Keep A Step Ahead of Cyber Criminals

Speakers: Karen Grosset & Jim Ash

Karen Grosset

Tyler Cybersecurity
Sales Manager

Jim Ash

Account Executive

tyler technologies + sage DATA SECURITY

Tyler and Sage partnered in 2013 to **monitor the Tyler Data Center and its 5000+ clients**

Sage has provided **innovative cybersecurity services** since 2002

email

banking info

utilities

critical services

SSNs

Municipal landscapes
are **prime targets**

A tale of **two cities**

Baltimore, Maryland		Riviera Beach, Florida
619,000	Population	35,000
50 people	IT Department	10 people
13,000	Employees	550
May 7, 2019	Attack date	May 29, 2019
RobbinHood	Infection type	Email Phishing
$76,000	Ransom Asked	$592,000
$0	Ransom Paid	$592,000
$18 Million	**Total Expenditure**	**$1.5 Million**

tyler detect™

a total tyler solution

Advanced threat detection, incident response support, and compliance reporting

tyler detect™

a total tyler solution

Managed **threat detection**

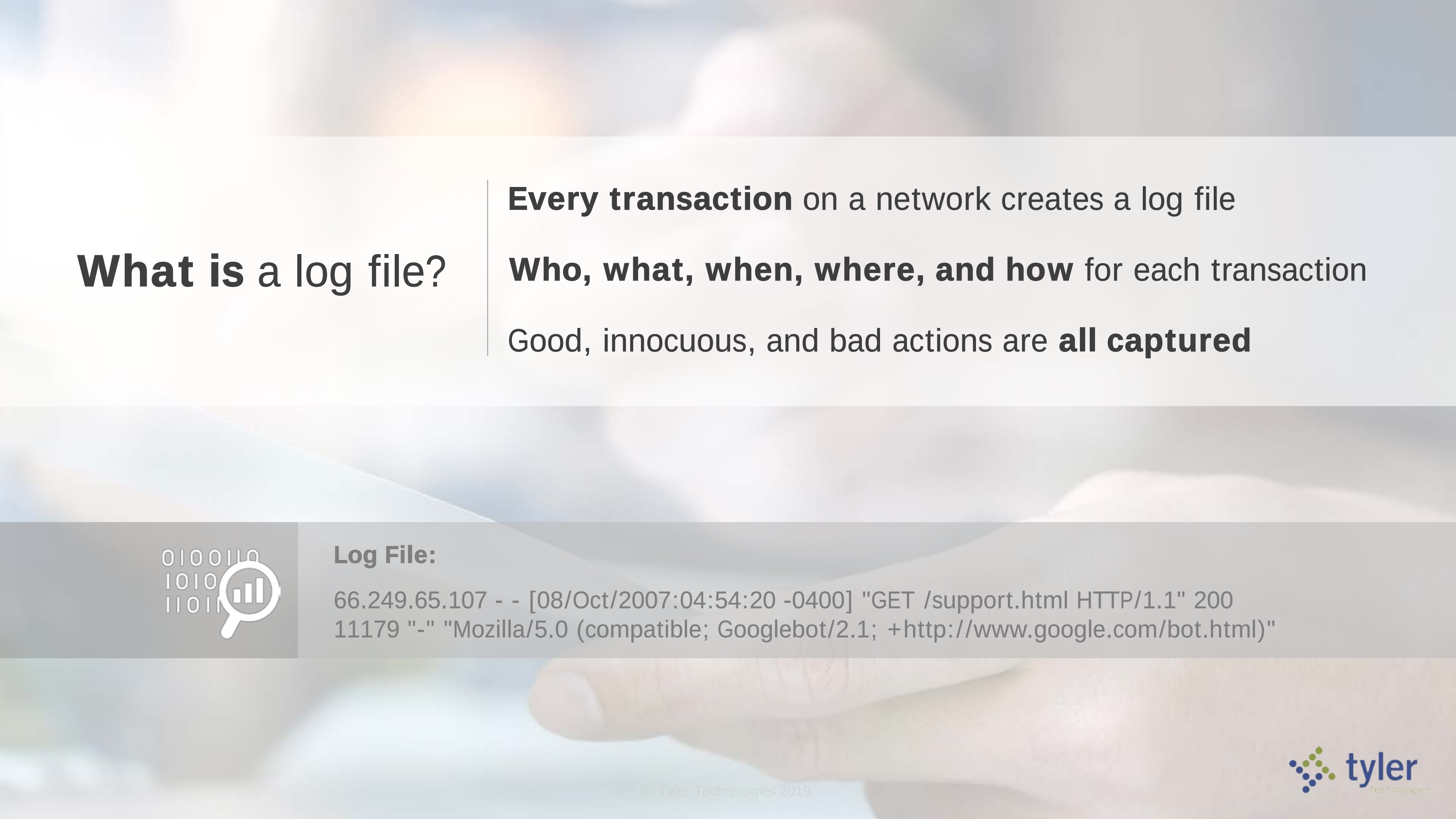
Malware | Zero-Day Exploits | Ransomware | Insider Threats | Compliance Violations | Errant Admin. Activity

No costly hardware

Security events **streamed in real-time**

Human experts investigating

tyler technologies



What is a log file?

Every transaction on a network creates a log file

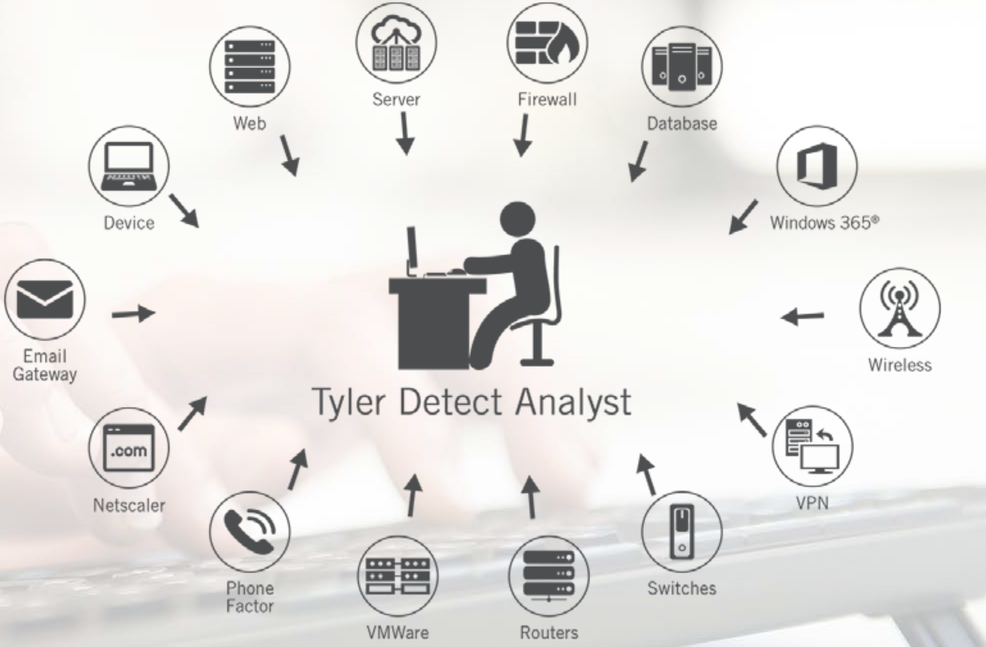
Who, what, when, where, and how for each transaction

Good, innocuous, and bad actions are **all captured**

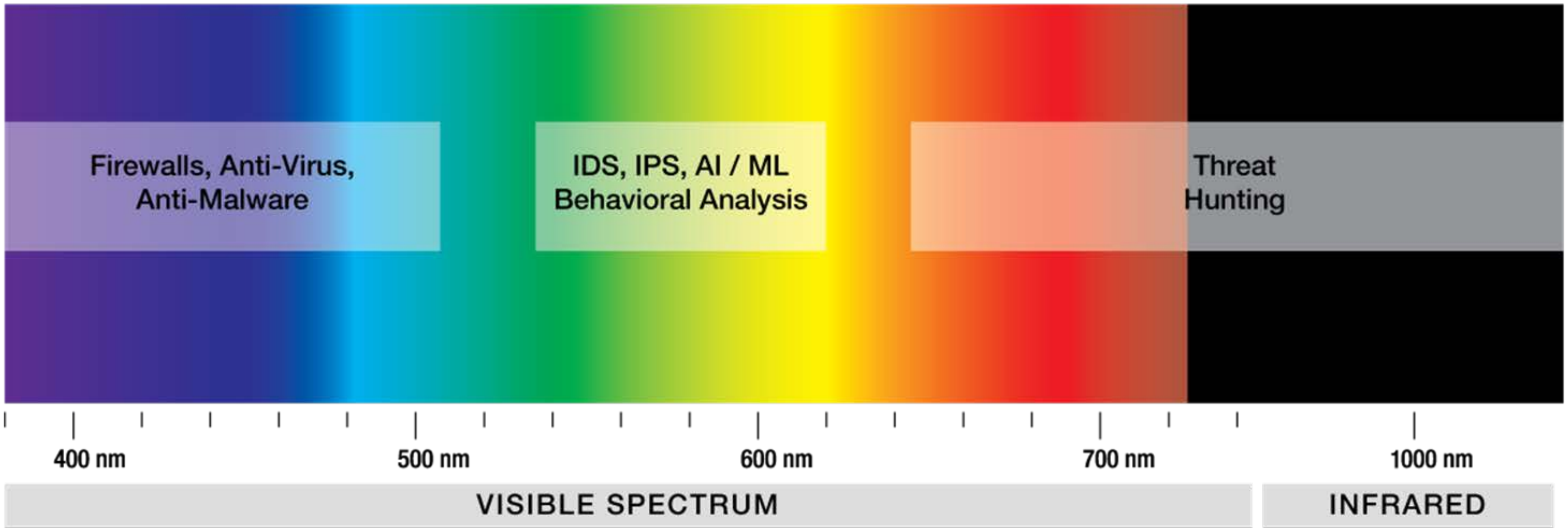
Log File:

```
66.249.65.107 - - [08/Oct/2007:04:54:20 -0400] "GET /support.html HTTP/1.1" 200
11179 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
```

We monitor everything
– not just Tyler apps



Threat spectrum


Firewalls, Anti-Virus, Anti-Malware
IDS, IPS, AI / ML Behavioral Analysis
Threat Hunting
400 nm
500 nm
600 nm
700 nm
1000 nm
VISIBLE SPECTRUM
INFRARED

Daily **report**

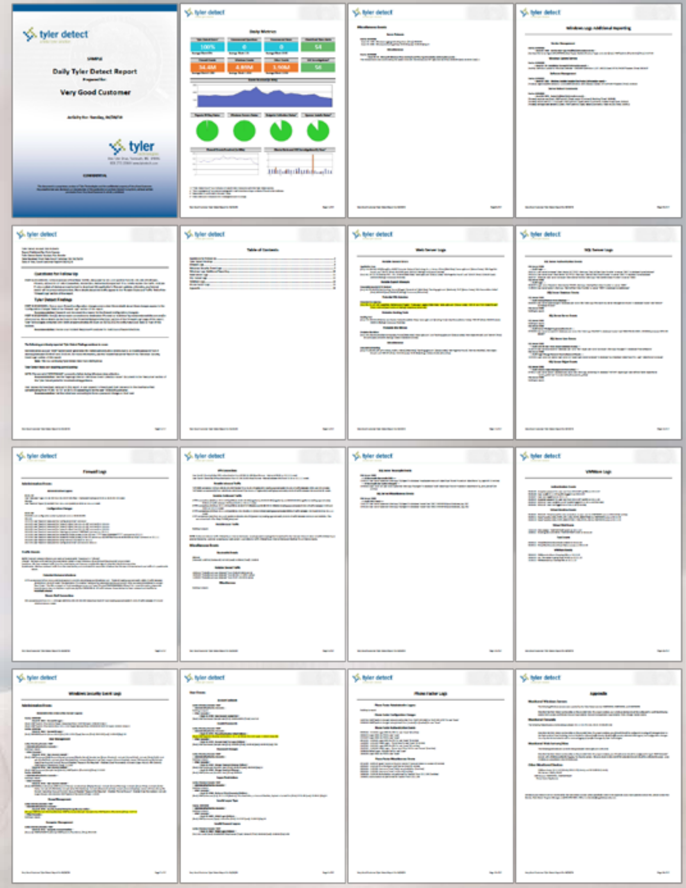
Reports published each business day

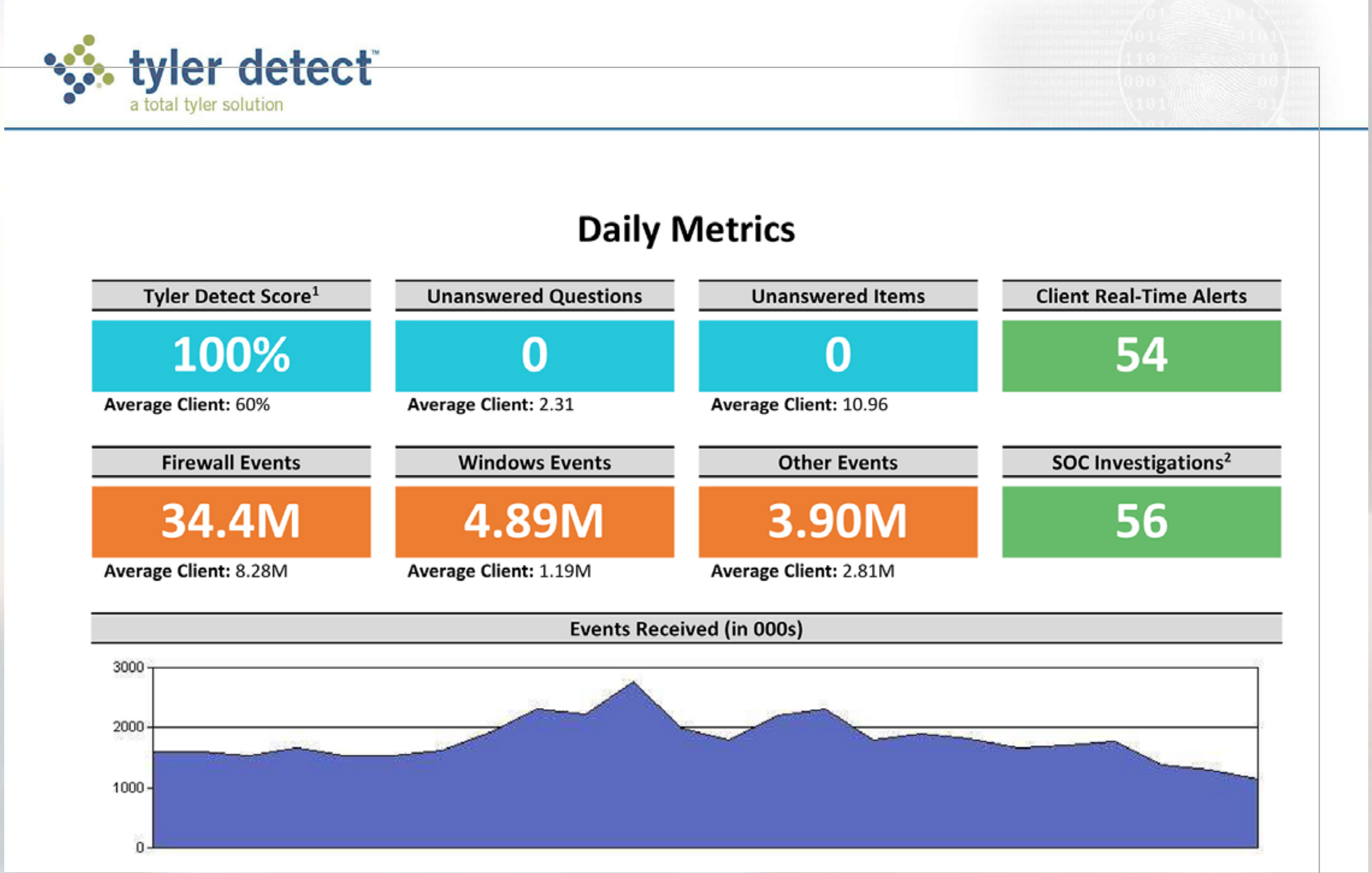
Critical log data for 24-hour period

Consolidated view of activity

Secure and documented **audit trail** for compliance

Summarized monthly reports that auditors love!





tyler detect™

a total tyler solution

Daily Metrics

Tyler Detect Score[1]	Unanswered Questions	Unanswered Items	Client Real-Time Alerts
100%	0	0	54
Average Client: 60%	**Average Client:** 2.31	**Average Client:** 10.96	

Firewall Events	Windows Events	Other Events	SOC Investigations[2]
34.4M	4.89M	3.90M	56
Average Client: 8.28M	**Average Client:** 1.19M	**Average Client:** 2.81M	

Events Received (in 000s)

Daily report **contents**

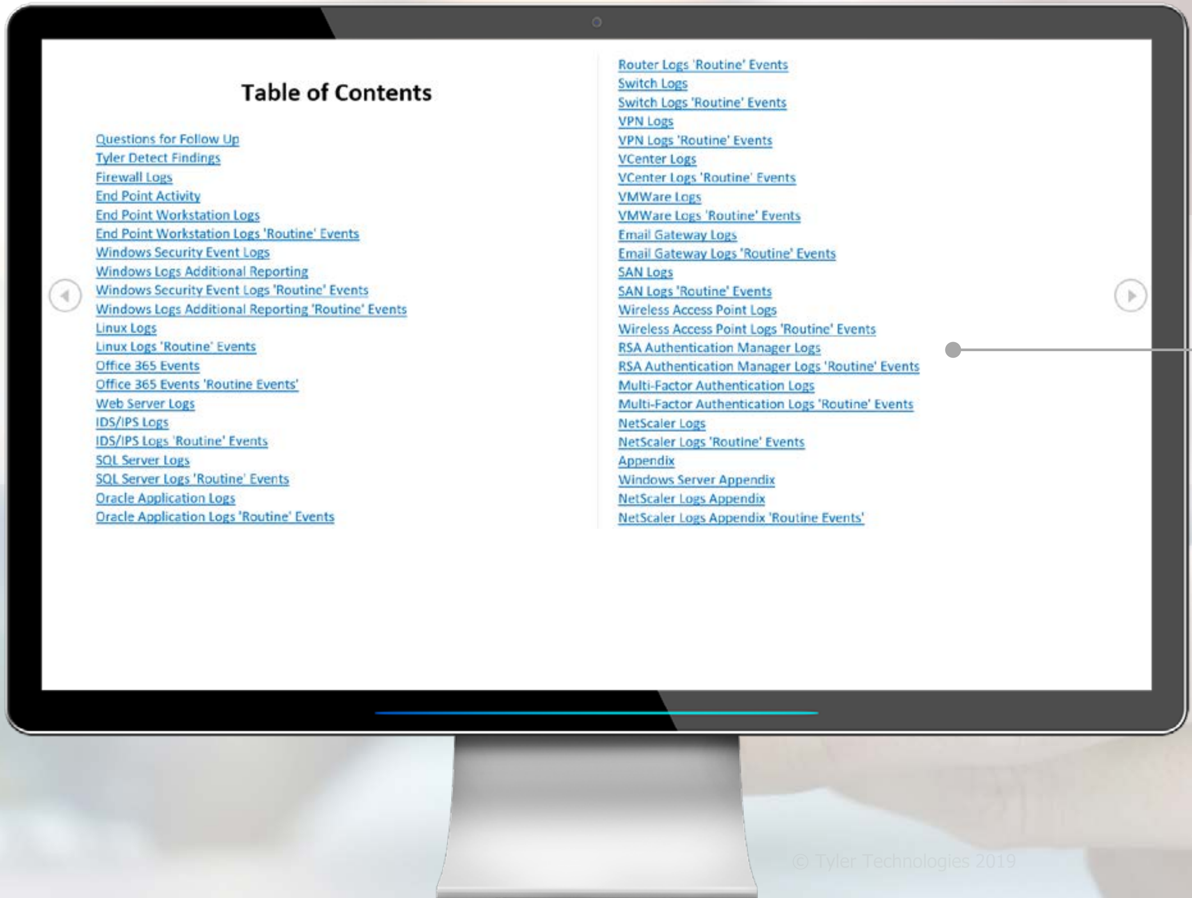


Table of Contents

- Questions for Follow Up
- Tyler Detect Findings
- Firewall Logs
- End Point Activity
- End Point Workstation Logs
- End Point Workstation Logs 'Routine' Events
- Windows Security Event Logs
- Windows Logs Additional Reporting
- Windows Security Event Logs 'Routine' Events
- Windows Logs Additional Reporting 'Routine' Events
- Linux Logs
- Linux Logs 'Routine' Events
- Office 365 Events
- Office 365 Events 'Routine Events'
- Web Server Logs
- IDS/IPS Logs
- IDS/IPS Logs 'Routine' Events
- SQL Server Logs
- SQL Server Logs 'Routine' Events
- Oracle Application Logs
- Oracle Application Logs 'Routine' Events
- Router Logs 'Routine' Events
- Switch Logs
- Switch Logs 'Routine' Events
- VPN Logs
- VPN Logs 'Routine' Events
- VCenter Logs
- VCenter Logs 'Routine' Events
- VMWare Logs
- VMWare Logs 'Routine' Events
- Email Gateway Logs
- Email Gateway Logs 'Routine' Events
- SAN Logs
- SAN Logs 'Routine' Events
- Wireless Access Point Logs
- Wireless Access Point Logs 'Routine' Events
- RSA Authentication Manager Logs
- RSA Authentication Manager Logs 'Routine' Events
- Multi-Factor Authentication Logs
- Multi-Factor Authentication Logs 'Routine' Events
- NetScaler Logs
- NetScaler Logs 'Routine' Events
- Appendix
- Windows Server Appendix
- NetScaler Logs Appendix
- NetScaler Logs Appendix 'Routine Events'

Click and view

Real-time **alerts**

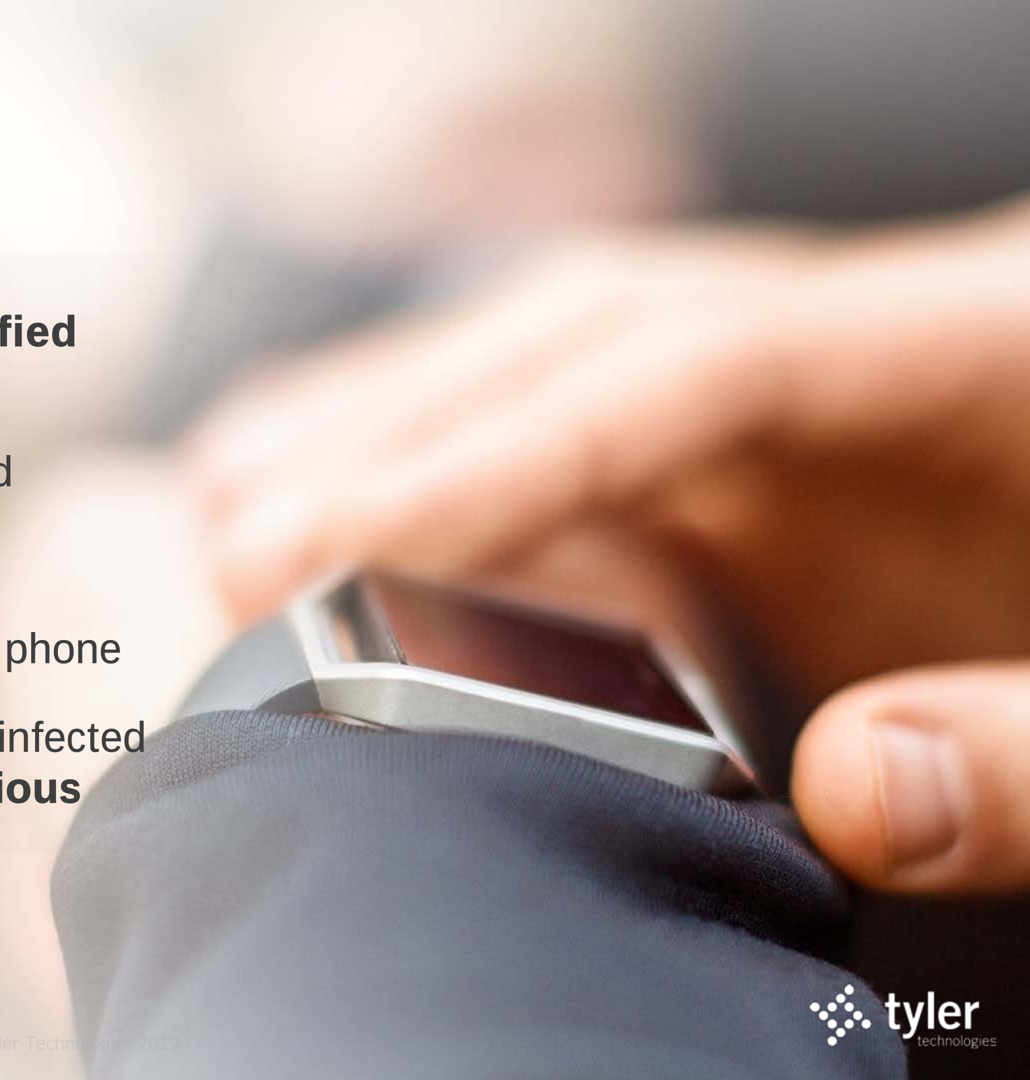
Unique and suspicious **activity is identified and confirmed**

Detailed notifications of what occurred

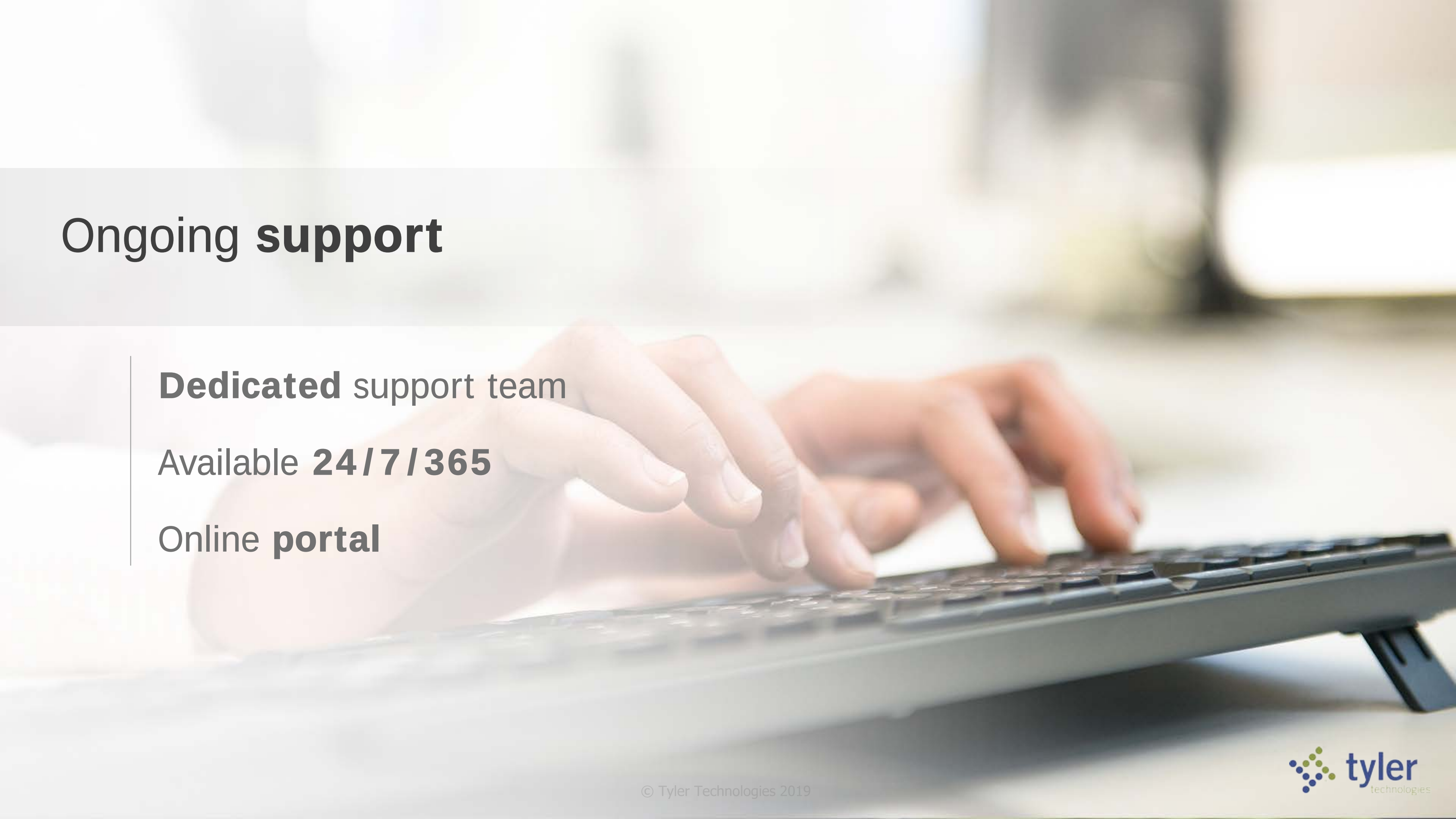
Customizable **alerts**

Malware threats are communicated by phone

Customers can authorize Tyler to disable infected Windows computers to **mitigate suspicious activity**



Ongoing **support**

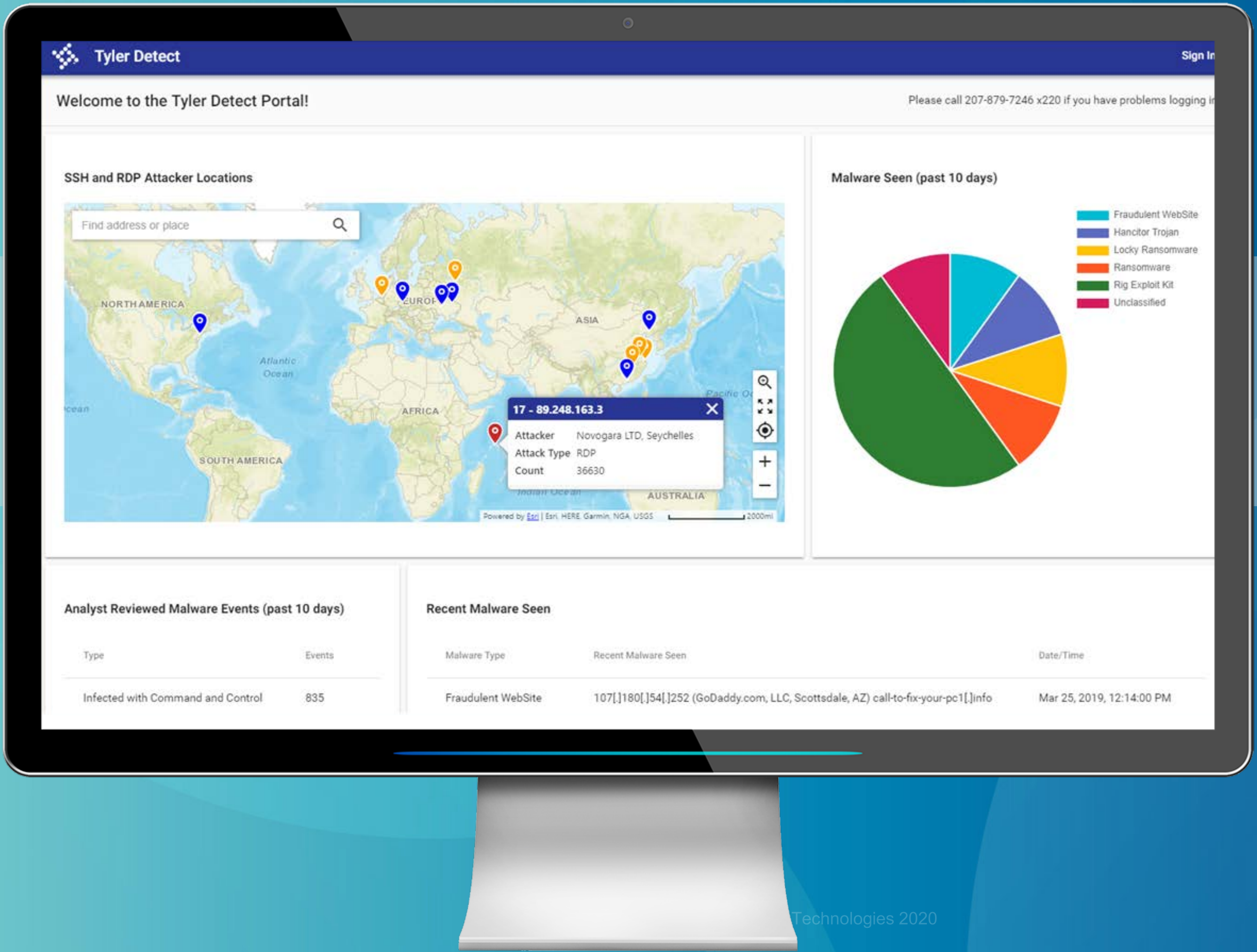


Dedicated support team

Available **24/7/365**

Online **portal**

Landing page



Tyler Detect

Sign In

Welcome to the Tyler Detect Portal!

Please call 207-879-7246 x220 if you have problems logging i

SSH and RDP Attacker Locations

Find address or place

17 - 89.248.163.3	
Attacker	Novogara LTD, Seychelles
Attack Type	RDP
Count	36630

Malware Seen (past 10 days)

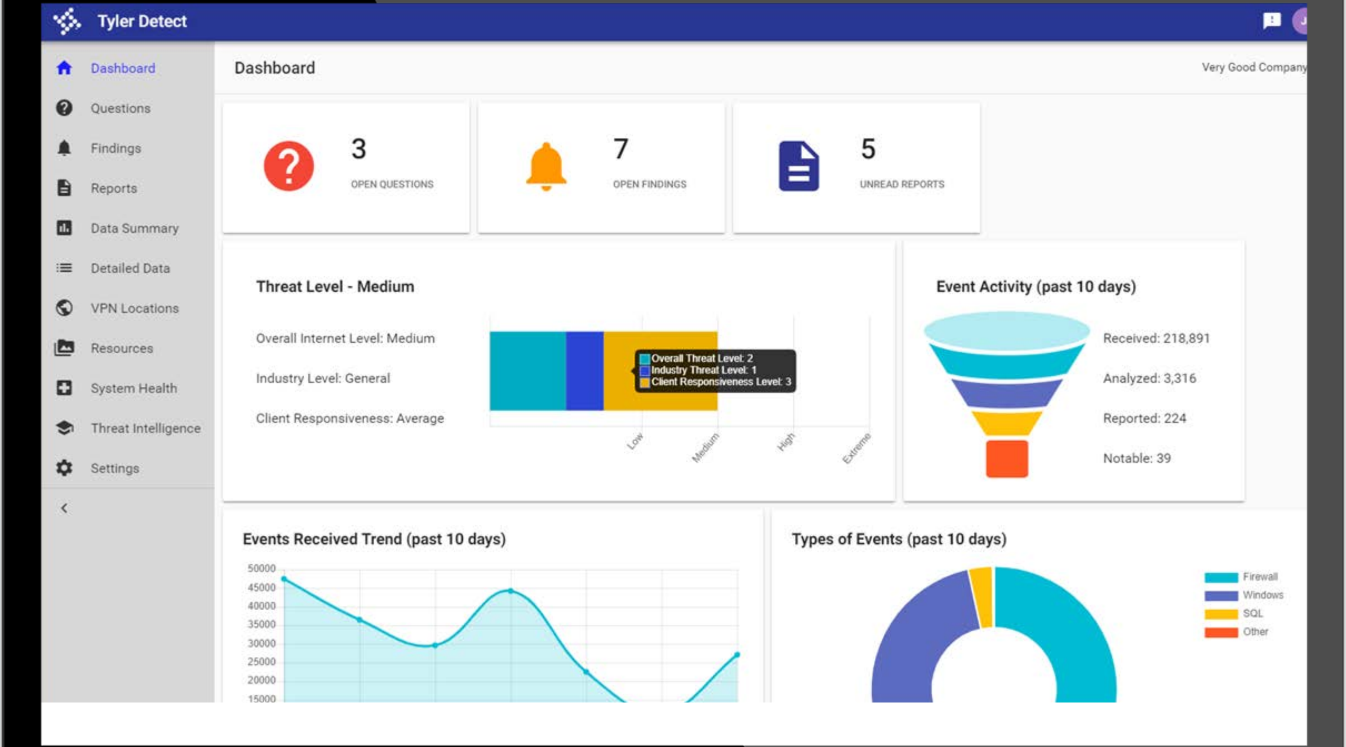
Analyst Reviewed Malware Events (past 10 days)

Type	Events
Infected with Command and Control	835

Recent Malware Seen

Malware Type	Recent Malware Seen	Date/Time
Fraudulent WebSite	107[.]180[.]54[.]252 (GoDaddy.com, LLC, Scottsdale, AZ) call-to-fix-your-pc1[.]info	Mar 25, 2019, 12:14:00 PM

Customizable home page



Tyler Detect

- Dashboard
- Questions
- Findings
- Reports
- Data Summary
- Detailed Data
- VPN Locations
- Resources
- System Health
- Threat Intelligence
- Settings

Dashboard

Very Good Company

3 OPEN QUESTIONS

7 OPEN FINDINGS

5 UNREAD REPORTS

Threat Level - Medium

Overall Internet Level: Medium

Industry Level: General

Client Responsiveness: Average

🟦 Overall Threat Level: 2
🟦 Industry Threat Level: 1
🟨 Client Responsiveness Level: 3

Event Activity (past 10 days)

Received: 218,891

Analyzed: 3,316

Reported: 224

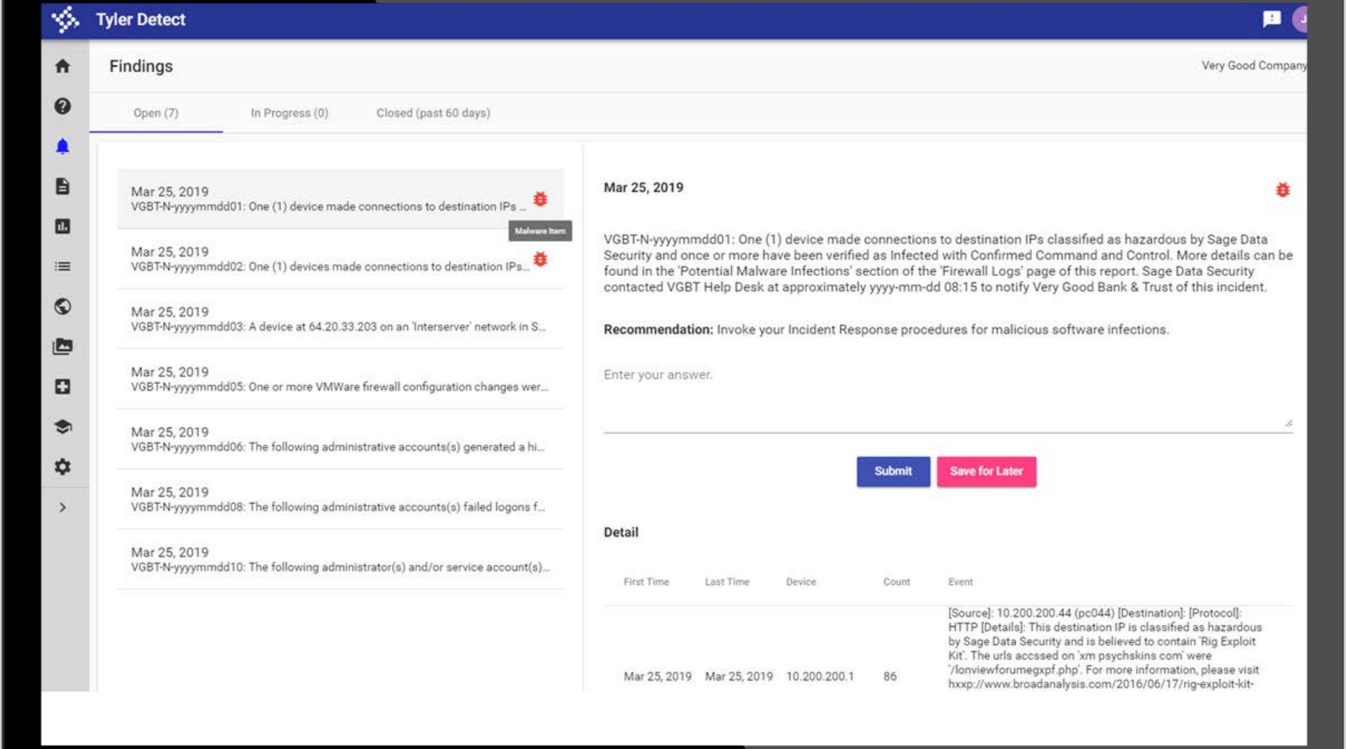
Notable: 39

Events Received Trend (past 10 days)

Types of Events (past 10 days)

🟦 Firewall
🟦 Windows
🟨 SQL
🟥 Other

Finding with details



Mar 25, 2019
VGBT-N-yyyymmdd01: One (1) device made connections to destination IPs ...

Mar 25, 2019
VGBT-N-yyyymmdd02: One (1) devices made connections to destination IPs...

Mar 25, 2019
VGBT-N-yyyymmdd03: A device at 64.20.33.203 on an 'Interserver' network in S...

Mar 25, 2019
VGBT-N-yyyymmdd05: One or more VMWare firewall configuration changes wer...

Mar 25, 2019
VGBT-N-yyyymmdd06: The following administrative accounts(s) generated a hi...

Mar 25, 2019
VGBT-N-yyyymmdd08: The following administrative accounts(s) failed logons f...

Mar 25, 2019
VGBT-N-yyyymmdd10: The following administrator(s) and/or service account(s)...

Mar 25, 2019

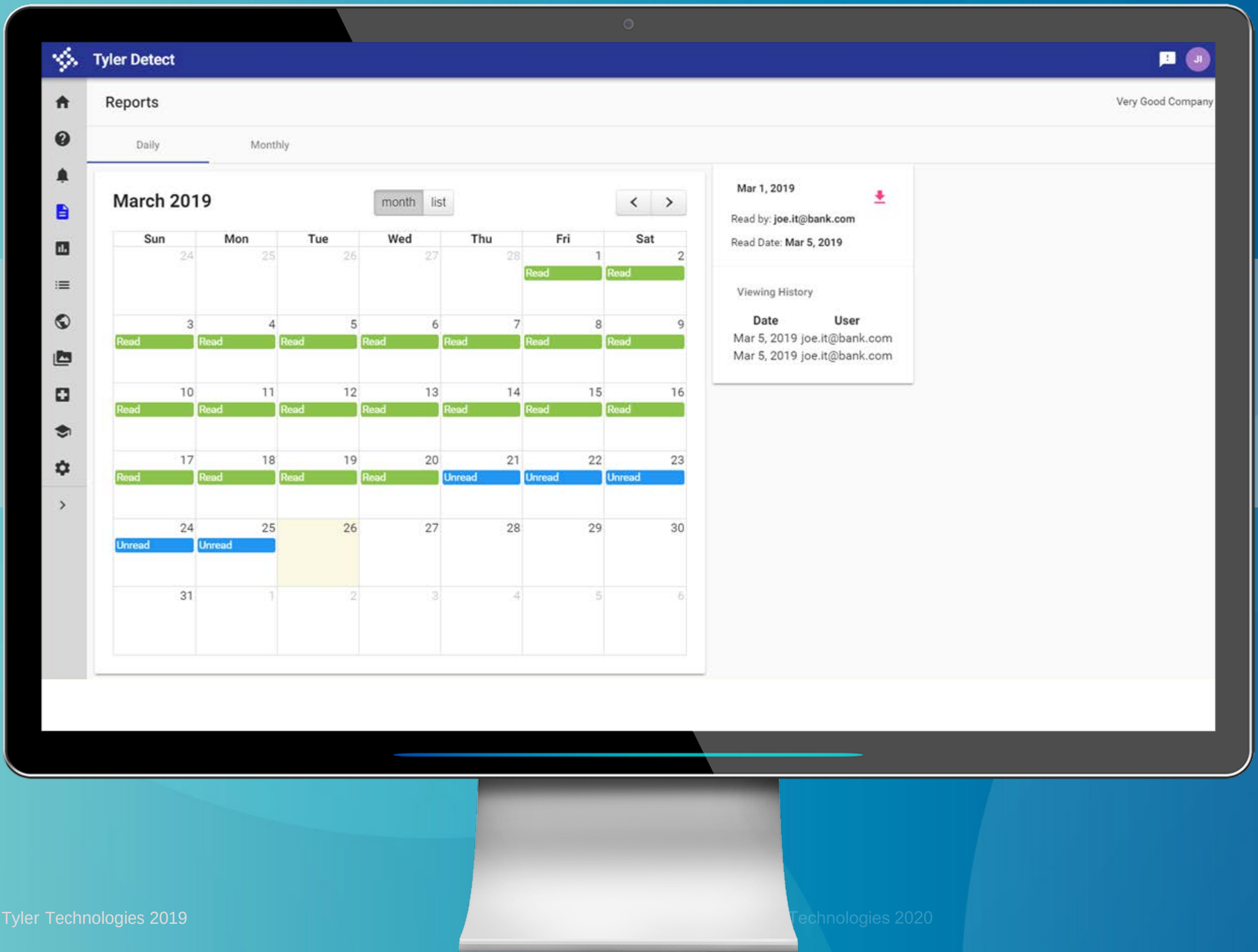
VGBT-N-yyyymmdd01: One (1) device made connections to destination IPs classified as hazardous by Sage Data Security and once or more have been verified as Infected with Confirmed Command and Control. More details can be found in the 'Potential Malware Infections' section of the 'Firewall Logs' page of this report. Sage Data Security contacted VGBT Help Desk at approximately yyyy-mm-dd 08:15 to notify Very Good Bank & Trust of this incident.

Recommendation: Invoke your Incident Response procedures for malicious software infections.

Enter your answer.

Detail

First Time	Last Time	Device	Count	Event
Mar 25, 2019	Mar 25, 2019	10.200.200.1	86	[Source]: 10.200.200.44 (pc044) [Destination]: [Protocol]: HTTP [Details]: This destination IP is classified as hazardous by Sage Data Security and is believed to contain 'Rig Exploit Kit'. The urls accssed on 'xm psychskins com' were '/lonviewforumegxpf.php'. For more information, please visit hxxp://www.broadanalysis.com/2016/06/17/rig-exploit-kit-



Tyler Detect

Reports

Very Good Company

Daily

Monthly

March 2019

month list

Sun	Mon	Tue	Wed	Thu	Fri	Sat
24	25	26	27	28	1 Read	2 Read
3 Read	4 Read	5 Read	6 Read	7 Read	8 Read	9 Read
10 Read	11 Read	12 Read	13 Read	14 Read	15 Read	16 Read
17 Read	18 Read	19 Read	20 Read	21 Unread	22 Unread	23 Unread
24 Unread	25 Unread	26	27	28	29	30
31	1	2	3	4	5	6

Mar 1, 2019

Read by: joe.it@bank.com

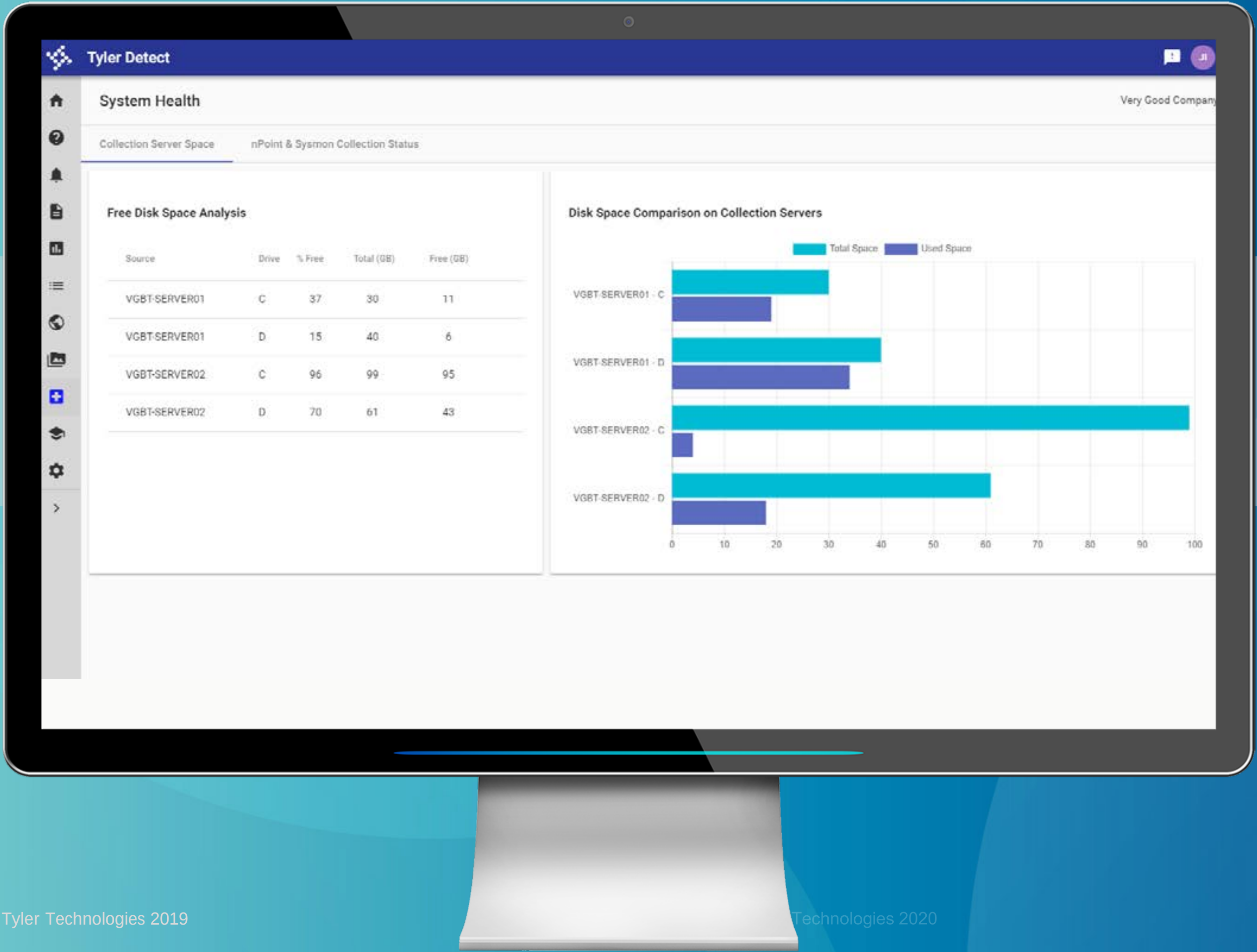
Read Date: Mar 5, 2019

Viewing History

Date	User
Mar 5, 2019	joe.it@bank.com
Mar 5, 2019	joe.it@bank.com

Reports with customizable views

System **health**



Tyler Detect

System Health

Very Good Company

Collection Server Space

nPoint & Sysmon Collection Status

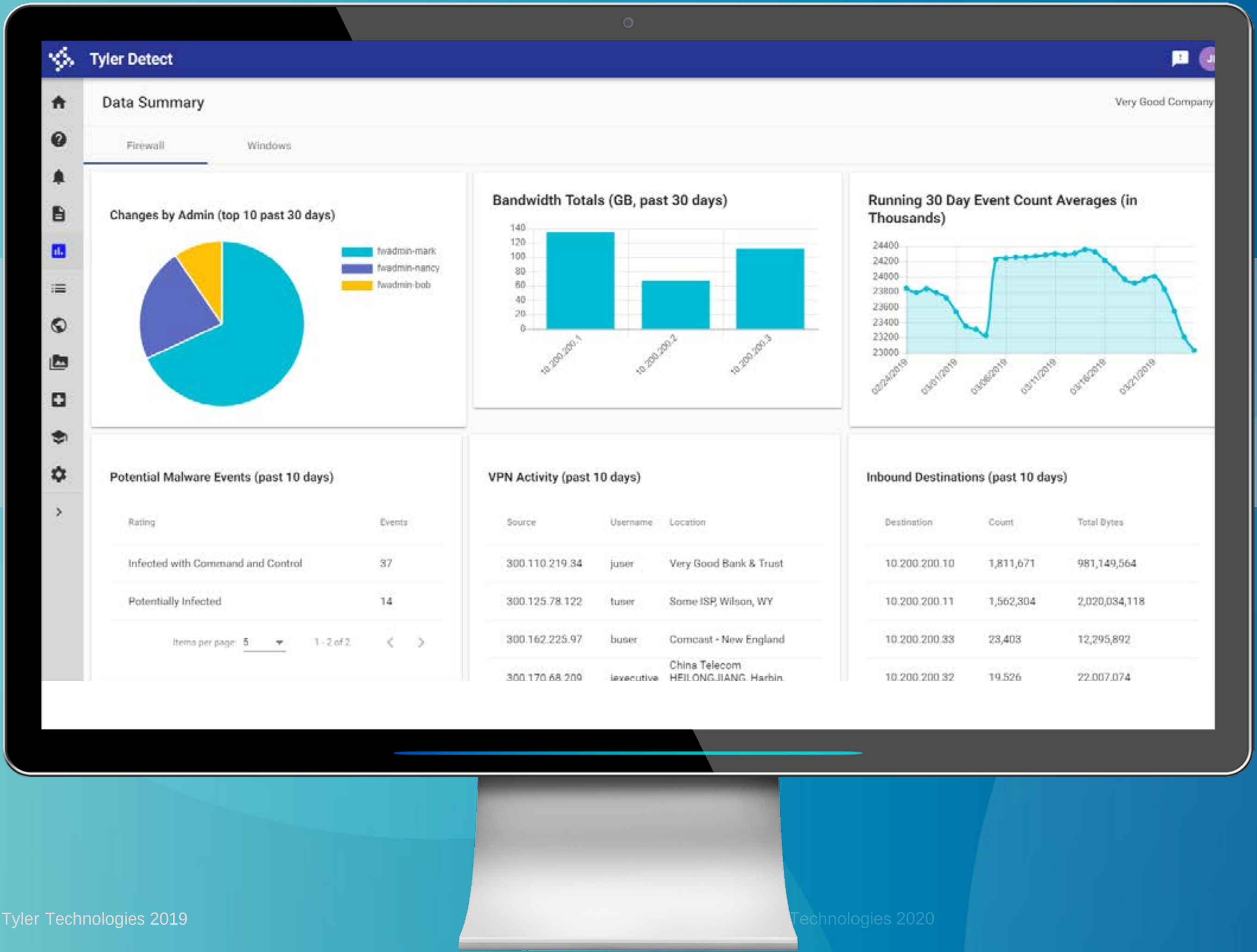
Free Disk Space Analysis

Source	Drive	% Free	Total (GB)	Free (GB)
VGBT-SERVER01	C	37	30	11
VGBT-SERVER01	D	15	40	6
VGBT-SERVER02	C	96	99	95
VGBT-SERVER02	D	70	61	43

Disk Space Comparison on Collection Servers

Technologies 2020

Firewall **activity**



Data Summary

Very Good Company

Changes by Admin (top 10 past 30 days)

Bandwidth Totals (GB, past 30 days)

Running 30 Day Event Count Averages (in Thousands)

Potential Malware Events (past 10 days)

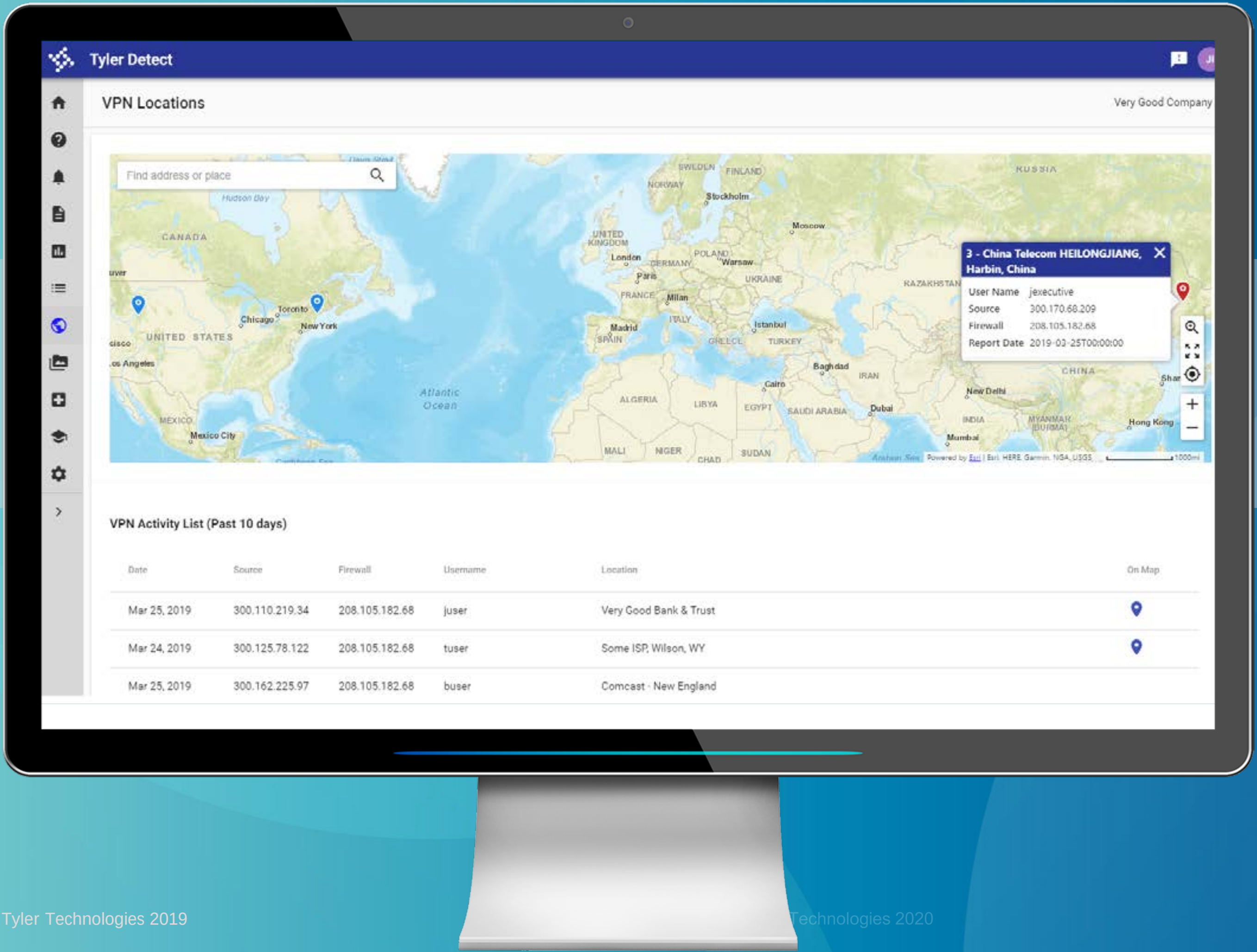
Rating	Events
Infected with Command and Control	37
Potentially Infected	14

VPN Activity (past 10 days)

Source	Username	Location
300.110.219.34	juser	Very Good Bank & Trust
300.125.78.122	tuser	Some ISP, Wilson, WY
300.162.225.97	buser	Comcast - New England
300.170.68.209	jexecutive	China Telecom HEILONGJIANG, Harbin

Inbound Destinations (past 10 days)

Destination	Count	Total Bytes
10.200.200.10	1,811,671	981,149,564
10.200.200.11	1,562,304	2,020,034,118
10.200.200.33	23,403	12,295,892
10.200.200.32	19,526	22,007,074



VPN Locations

Very Good Company

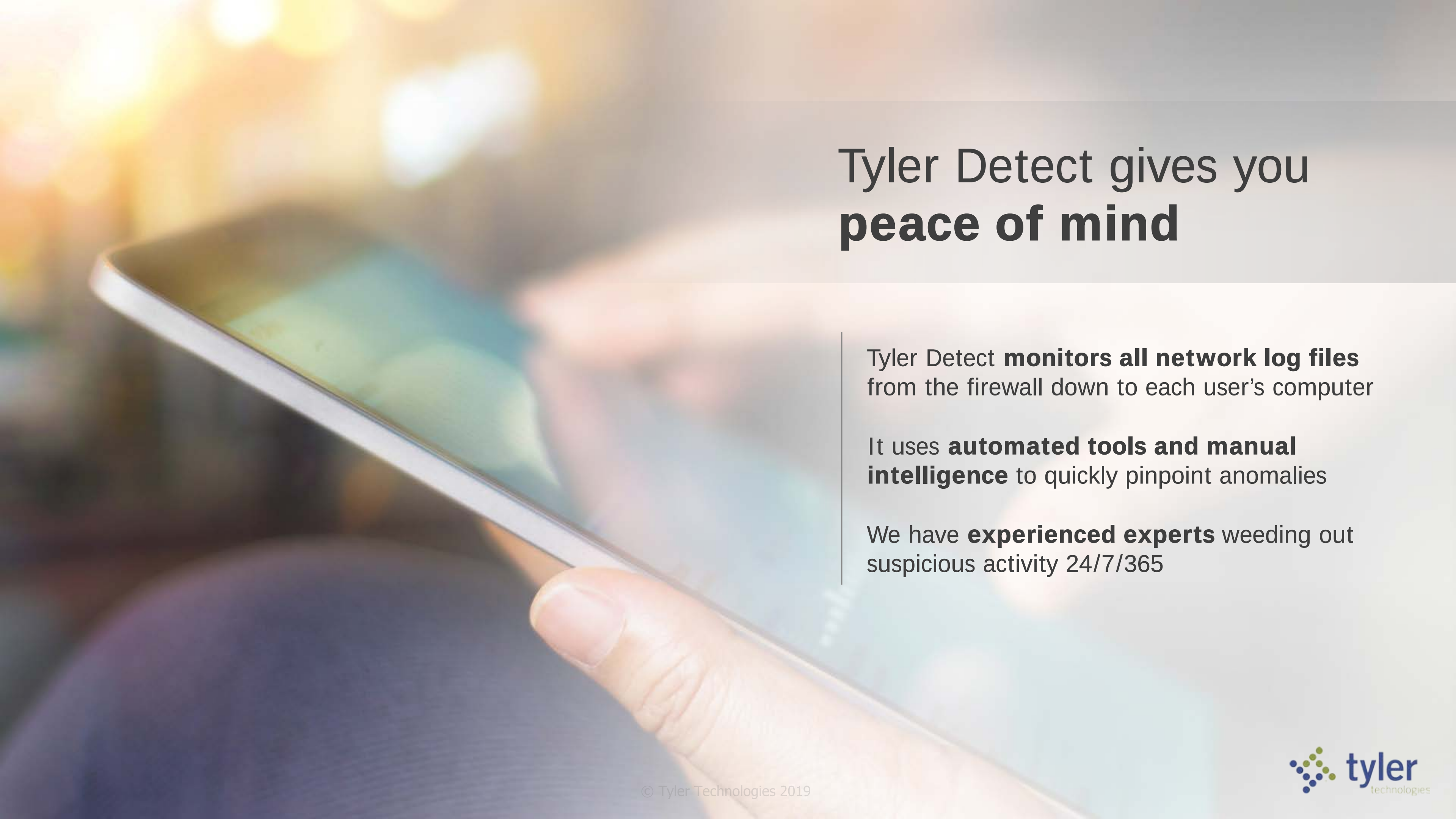
3 - China Telecom HEILONGJIANG, Harbin, China

User Name	jexecutive
Source	300.170.68.209
Firewall	208.105.182.68
Report Date	2019-03-25T00:00:00

VPN Activity List (Past 10 days)

Date	Source	Firewall	Username	Location	On Map
Mar 25, 2019	300.110.219.34	208.105.182.68	juser	Very Good Bank & Trust	●
Mar 24, 2019	300.125.78.122	208.105.182.68	tuser	Some ISP, Wilson, WY	●
Mar 25, 2019	300.162.225.97	208.105.182.68	buser	Comcast - New England	

Map of **VPN locations**



Tyler Detect gives you **peace of mind**

Tyler Detect **monitors all network log files** from the firewall down to each user's computer

It uses **automated tools and manual intelligence** to quickly pinpoint anomalies

We have **experienced experts** weeding out suspicious activity 24/7/365

Mike Caffrey
Blount County, TN

“With Tyler Detect, I feel like I have a team working around the clock to uncover all those things I didn’t know before.”

Laurie Gagner, City of Sunrise, FL

“We are VERY happy with the results from Tyler Detect. Having trusted humans monitoring our logs in real-time is invaluable. Yes it’s an investment in time and dollars, but it’s way less costly than being forced to react after something bad happens.”

Aaron Kostyu
Director of Technology
Lowndes County, GA

“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. My awareness of my network has increased 80%. Knowing that it is also monitoring my traffic 24/7 for any deviant behavior is an added bonus that gives me and the county’s management team a strong sense of comfort.”

Installation

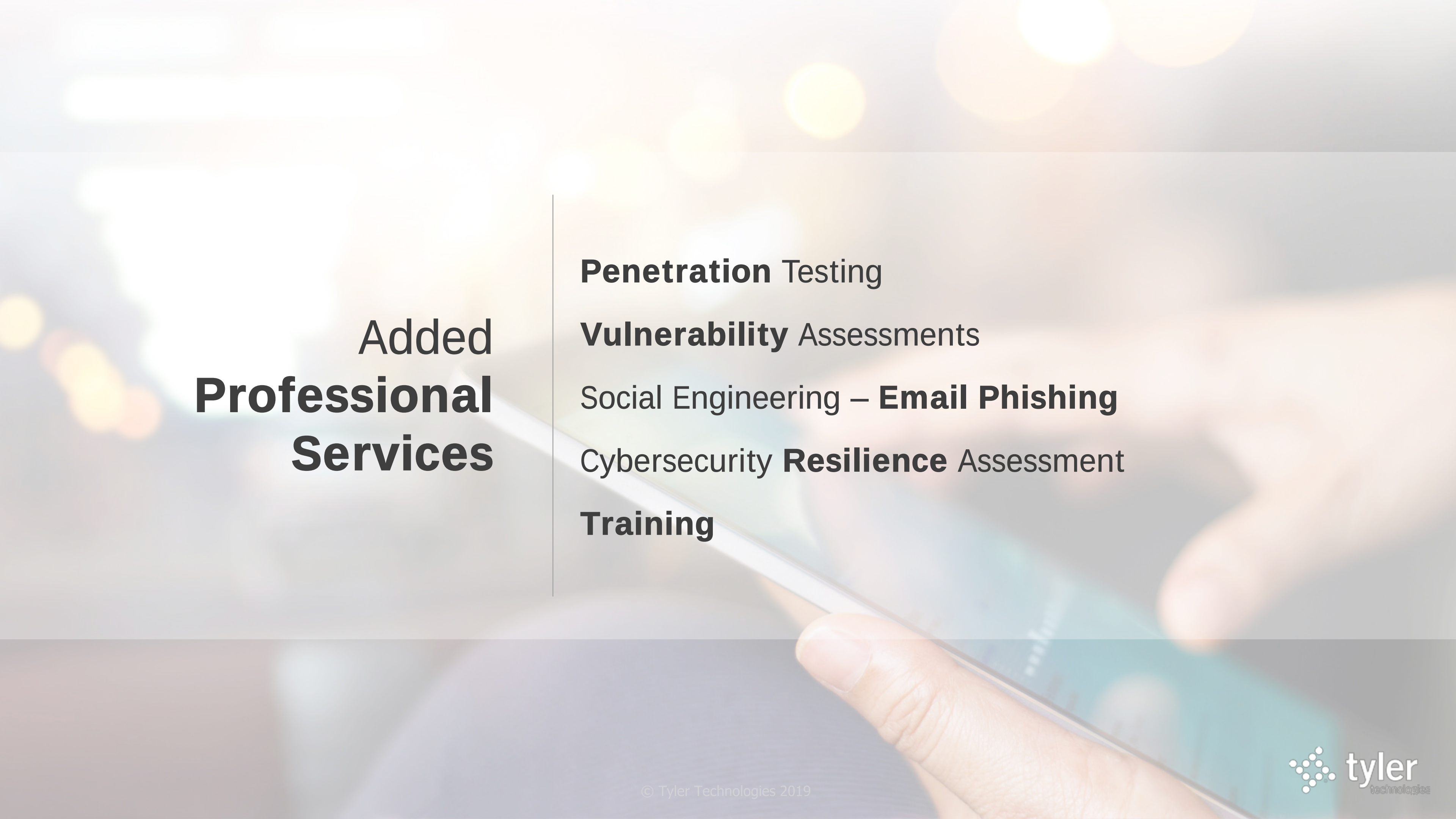
Annual **subscription**

Light and nimble **deployment**

Handful of scripts and stored procedures for **log collection**

Kiwi application **user license**

Negligible performance **impact to your system**



Added **Professional Services**

Penetration Testing

Vulnerability Assessments

Social Engineering – **Email Phishing**

Cybersecurity **Resilience** Assessment

Training

We’re here for **you**

Karen Grosset

Karen.grosset@tylertech.com

800-772-2260 x4222

Empowering people who serve the public®

tyler technologies

tylertech.com