

RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: SPO2-W10

Simplicity from Complexity: Cybersecurity Insights That Matter Most

Leah MacMillan

Senior VP, Global Marketing
Trend Micro

#RSAC

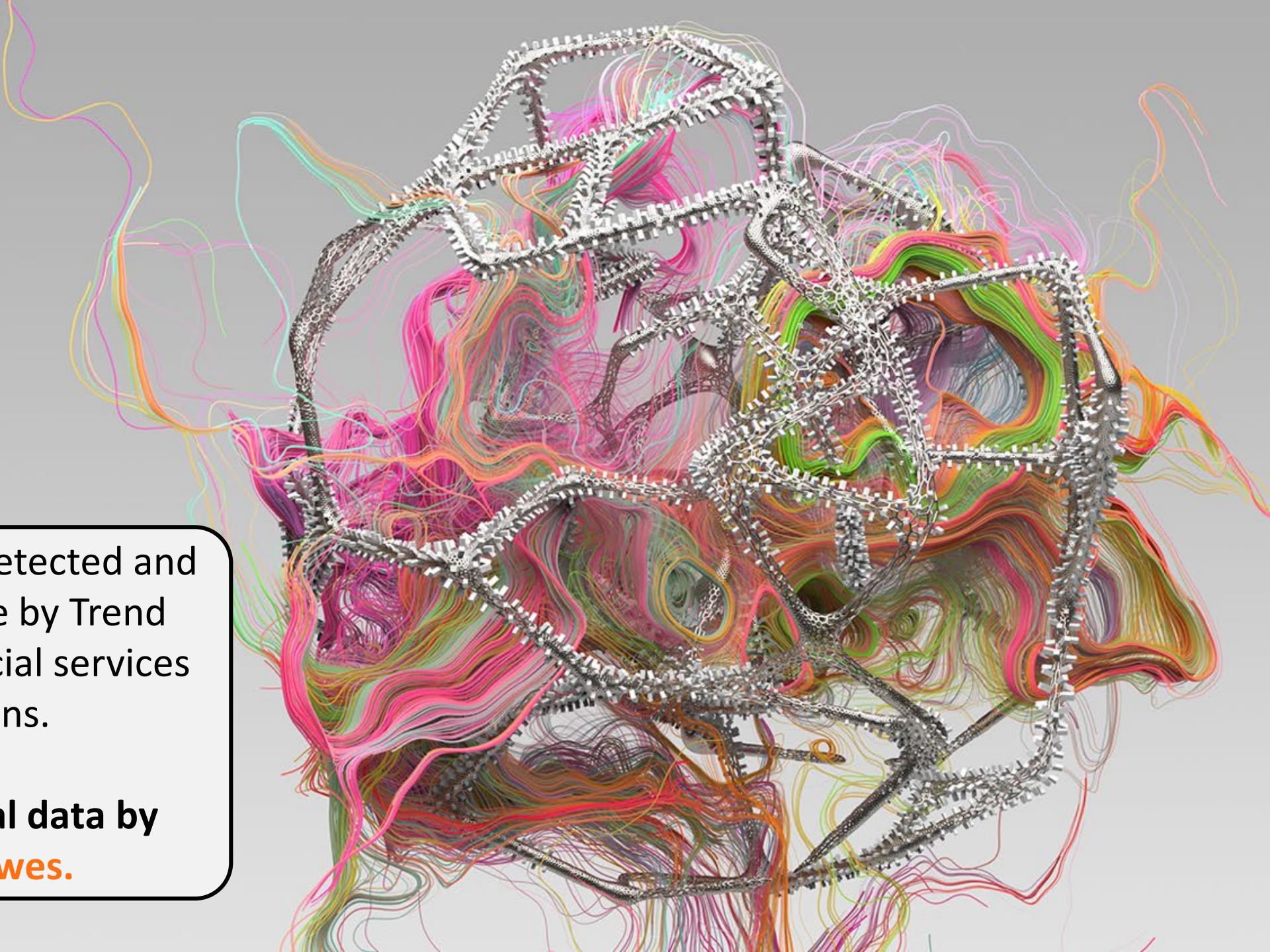
“Apply” Slide

- Learn how global threats are impacting IT, including cloud & IoT
- Consider strategies for gaining meaningful visibility
- Think differently about addressing the skills and gender gap in cybersecurity

- Art
- Data
- Both

Unknown threats detected and stopped over time by Trend Micro within financial services organizations.

**Created with real data by
Brendan Dawes.**





Cloud becomes the norm, even for laggards

Augmentation through AI

Digital transformation becomes table stakes



New and emerging technologies help compete for customers, partners *and* talent

But cyber attacks are preventing organizations from being their best

2018 saw a 16% YoY increase in '**mega breaches**'



Heightened Risk in 2019

A photograph of a man and a woman sitting at a desk, looking intently at a computer monitor. The woman is in the foreground, her hand near her mouth in a shocked or worried expression. The man is behind her, also looking at the screen. The background is blurred green foliage.

Enterprises believe
Businesses will be
targeted by cyberattackers
as more than half of CIOs expect
their organizations to be hit by a cyberattack
in the next 12 months.

Heightened Risk in 2019

99.99% of exploit-based attacks will be AI to predict movements of Cybercriminals will use normal computing objects to **blend in** (hotels, routes, flights, preferences, etc.)



Heightened Risk in 2019



**Faster response demanded
Heavier fines
More oversight**

Let's face it, threats are ugly!

1,658,148 events (8/26/15 10:33:00.000 AM to 8/26/15 11:33:37.000 AM)		
Events (1,658,148) Statistics Visualization		
Format Timeline ▾ <input checked="" type="radio"/> Zoom Out <input type="radio"/> Zoom to Selection <input type="radio"/> Deselect 1 minute per column		
Show Fields List ▾ Format ▾ 50 Per Page ▾		
i	Time	Event
▶	8/26/15 11:33:36	10.1.221.3 TW-IWSVABC03: <Wed, 26 Aug 2015 11:33:36,CST> [EVT_URL_ACCESS_TRACKING LOG_INFO] Access tracking log tk_username=10.1.200.93,tk_ur
	host = 10.1.221.3 tk_url = https://dc1.twops.co/	
▶	8/26/15 11:33:36	10.1.221.3 TW-IWSVABC03: <Wed, 26 Aug 2015 11:33:36,CST> [EVT_URL_ACCESS_TRACKING LOG_INFO] Access tracking log tk_username=10.1.185.161,tk_ur
	host = 10.1.221.3 tk_url = http://217.146.21.6/dout.aspx?s=22241030	
▶	8/26/15 11:33:36	10.1.221.1 TW-IWSVABC01: <Wed, 26 Aug 2015 11:33:35,CST> [EVT_URL_ACCESS_TRACKING LOG_INFO] Access tracking log tk_username=10.1.224.132,tk_ur
	host = 10.1.221.1 tk_url = http://37.252.246.3/dout.aspx?s=47796908	
▶	8/26/15 11:33:36	10.1.221.1 TW-IWSVABC01: <Wed, 26 Aug 2015 11:33:35,CST> [EVT_URL_ACCESS_TRACKING LOG_INFO] Access tracking log tk_username=10.1.228.186,tk_ur
	host = 10.1.221.1 tk_url = http://www.chinatimes.com/images/chinagroup_logo_80x80.gif	
▶	8/26/15 11:33:36	10.1.2.17 TW-IWSVAA01: <Wed, 26 Aug 2015 11:33:35,CST> [EVT_URL_ACCESS_TRACKING LOG_INFO] Access tracking log tk_username=10.1.152.71,tk_ur
	host = 10.1.2.17 tk_url = http://oscell1.p.activeupdate.trendmicro.com/activeupdate/server.in	
▶	8/26/15 11:33:36	10.1.107.222 TW-IWSVAA03: <Wed, 26 Aug 2015 11:33:36,CST> [EVT_URL_ACCESS_TRACKING LOG_INFO] Access tracking log tk_username=10.1.106.197,tk_ur
	host = 10.1.107.222 tk_url = http://ddi38-en.url.trendmicro.com/T/152/90bwNJtyz1c0zQvELdnADTYmU-N-wSLc0vP5CH25T_vLWUV6NYLudHSOr3Go4htynoqXmuza-drcISgqygDbi804SZ0XKJ0v8cZoaqN4mcyeQppw90tNJRjC	
▶	8/26/15 11:33:36	10.1.221.3 TW-IWSVABC03: <Wed, 26 Aug 2015 11:33:36,CST> [EVT_URL_ACCESS_TRACKING LOG_INFO] Access tracking log tk_username=10.1.197.131,tk_ur
	host = 10.1.221.3 tk_url = http://92.51.156.76/din.aspx?s=18421609	
▶	8/26/15 11:33:36	10.1.2.18 TW-IWSVAA02: <Wed, 26 Aug 2015 11:33:35,CST> [EVT_URL_ACCESS_TRACKING LOG_INFO] Access tracking log tk_username=10.1.107.222,tk_ur
	host = 10.1.2.18 tk_url = http://ddi38-en.url.trendmicro.com/T/152/90bwNJtyz1c0zQvELdnADTYmU-N-wSLc0vP5CH25T_vLWUV6NYLudHSOr3Go4htynoqXmuza-drcISgqygDbi804SZ0XKJ0v8cZoaqN4mcyeQppw90tNJRjC	
▶	8/26/15 11:33:36	10.1.221.3 TW-IWSVABC03: <Wed, 26 Aug 2015 11:33:36,CST> [EVT_URL_ACCESS_TRACKING LOG_INFO] Access tracking log tk_username=10.1.230.173,tk_ur
	IWSVABC03,tk_client_ip=10.1.230.173,tk_server_ip=140.205.96.3,tk_domain=log.mmstat.com,tk_path=1.gif,tk_file_name=1.gif,tk_operation=POST,tk_uid=0259986263-S	
	host = 10.1.221.3 tk_url = http://log.mmstat.com/1.gif?logtype=1	

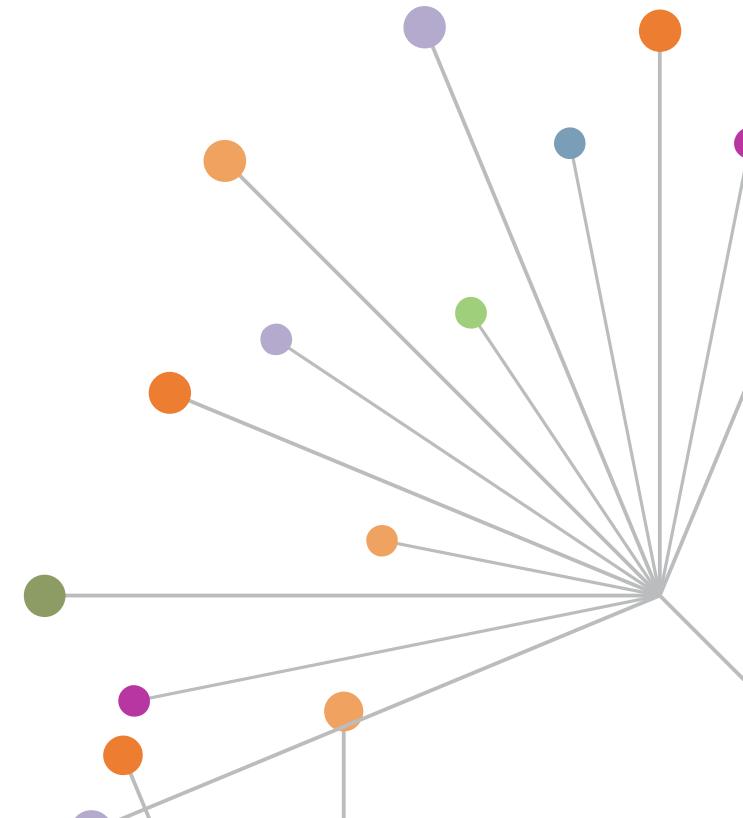
SHING ATTACK
9.2.7-5:14PM



CEDER MALWARE

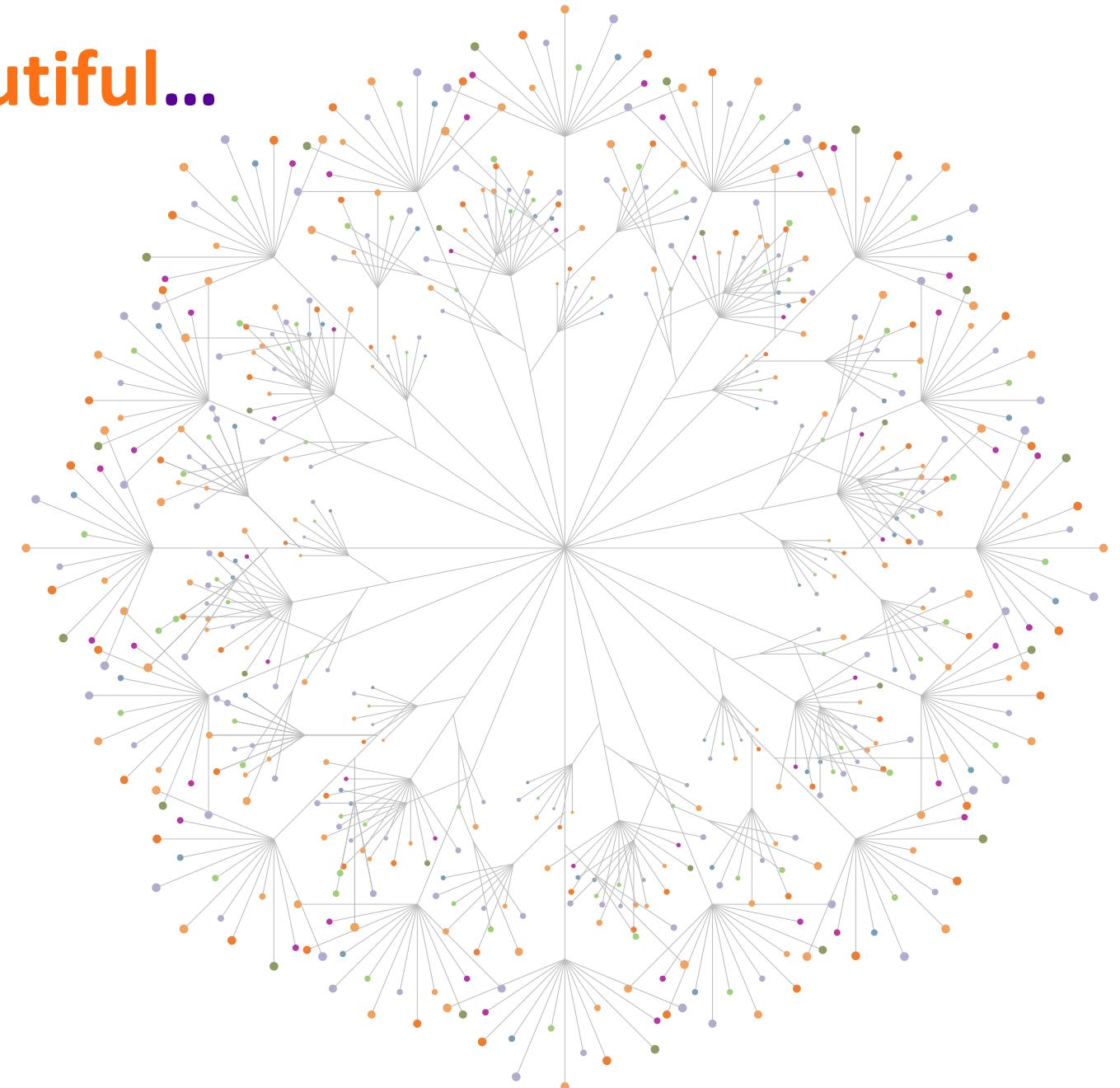
2019.2.5-8:01AM

BUT threats can be beautiful...



BUT threats can be beautiful...

**...when you can
SEE them!**

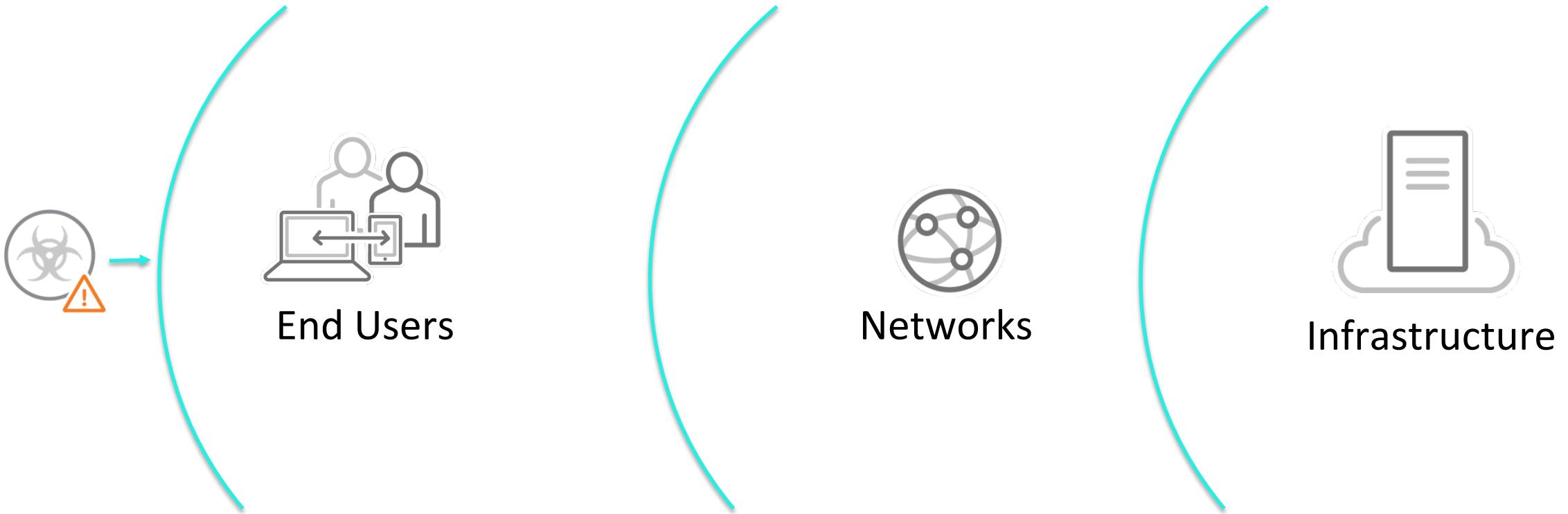


Why is it so hard to get meaningful visibility these days?



- Rapidly shifting IT environment
- Too many independent security tools
- Cybersecurity skills shortage

Growing Complexities at Every Layer



Users are More Mobile, Productive, Liberated

70% work remotely at least one day per week¹

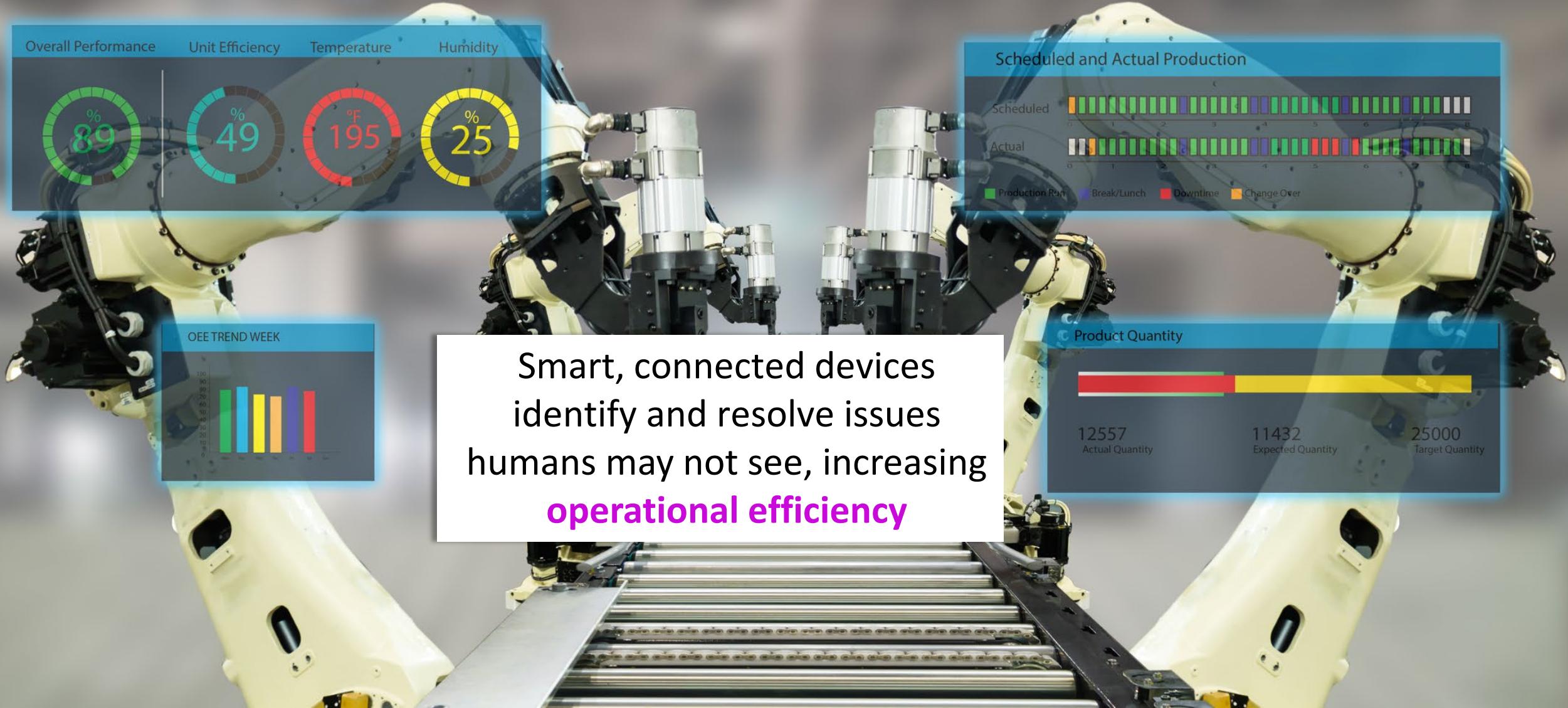
“BYOC” is the new “BYOD”

In 2019, 70% of MS Office users will be using Office 365²

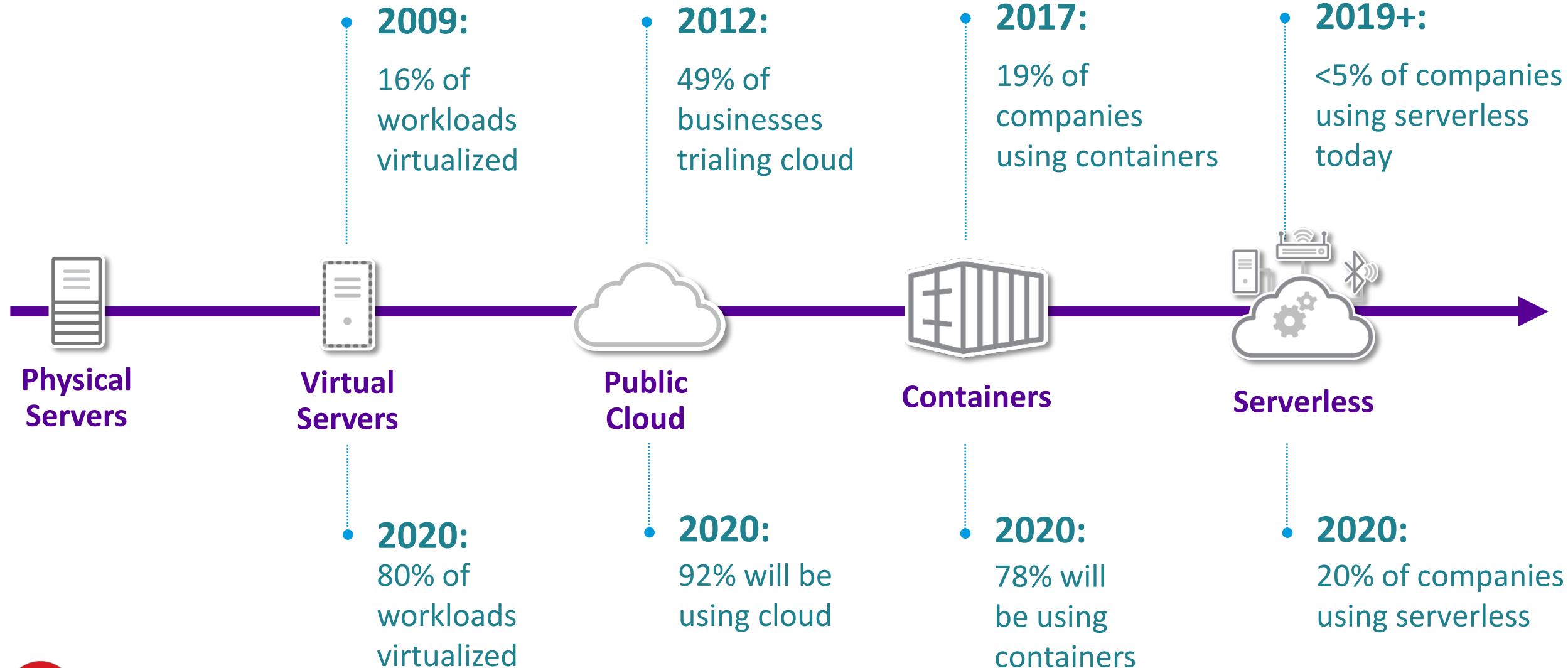


Office 365

Networks Now Include the Operational Technology (OT) Side of the Business



The Shift to Hybrid Cloud



DevOps: Build Quickly and Deploy Anywhere



69% of organizations are evaluating or piloting DevOps¹

Elite performers are updating applications **multiple times per day**, with changes/recovery in < hour²



1. Gartner S&R Summit, 2018; 2. "Accelerate: State of DevOps, Strategies for a New Economy", Dora, 2018

Too Many Tools, Siloed Across Layers



36% of organizations use between 25-49 individual security tools,
19% use 50+ products (ESG, Nov 2018)



Skills Shortage Increasing Risk and Affecting Job Satisfaction



3M
job openings

59% claim to be at extreme or moderate risk due to cybersecurity staff shortage

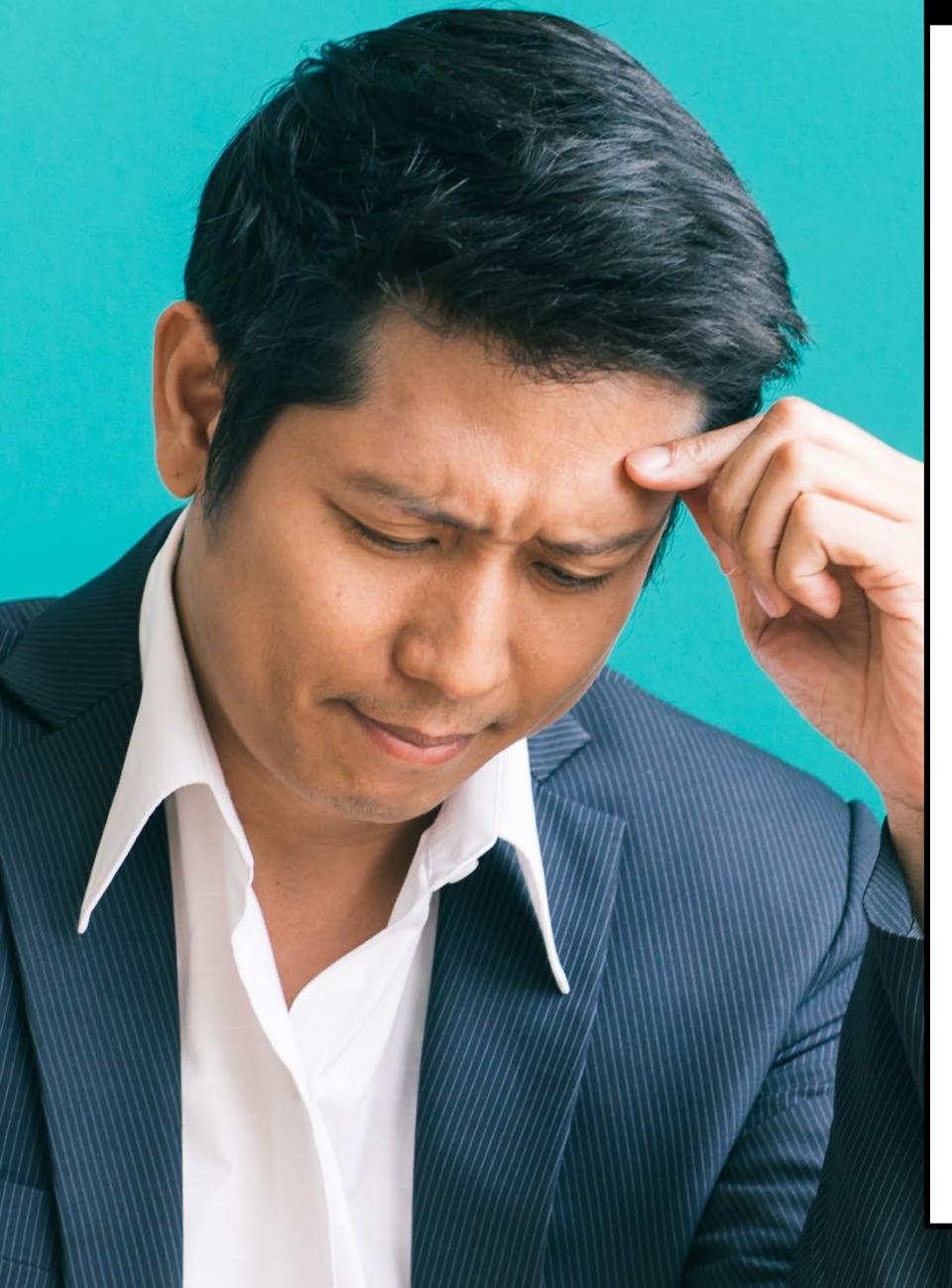
29% cite lack of resources to do job effectively

Opportunity to Expand the Pool

Only 24% women



Source: (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2018



THE RESULT

Monitoring of huge number of alerts

Management of individual events

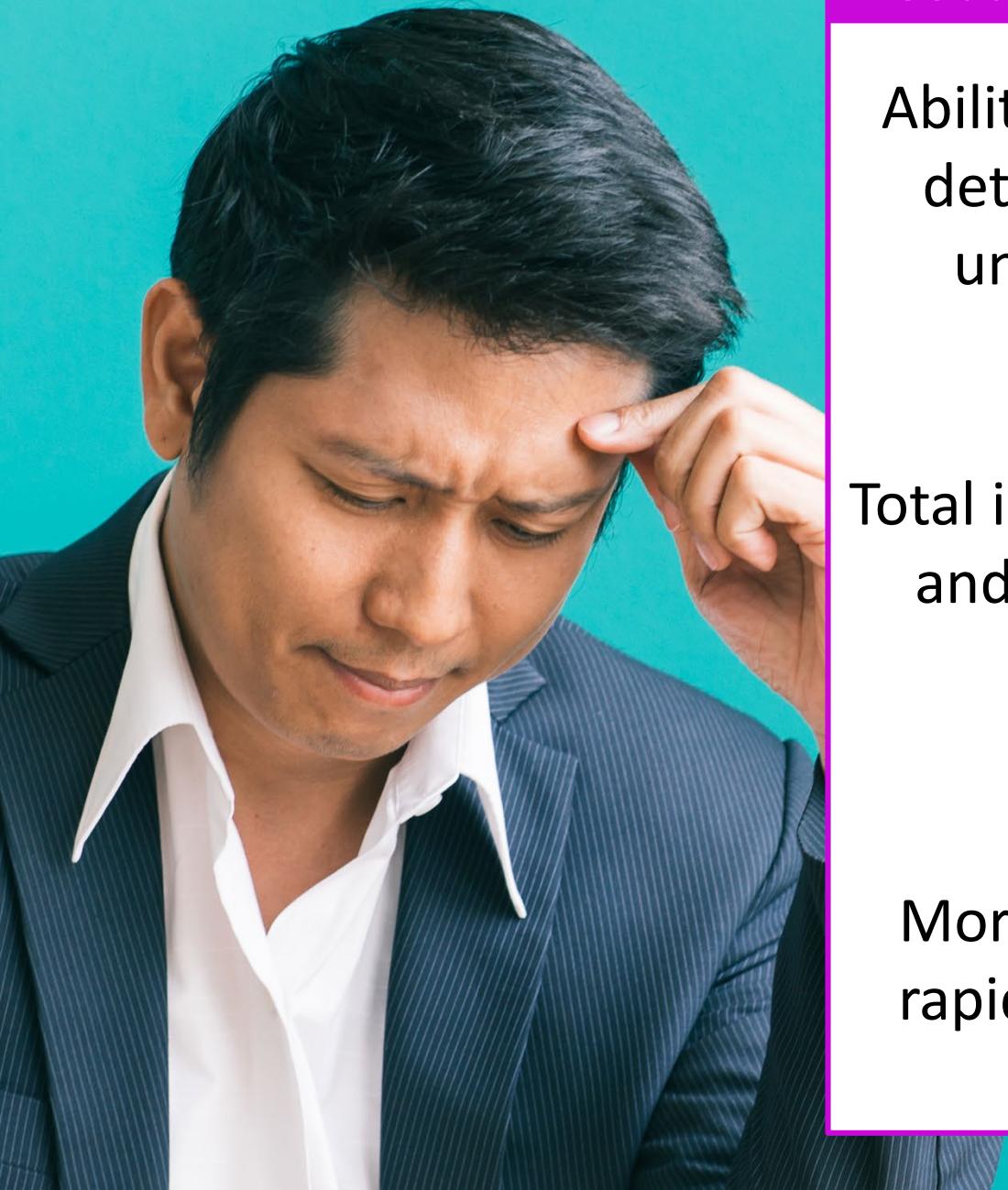
Report generation to enable response

WHAT'S NEEDED?

Ability to more quickly detect and hunt for unknown threats

Total incident root and impact analysis

More automated and rapid threat response



WHAT'S NEEDED?

Ability to more quickly detect and hunt for unknown threats

Total incident root cause and impact analysis

More automated and rapid threat response

LEVERAGING AI

AI-enabled prioritization of highest risk threats

Automated combination & correlation of threat information from across security layers

Orchestration and automation of response

RSA® Conference 2019

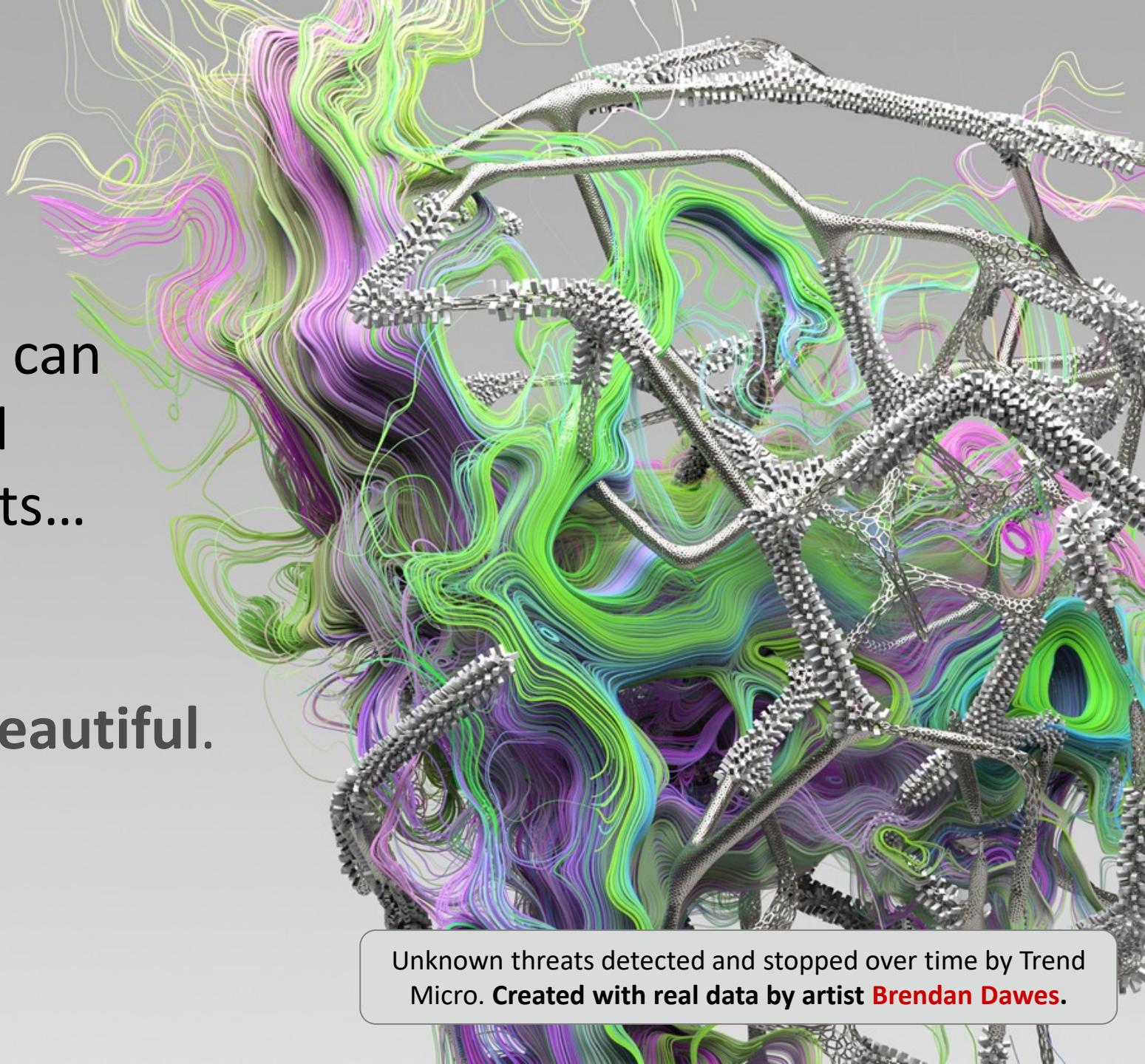
**How we can help turn cybersecurity
into something beautiful**





We believe that when you can
prepare for, *withstand* and
rapidly *recover* from threats...

...cybersecurity can be **beautiful.**



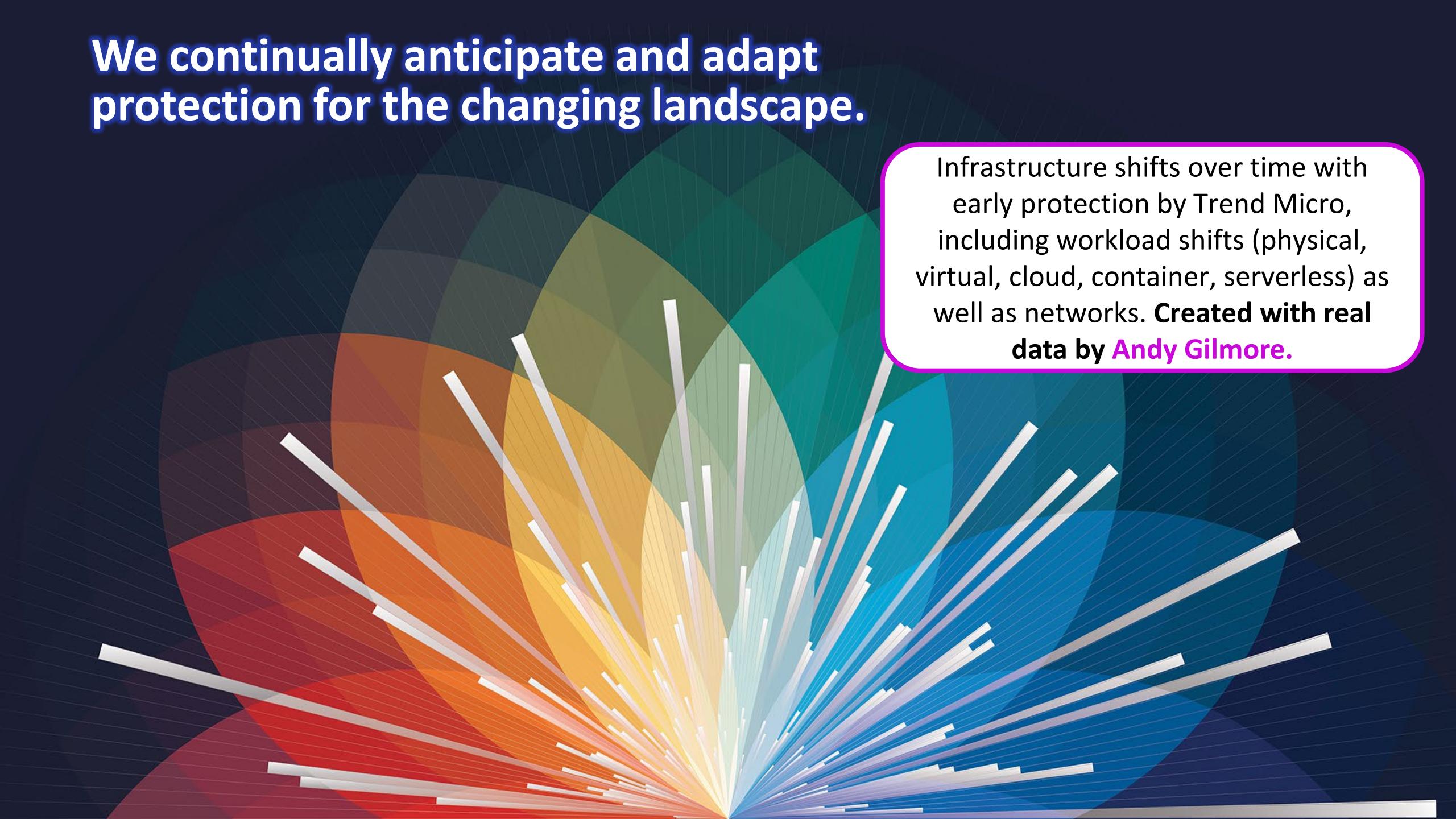
Unknown threats detected and stopped over time by Trend Micro. Created with real data by artist **Brendan Dawes**.

We protect users and their information – on any device, any application, anywhere



Threats detected and blocked globally in 2018 by Trend Micro across multiple arrival vectors, including endpoints, email, web, and USB devices. **Created with real data by Stefanie Posavec.**

We continually anticipate and adapt protection for the changing landscape.



Infrastructure shifts over time with early protection by Trend Micro, including workload shifts (physical, virtual, cloud, container, serverless) as well as networks. **Created with real data by Andy Gilmore.**

We provide protection across all layers of the enterprise. In 2018, we detected and blocked over 40B threats globally.



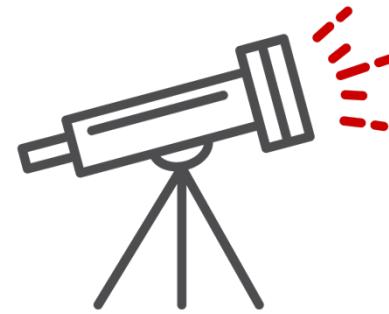
Threats detected and blocked globally by Trend Micro in 2018 across multiple arrival vectors, including endpoint, email, web, network, server, cloud, and container environments. **Created with real data by Daniel Beauchamp.**

What are the qualities of a great artist?

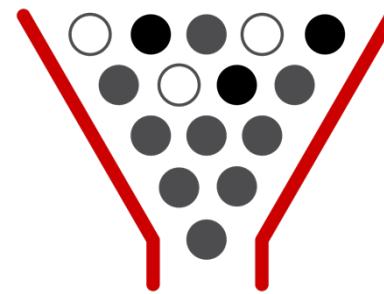
1. Ability to see and interpret what others do not
2. Mastery of skills
3. Deep passion for what they do



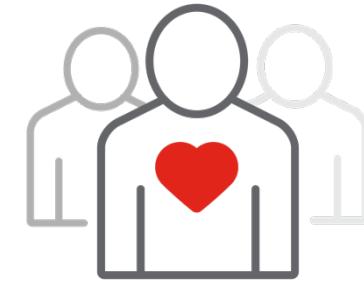
Similarly, we've turned cybersecurity into an artform,
uniquely combining...



Proven Foresight



XGen™ Security Strategy



Passionate People

A man in a purple vest and blue jeans stands on a red stool, painting a large, colorful mural on the side of a shipping container. The mural features abstract, flowing shapes in shades of red, orange, yellow, green, and blue. A metal ladder leans against the wall, and a small wooden structure is visible in the background. The overall scene conveys a sense of creativity and urban art.

When given a new medium, a great
artist always sees an opportunity

For three decades, we've successfully bet on upcoming technology trends— proactively securing new environments so customers can take full advantage of them

1988

Peace of mind computing

1998

Your Internet Virus Wall

2008

Securing Your Journey to the Cloud

2018

Securing Your Connected World

Responsible disclosure to
software/hardware vendors



Threat intelligence and research for
consumers, businesses and governments



Public/private partnerships
(e.g. law enforcement)



Threats



Vulnerabilities
& Exploits



Targeted
Attacks



AI & ML



IoT



OT / IIoT



Cybercriminal
Undergrounds



Future Threat
Landscape



TREND
MICRO™

research

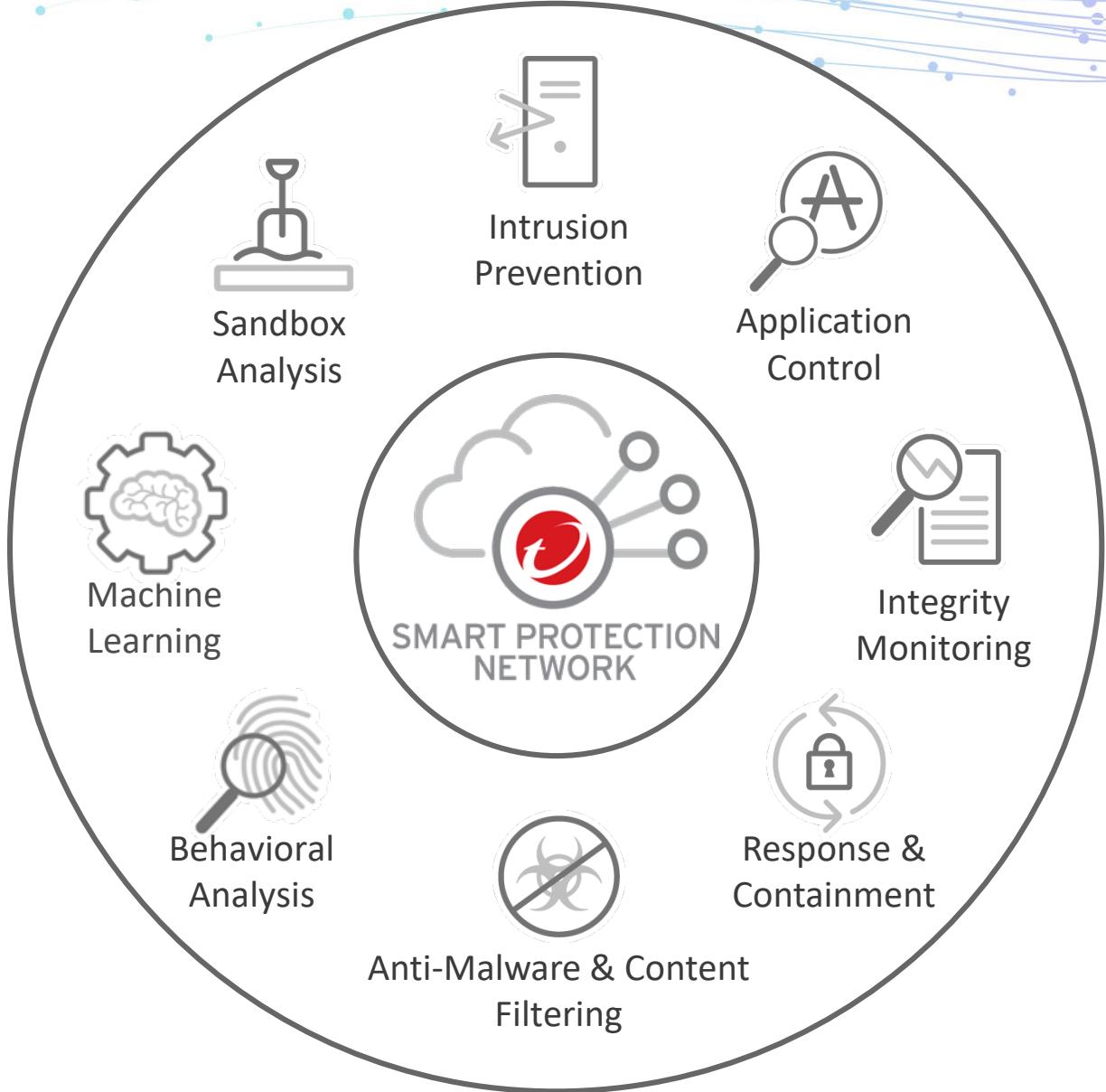


Trend Micro Core
Technology & Products

**While fads come and
true art is timeless**



SMART *Maximizes protection*



OPTIMIZED

*Minimizes IT
impact*



RAPID7



vmware®

aws

Azure



HYBRID CLOUD SECURITY



kubernetes



Office 365

ArcSight

**IBM
@Radar**

splunk®

Google

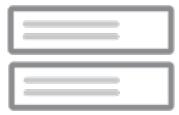
NETWORK DEFENSE



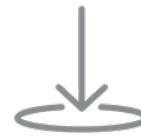
USER PROTECTION

OPTIMIZED
*Minimizes IT
impact*

Appliance



Software



Software



MSP



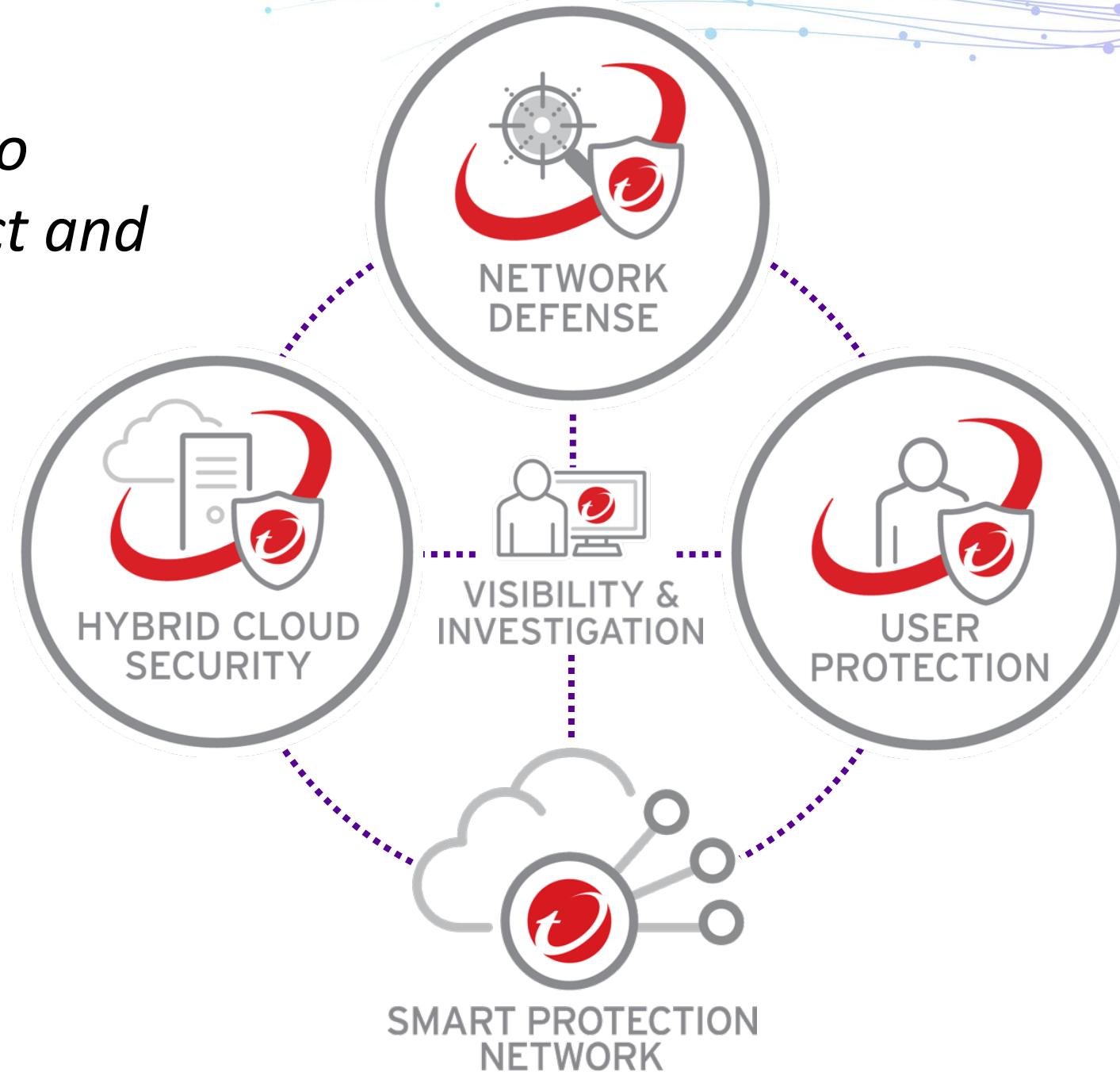
SaaS

Software

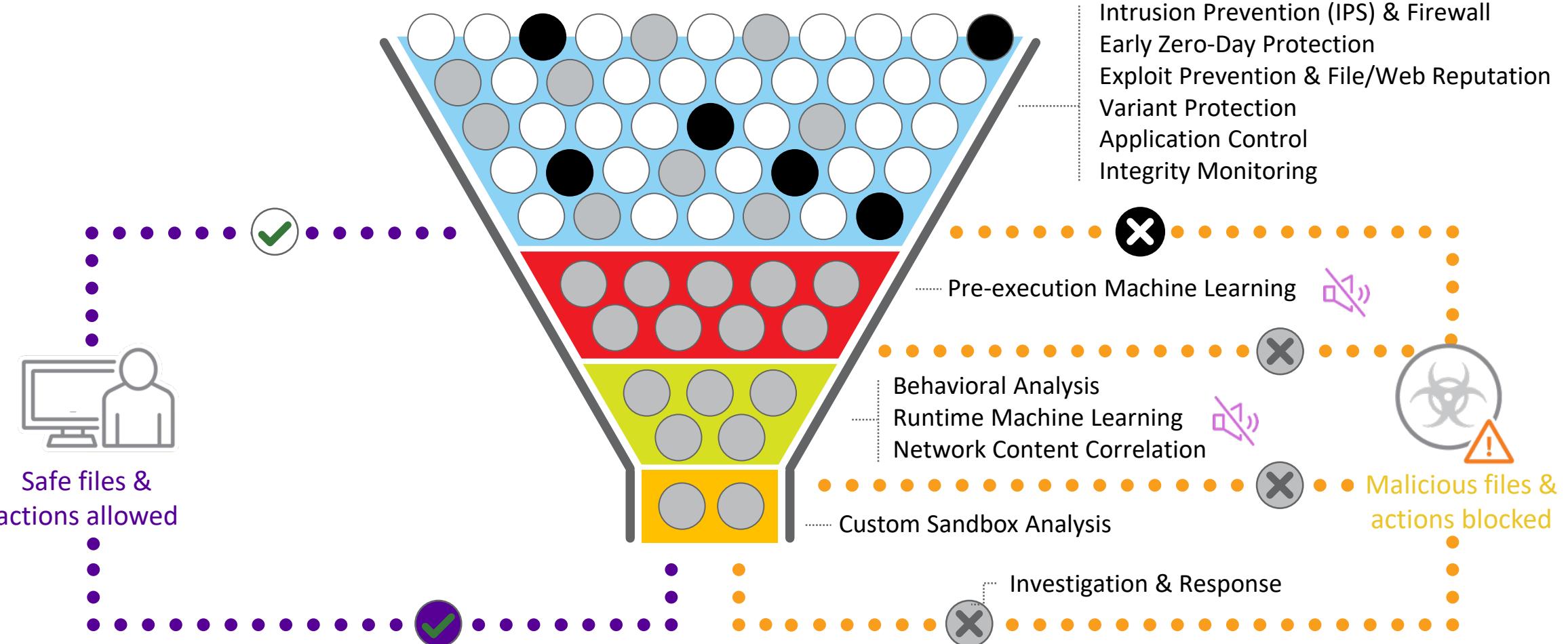


CONNECTED

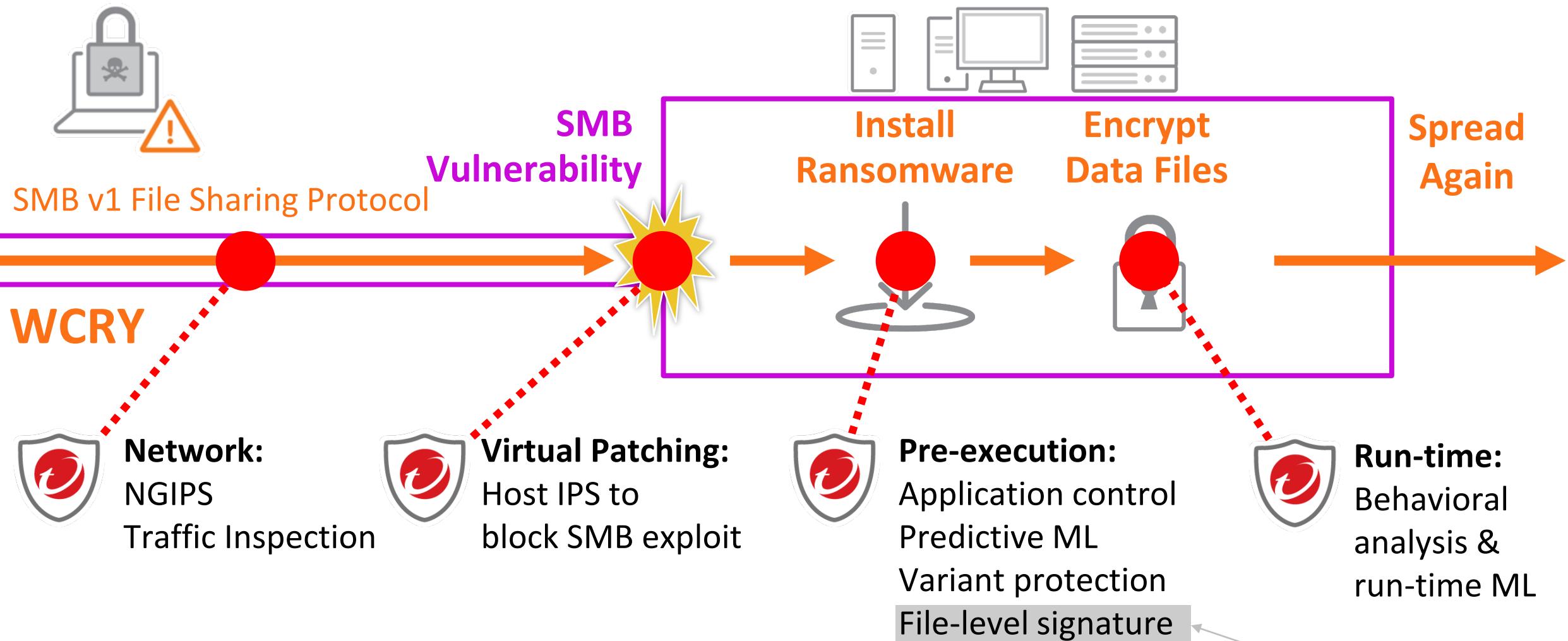
*Speeds time to
protect, detect and
respond*



Right Technique at the Right Time



Real-life Example of Layered Defense: WannaCry



Prepare for, Withstand and Rapidly Recover with a Connected Threat Defense

Enable rapid response through shared threat intelligence and delivery of real-time security updates

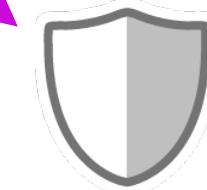


RESPOND

Gain operational visibility, and investigate threat severity and impact

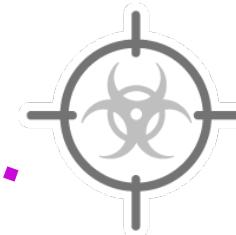


VISIBILITY & INVESTIGATION



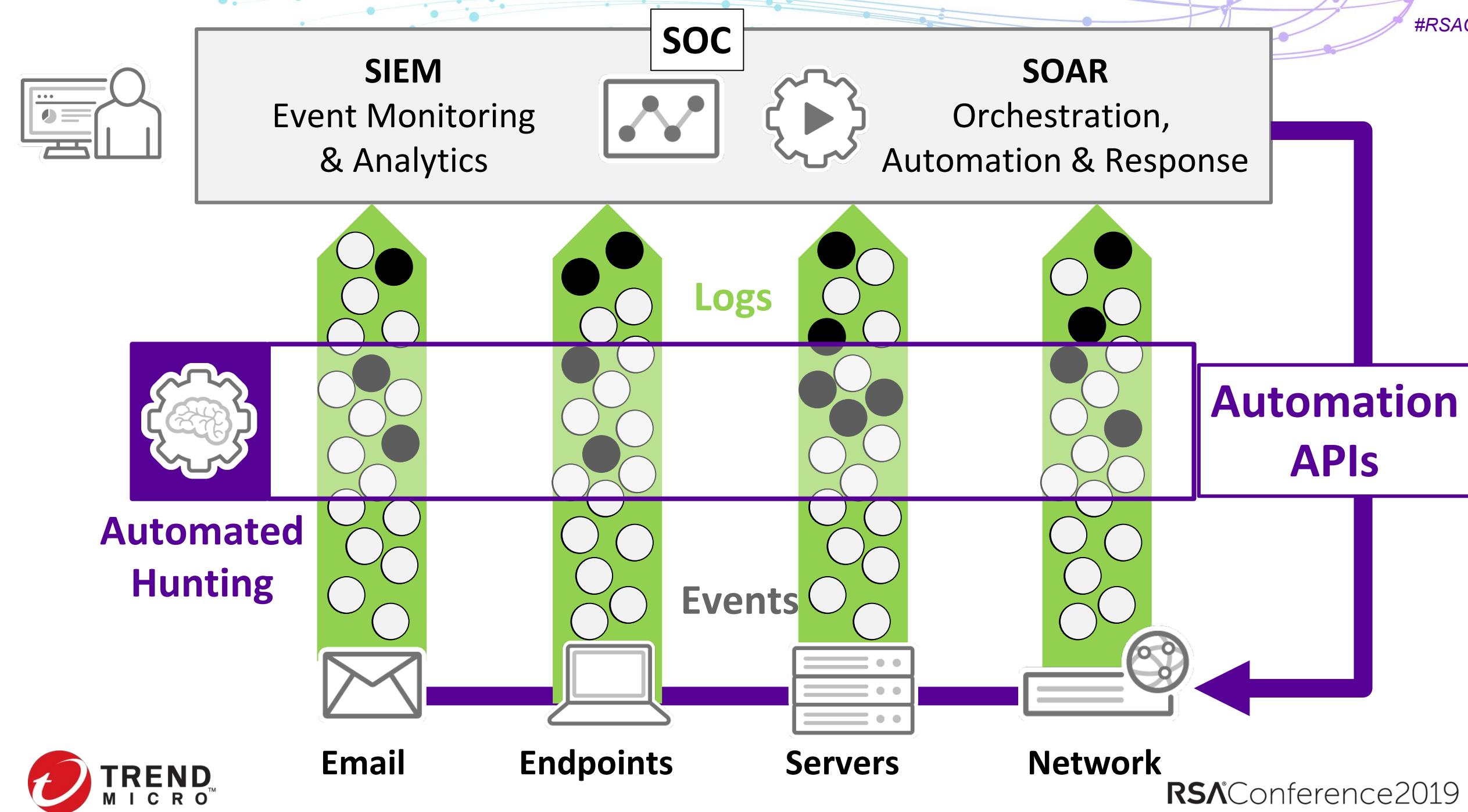
PROTECT

Assess potential vulnerabilities and proactively protect endpoints, servers and applications



DETECT

Detect advanced malware, suspicious behavior and communications invisible to standard defenses



When artists pour
their hearts into
their work,
it shows



We Love What We Do, and it Shows

A photograph of three Trend Micro employees in an office setting. Two men are in the foreground, smiling and looking towards the camera. One wears glasses and a blue plaid shirt, the other wears glasses and a white t-shirt. A third man is visible in the background, also smiling. They are all working at a desk with a laptop.

At Trend Micro, we live and breathe cybersecurity, artfully applying our passion every day to make the world a safer place!

6600+ Trenders
50+ countries around the world

Investing in Security Expertise

Multiple training programs located in US, Canada,
Egypt, Brazil & Saudi Arabia

300+
new security
experts

47%
women



TREND MICRO
CERTIFICATION PROGRAM IN IT SECURITY

This Document Certifies That

Has successfully completed the required course of study approved by
Trend Micro Education, and is therefore awarded this

CERTIFICATE

Given at Cairo, Egypt this 24th Day of November, 2016

Wael Mohamed
President & COO



Carrie [Signature]
Program Instructor

TREND
MICRO™

close the gap®

Close the Gap: Secure the Future.

Girls in Tech™



close the gap

Key Success Factors

1. Choose security that is optimized for *your* environment
2. Consolidate vendors with a connected threat defense
3. Be creative about developing cybersecurity skills



Built by passionate people who live and breathe cybersecurity, Trend Micro empowers you to prepare for, withstand, and rapidly recover from threats, now and in the future.

With Trend Micro, you can be your most resilient—freeing you to go further and do more.

freedom



RSA® Conference 2019

**Come visit our Trend Micro security experts
in the South Hall (S627)**

More info:

TheArtofCybersecurity.com

Trendmicro.com

