Our nDiscovery team is so much more than just cybersecurity experts. We are trusted advisors and your go-to resource.

We are an extension of your team, and you can rely on us just like your other employees. Pick up the phone and a dedicated specialist will be there to provide support and answer questions.

You can trust the nDiscovery team to answer your mission critical questions!

> **"I just don't have the resources to stay up-to-date on the threat landscape and constantly tweak how we go about uncovering suspicious network activity. nDiscovery functions as an extension of our team. The analysts provide a consistently excellent level of service, which allows us to feel confident in the analysis and support we receive through nDiscovery."**
>
> —Brian Stoughton,
> IT Security Engineer,
> Massachusetts Medical Society

nDiscovery Provides all the Benefits you Need, at a Low Cost

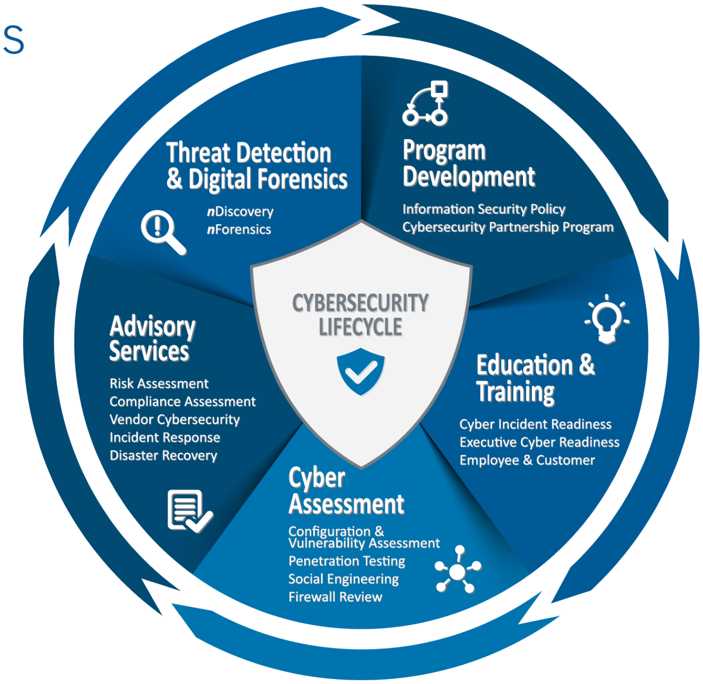
	nDiscovery	MSSP	SIEM	Cloud Log Mgt
TECHNOLOGY: A foundation for effective data collection & processing.	✓	✓	✓	✓
METHODOLOGY: A proven process for reliable, consistent detection.	✓	✗	✗	✗
HUMAN EXPERTISE: Expert analysis and a go-to resource for answers.	✓	✗	✗	✗
THREAT HUNTING: Uncovers activity missed by automated systems.	✓	✗	✗	✗
CROSS INDUSTRY METRICS: Active threat intelligence center for better insight.	✓	✓	✗	✗
INDEPENDENT OVERSIGHT: Offers transparency & removes conflict of interest.	✓	✗	✗	✗
COST OF OWNERSHIP: An in-house security expert is expensive.	$	$$$	$$$	$$

nDiscovery is a subscription-based service. Licensing is determined by type of device and the size of your environment.

About Tyler Technologies

Protecting your business from cyberattacks is a full-time endeavor that grows more demanding, specialized, and sophisticated every day.

Tyler Technologies has the expertise and resources to help you achieve cyber resiliency.



Discover the Tyler Difference

We are an extension of your team.

We are human experts who you can talk to on the phone, over email, or in person about your questions and concerns. We aren't satisfied with our job until we've made sure that you are completely comfortable and confident in the cybersecurity plan of action we've developed together for you.

We can support your entire cybersecurity life cycle.

Every organization's cybersecurity needs are unique, and there is no such thing as a one-size-fits-all solution. From risk assessment to threat detection and everywhere in between, Tyler partners with you to help you make informed choices about the services that are right for your organization, regardless of where you are in your cybersecurity life cycle.

We are 100 Percent Focused on Cybersecurity.

A comprehensive approach to cybersecurity requires thoughtfulness and adaptability. That means real people working in real time to react to everchanging threats, with expertise and judgment gained over decades of experience. This is who we are and what we do at Tyler, and we pass that expertise on to you.

Explore our services at www.tylertech.com/nDiscovery.

About Tyler Technologies

Tyler Technologies is a leading provider of end-to-end information management solutions and services for local governments. Tyler partners with clients to empower the public sector — cities, counties, schools and other government entities — to become more efficient, more accessible, and more responsive to the needs of their constituents. Tyler's client base includes more than 15,000 local government offices in all 50 states, Canada, the Caribbean, Australia, and other international locations. In 2017, Forbes ranked Tyler on its "Most Innovation Growth Companies" list, and Fortune included Tyler on its "100 Fastest-Growing 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®