



Security-as-a-Service for Small and Medium Sized Businesses

June 5, 2019



Today's web conference is generously sponsored by:



Cygilant

<https://www.cygilant.com/>

Security-as-a-Service for Small and Medium Sized Businesses



Moderator

Tyler Cohen Wood, Private Consultant

Tyler Cohen Wood is a cyber-authority with 20 years of highly technical experience, 13 of which were spent working for the Department of Defense (DoD). As a keynote speaker, author, blogger, national security expert, and overall cyber expert, she is relied on to provide unique insight into cyber threats, cyber warfare, mitigating cyber risk, national security, and ensuring industries have the tools they need to defend themselves in the digital world. Tyler sits on several cyber advisory boards, including CyberSat and The Internet of Things Consortium.

Before becoming a private consultant, Tyler worked in the public sector as an Executive Director for CyberVista and as a Director of Cyber Risk Management group at AT&T using thought leadership and her cybersecurity expertise to develop new and inventive solutions to protect customers from hackers and the ever-increasing cyber threat landscape.

Security-as-a-Service for Small and Medium Sized Businesses



Speaker

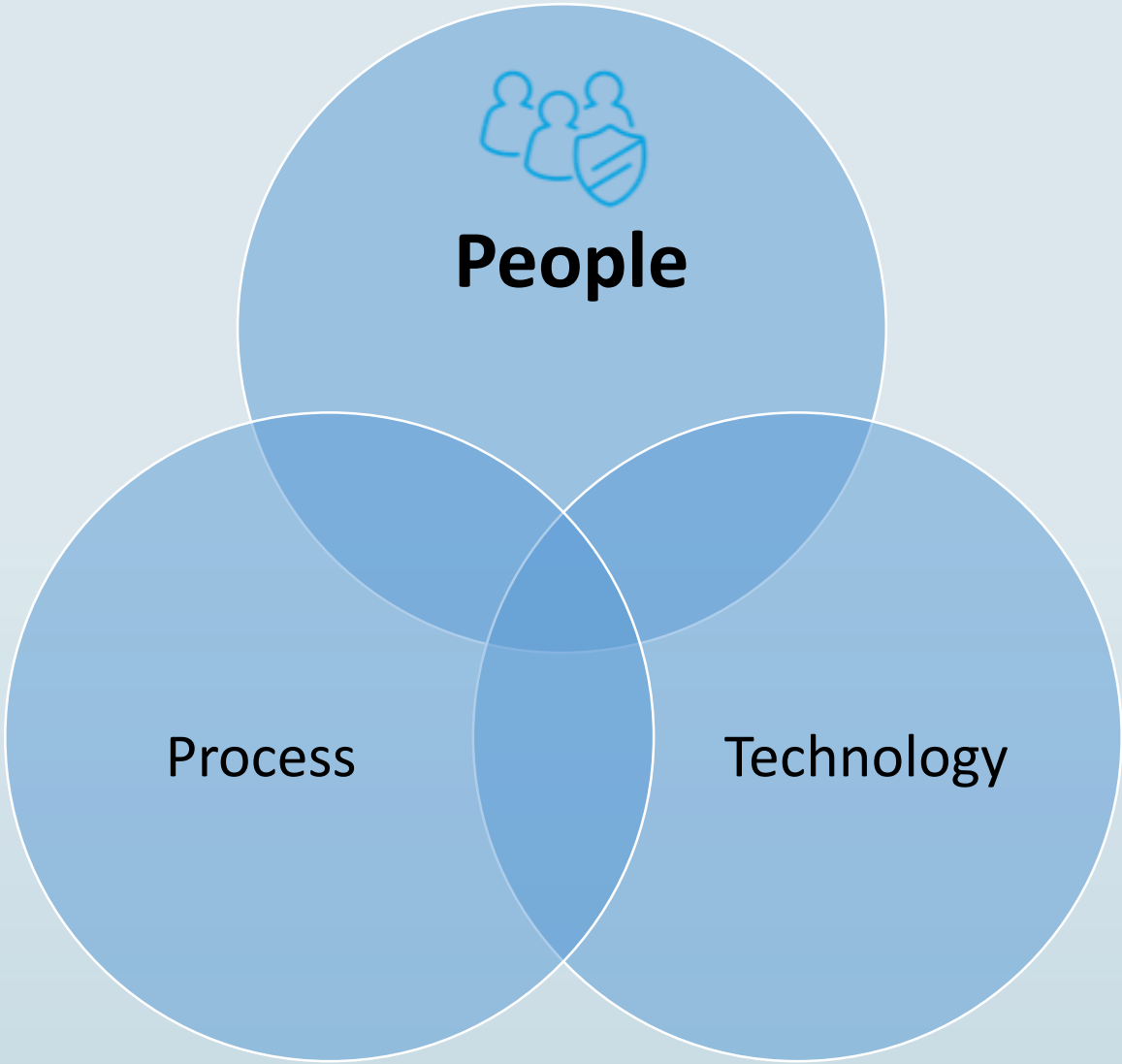
Ryan Kelly, Solutions Engineer, AT&T Cybersecurity

Ryan has been in the tech industry for nearly 20 years with the last 6 years spent focusing on the deeply technical side of cyber security. He has held positions at companies such as Dell, Apple, Forcepoint, Cylance, NSS Labs, and now AlienVault. His responsibilities have included securing enterprise grade infrastructure to include sensitive government networks, researching and reporting on advanced security threats, analyzing and reverse engineering malware in order to train machine learning algorithms, and testing some of the most advanced endpoint security products in the world with the end goal of bypassing or breaking their security mechanisms.

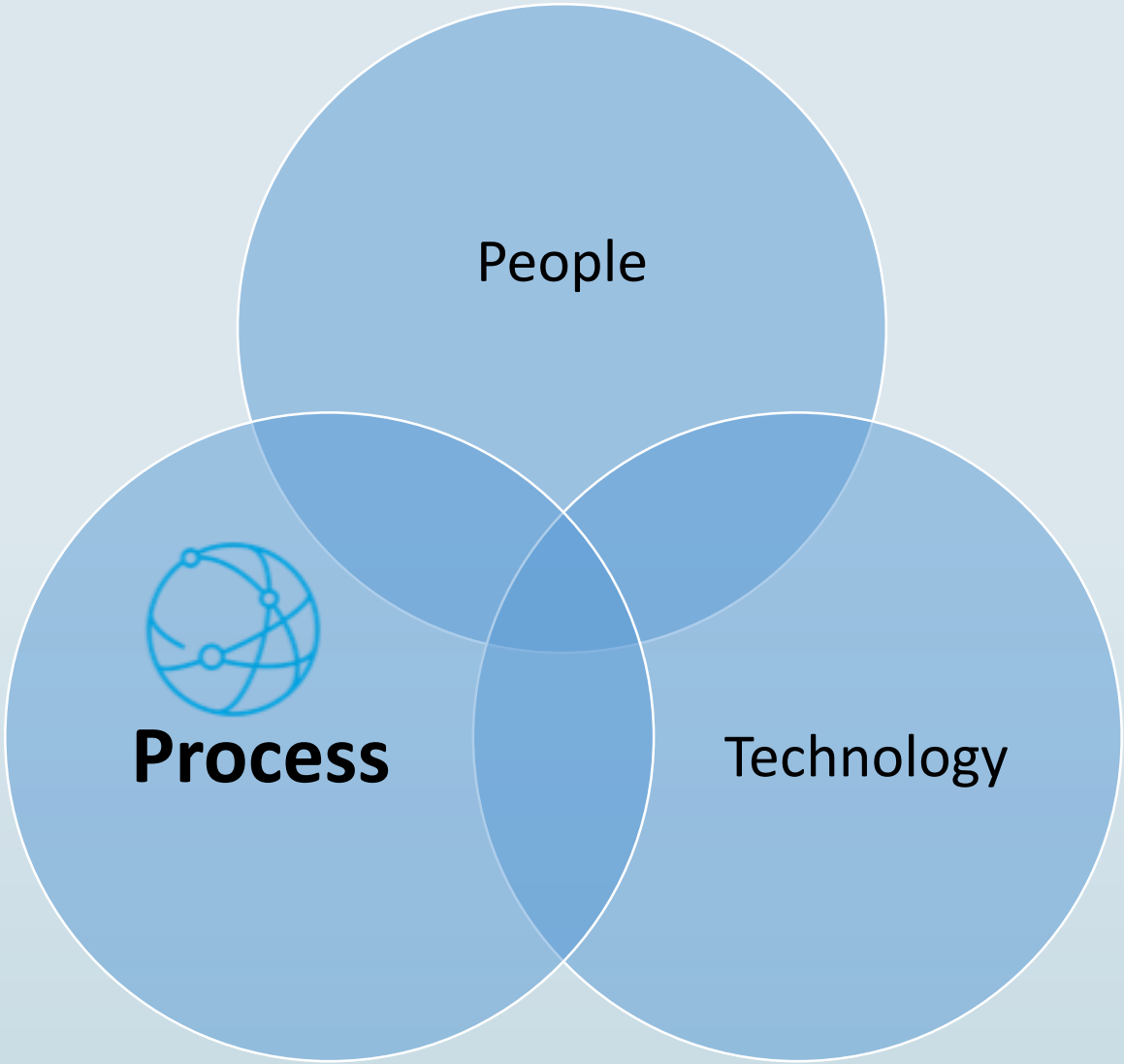
Ryan Kelly

Solutions Architect – AT&T Cybersecurity

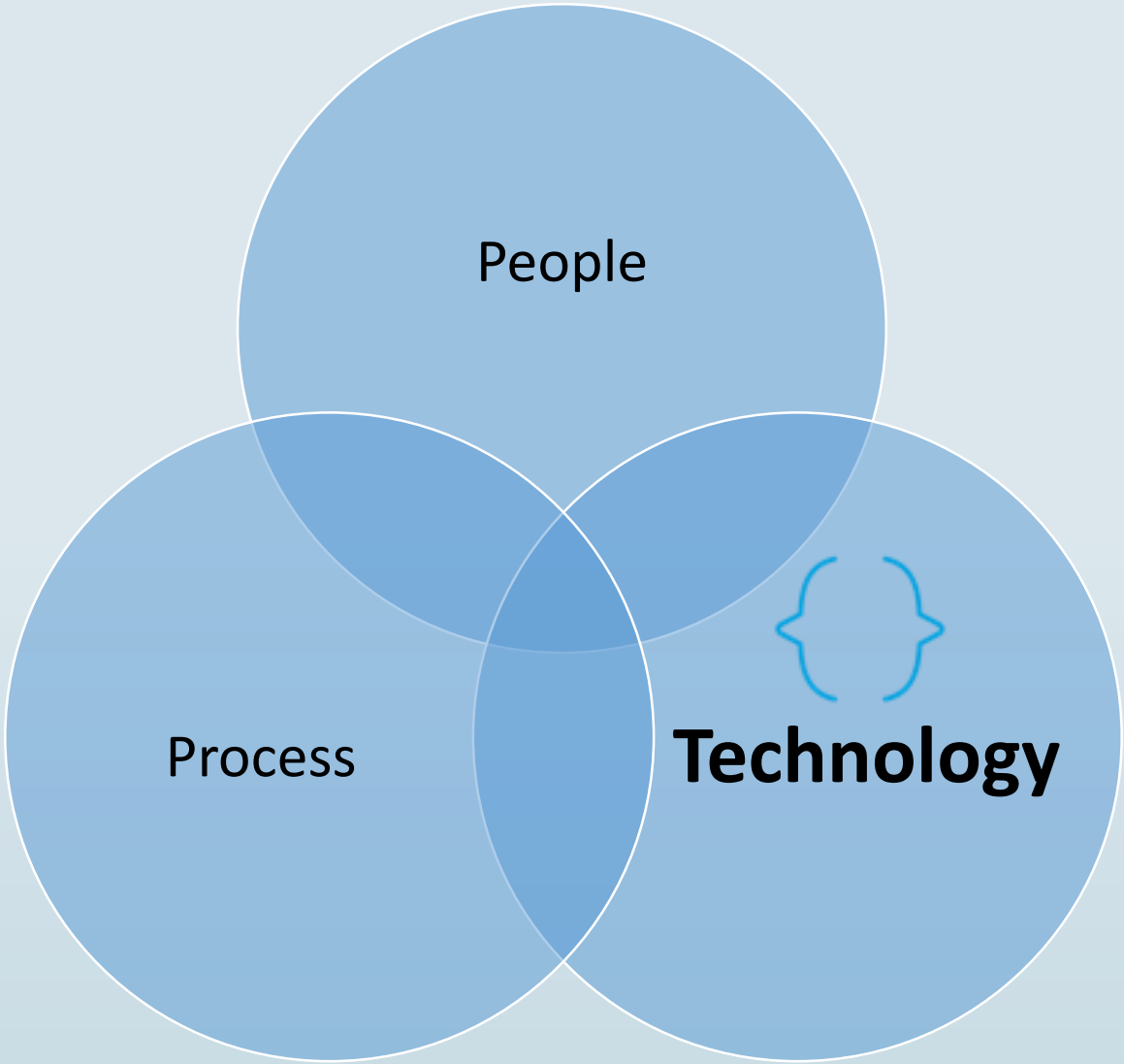
What's Needed?



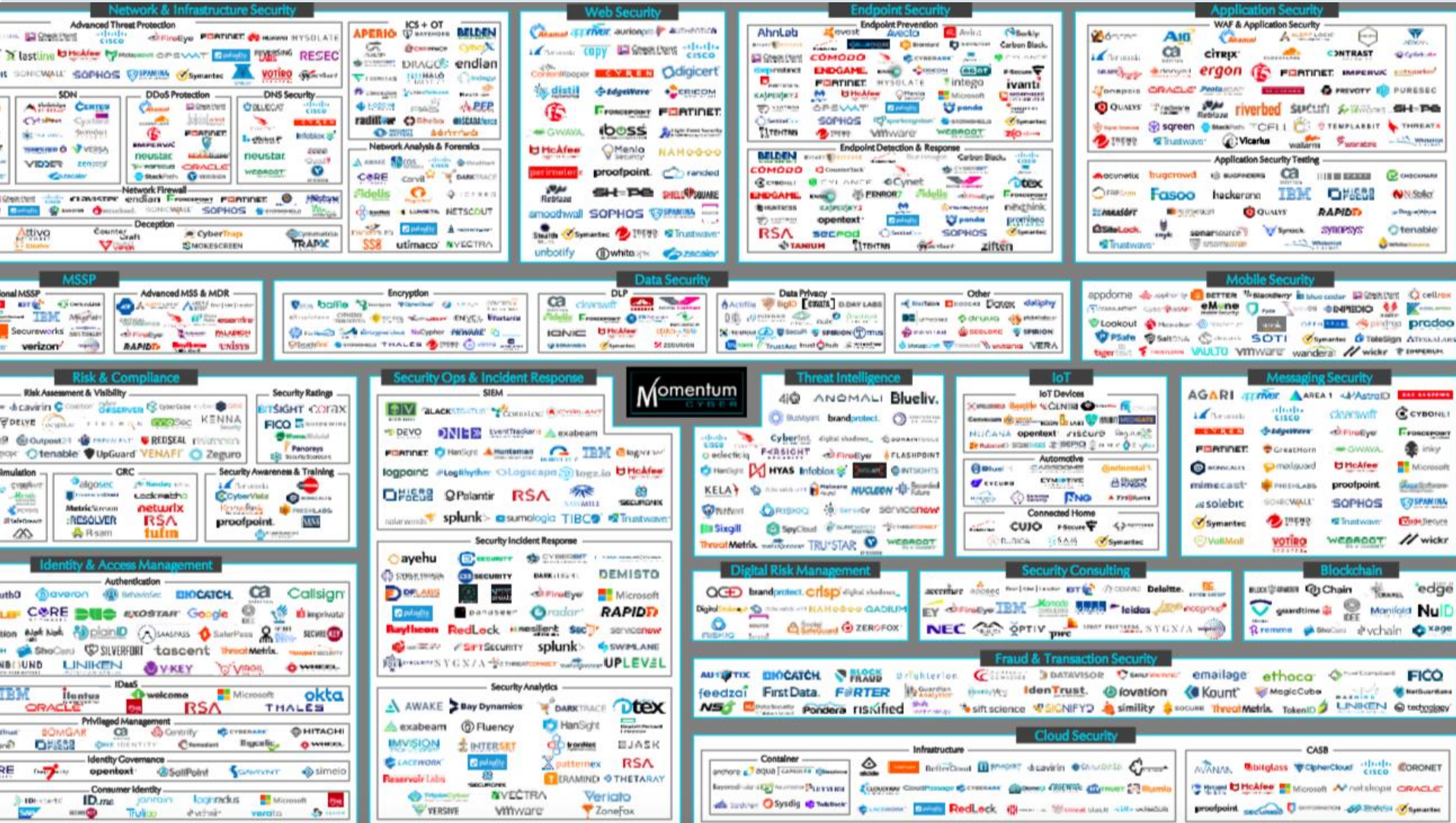
What's Needed?



What's Needed?



More Products, More Noise



The image displays a comprehensive grid of cybersecurity products and services, organized into 18 distinct categories. Each category is represented by a rectangular box containing numerous company logos. The categories are as follows:

- Network & Infrastructure Security:** Includes sub-sections for Advanced Threat Protection, SDN, DDoS Protection, DNS Security, Network Firewall, and Deception.
- Web Security:** Focuses on content filtering and web application security.
- Endpoint Security:** Divided into Endpoint Prevention and Endpoint Detection & Response.
- Application Security:** Includes WAF & Application Security and Application Security Testing.
- MSSP:** Managed Security Service Provider services.
- Data Security:** Includes Encryption, DLP (Data Loss Prevention), and Data Privacy.
- Mobile Security:** Security solutions for mobile devices.
- Risk & Compliance:** Includes Risk Assessment & Visibility, Security Ratings, and Security Awareness & Training.
- Security Ops & Incident Response:** Includes SIEM (Security Information and Event Management) and Security Incident Response.
- Threat Intelligence:** Services for gathering and analyzing threat data.
- IoT:** Security solutions for Internet of Things devices.
- Messaging Security:** Security for messaging and communication channels.
- Identity & Access Management:** Includes Authentication, IDaaS (Identity as a Service), Privileged Management, Identity Governance, and Consumer Identity.
- Digital Risk Management:** Services for managing digital brand and reputational risk.
- Security Consulting:** Professional consulting services.
- Blockchain:** Security solutions for blockchain technology.
- Fraud & Transaction Security:** Services for detecting and preventing fraud.
- Cloud Security:** Includes Container security, Infrastructure security, and CASB (Cloud Access Security Broker).

What Makes a Good SIEM?

A Single Pane of Glass for Orchestration, Analysis, Detection, Intelligence, and Response.



Data Analysis



Threat Detection



Automation &
Response

Threat Intelligence

Security-as-a-Service for Small and Medium Sized Businesses



Speaker

Kevin Landt, VP of Product Management, Cygilant

Kevin Landt is VP of Product Management at Cygilant and has over a decade of experience helping Security and IT Operations teams increase efficiency and reduce risk. Prior to Cygilant, Kevin held director and leadership roles at Opsgenie (now part of Atlassian), Kanguru Solutions, and Intel.

Kevin Landt

VP Product Management – Cygilant



Securing SMBs

- Small teams
- Broad responsibilities
- Seeking balance
- Striving for efficiency

Cost of Security Monitoring



Example Company:

1000 Systems and 1 TB monthly log data

Security Monitoring Costs		
Full Time Equivalents (FTE)		2
Incidents Per Year		130
Fully Loaded Cost Per FTE	\$	75,000.00
Total Cost	\$	150,000.00

Source: Forrester, *The Total Economic Impact™ Of AlienVault® Unified Security Management® (USM)™*, March 2018

Help is not on the way

- **Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021¹**
- 74% - organization is significantly or somewhat impacted by global cybersecurity skills shortage²
- 66% - reported an increased workload on existing staff²
- 44% - solicited by recruiters at least once a week²

1. *Cybersecurity Jobs Report, 2017, Cybersecurity Ventures*

2. *The Life and Times of Cybersecurity Professionals, 2018, ESG and ISSA*

Help is not on the way

- Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021¹
- **74% - organization is significantly or somewhat impacted by global cybersecurity skills shortage²**
- 66% - reported an increased workload on existing staff²
- 44% - solicited by recruiters at least once a week²

1. *Cybersecurity Jobs Report, 2017, Cybersecurity Ventures*

2. *The Life and Times of Cybersecurity Professionals, 2018, ESG and ISSA*

Help is not on the way

- Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021¹
- 74% - organization is significantly or somewhat impacted by global cybersecurity skills shortage²
- **66% - reported an increased workload on existing staff²**
- 44% - solicited by recruiters at least once a week²

1. *Cybersecurity Jobs Report, 2017, Cybersecurity Ventures*

2. *The Life and Times of Cybersecurity Professionals, 2018, ESG and ISSA*

Help is not on the way



- Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021¹
- 74% - organization is significantly or somewhat impacted by global cybersecurity skills shortage²
- 66% - reported an increased workload on existing staff²
- **44% - solicited by recruiters at least once a week²**

1. *Cybersecurity Jobs Report, 2017, Cybersecurity Ventures*

2. *The Life and Times of Cybersecurity Professionals, 2018, ESG and ISSA*

Obligatory Scary Slide



197

AVG DAYS TO
DISCOVER BREACH

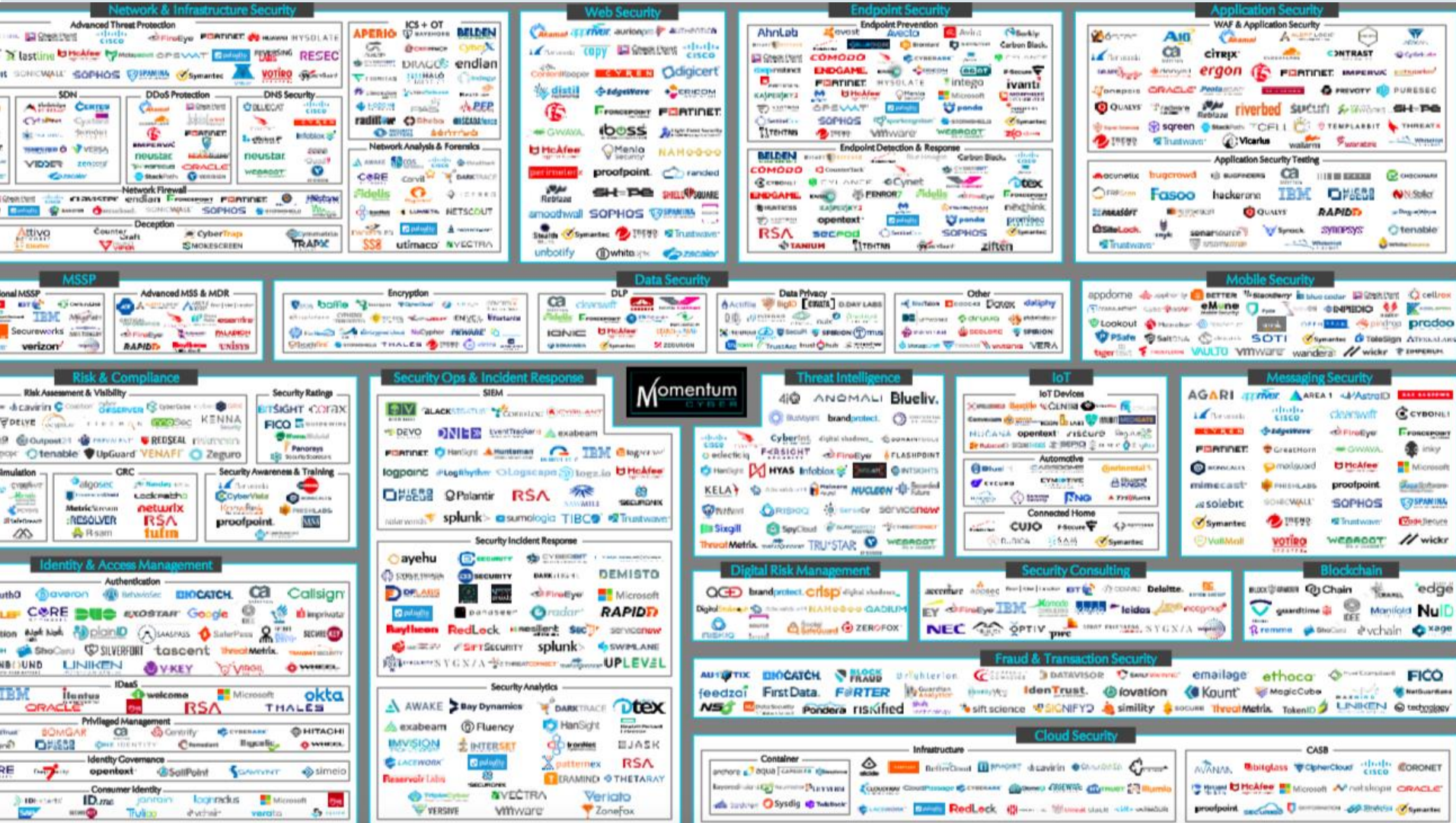
69

AVG DAYS TO CONTAIN
BREACH ONCE FOUND

\$3.6M

AVG COST/BREACH

More Products, More Noise



The image displays a comprehensive grid of cybersecurity products and services, organized into 18 main categories. Each category is represented by a rectangular box containing numerous company logos. The categories are:

- Network & Infrastructure Security:** Includes sub-sections like Advanced Threat Protection, SDN, DDoS Protection, DNS Security, Network Firewall, and Deception.
- Web Security:** Focuses on web-based threats and application security.
- Endpoint Security:** Covers endpoint prevention, detection, and response.
- Application Security:** Includes WAF & Application Security and Application Security Testing.
- MSSP:** Managed Security Service Provider services.
- Data Security:** Includes Encryption, DLP, Data Privacy, and Other.
- Mobile Security:** Security solutions for mobile devices.
- Risk & Compliance:** Risk Assessment & Visibility, Security Ratings, and Security Awareness & Training.
- Security Ops & Incident Response:** SIEM, Security Incident Response, and Security Analytics.
- Threat Intelligence:** Solutions for gathering and analyzing threat data.
- IoT:** Security for Internet of Things devices.
- Messaging Security:** Security for messaging and communication.
- Identity & Access Management:** Authentication, Privileged Management, Identity Governance, and Consumer Identity.
- Digital Risk Management:** Managing digital brand and reputational risk.
- Security Consulting:** Professional consulting services.
- Blockchain:** Security solutions for blockchain technology.
- Fraud & Transaction Security:** Solutions for preventing fraud and securing transactions.
- Cloud Security:** Security for cloud environments, including Container, Infrastructure, and CASB.

Security as a Service

- 3rd-party service provider
- Subscription basis
- Economies of scale
- Best practices
- Specialized security skills

Service Models



What's in scope?

- Deployment and maintenance
- Alert tuning
- Alert and incident response process
- Change requests
- Research and reporting
- Breadth of services
- Compliance and certifications

The business case

- Security force multiplier
- Compliance cost saver
- Replace expensive legacy technology
- Reduce risk



Winning



About Cygilant



**Dedicated
Cybersecurity
Advisor**

**24x7x365
Security
Operations**

**Actionable
Alerts and
Findings**

**Reporting and
Artifacts for
Compliance**

www.cygilant.com



ISSA

Information Systems Security Association
International

www.issa.org

QUESTIONS?