Shop carefully before hiring a managed security service provider (MSSP) to meet your exploding security needs. An MSSP that just throws hundreds of thousands of alerts at your overworked staff can do more harm than good. Here is what an Advanced MSSP must provide to really protect your ever-growing landscape of digital devices and users.

To help in your search for the right MSSP, below are the differences between a Legacy and an Advanced MSSP, and the technologies which support it.

---

**Legacy MSSP**

- Floods internal security staff with lookalike alerts that lack context.
- SIEM (Security Information & Event Management)
- TI (Threat Intelligence)
- MDR (Managed Detection Response)

---

**Advanced MSSP**

- Prioritizes alerts based on the likelihood they signal a threat, and the importance of the affected data and systems.
- SIEM (Security Information & Event Management)
- TI (Threat Intelligence)
- MDR (Managed Detection Response)
- SOAR (Security Orchestration, Automation and Response)
- VM (Vulnerability Management)
- UEBA (User Entity Behavior Analysis)

---

Forrester Analytics, Global Business Technographics® Security Survey, 2018

- 43% of global network security decision-makers say that their firm has implemented or is expanding their implementation of a Threat Intelligence Platform (TIP).
- 61% of global security technology decision-makers say that improving security analytics capabilities is a critical or high priority.

---

**Legacy MSSP**

- Recommends detailed workflows for finding and fighting the most serious threats.
- Focuses on the business impact with tools and processes geared to the most critical systems and data.

**Advanced MSSP**

- Focuses on the network perimeter, neglecting internal threats and not focused on the most critical assets.
- Proactively searches for the latest threats, tapping everything from AI to real-time device data.

---

What to Look for in an Advanced MSSP

- Prioritization of alerts
- Advanced technology
- Triage and response
- Security automation
- Threat intelligence

---

Advanced Cyber Threat Defense

Cognizant Cyber Threat Defense

Forrester Analytics, Global Business Technographics® Security Survey, 2018

- 61% of global security technology decision-makers say that improving security analytics capabilities is a critical or high priority.
- 51% of global client security decision-makers say that their firm has implemented or is expanding their implementation of Endpoint Detection and Response (EDR).
- 63% of global security technology decision-makers say that improving security analytics capabilities is a critical or high priority.

---

**Legacy MSSP**

- Responds to security events, often based on static policies applied only to legacy systems.
- VM (Vulnerability Management)
- UEBA (User Entity Behavior Analysis)

**Advanced MSSP**

- Proactively searches for the latest threats, leaps over network systems to detect the root cause of data breaches.
- MDR (Managed Detection Response)
- SIEM (Security Information & Event Management)
Forrester Analytics, Global Business Technographics® Security Survey, 2018

**Technology Adoption Rate**

- **Advanced Technology**
  - **TI (Threat Intelligence)**
    - Ongoing improvement to systems and processes based on security analytics, new threats and changes to the business.
  - **SOAR (Security Orchestration, Automation and Response)**
    - Advanced Technology
  - **VM (Vulnerability Management)**
    - Custom-configured tools and processes that analyze vulnerabilities, prioritize them, and act on an enterprise security offering.

- **Legacy MSSP**
  - **Advanced Technology**
    - TI (Threat Intelligence)
    - SOAR (Security Orchestration, Automation and Response)
  - **Technology Adoption Rate**
    - 55%

- **Advanced Technology**
  - **SIEM (Security Information & Event Management)**
    - Of global technology decision-makers say their firm has implemented or is expanding their implementation of Threat Intelligence Capabilities in an 'as-a-service' security offering.
  - **UEBA (User Entity Behavior Analysis)**
    - Advanced Technology
  - **MDR (Managed Detection Response)**
    - Advanced Technology

- **Legacy MSSP**
  - **Advanced Technology**
    - TI (Threat Intelligence)
    - SOAR (Security Orchestration, Automation and Response)
  - **Technology Adoption Rate**
    - 68%

- **Advanced Technology**
  - **EI (Enterprise Information)**
    - Of global technology decision-makers say their firm has implemented or is expanding their implementation of Security Analytics/UEBA in an 'as-a-service' security offering.
  - **UEBA (User Entity Behavior Analysis)**
    - Advanced Technology
  - **MDR (Managed Detection Response)**
    - Advanced Technology

- **Legacy MSSP**
  - **Advanced Technology**
    - TI (Threat Intelligence)
    - SOAR (Security Orchestration, Automation and Response)
  - **Technology Adoption Rate**
    - 62%

- **Advanced Technology**
  - **TI (Threat Intelligence)**
    - Of global technology decision-makers say their firm has implemented or is expanding their implementation of Security User Behavior Analytics (SUBA) in an 'as-a-service' security offering/approach.
  - **UEBA (User Entity Behavior Analysis)**
    - Advanced Technology
  - **MDR (Managed Detection Response)**
    - Advanced Technology

- **Legacy MSSP**
  - **Advanced Technology**
    - TI (Threat Intelligence)
    - SOAR (Security Orchestration, Automation and Response)
  - **Technology Adoption Rate**
    - 65%

- **Advanced Technology**
  - **TI (Threat Intelligence)**
    - Of global technology decision-makers say their firm has implemented or is expanding their implementation of Threat Intelligence Capabilities in an 'as-a-service' security offering.
  - **UEBA (User Entity Behavior Analysis)**
    - Advanced Technology
  - **MDR (Managed Detection Response)**
    - Advanced Technology

- **Legacy MSSP**
  - **Advanced Technology**
    - TI (Threat Intelligence)
    - SOAR (Security Orchestration, Automation and Response)
  - **Technology Adoption Rate**
    - 60%

---

**About Cognizant Security**

Cognizant Security helps you achieve better business outcomes by securing your digital transformation. We provide the security capabilities you need to address ever-changing threats, maintain compliance and reduce the unsustainable burden of managing security infrastructure.

To learn more visit our website, [http://www.cognizant.com/security](http://www.cognizant.com/security) or feel free to contact us directly at [cognizantsecurity@cognizant.com](mailto:cognizantsecurity@cognizant.com)

Cognizant (Nasdaq-100: CTSH) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 19 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at [www.cognizant.com](http://www.cognizant.com) or follow us @Cognizant.

© Copyright 2019, Cognizant. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission from Cognizant. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.