



# Eliminate alert overload with simplified breach prevention

Combine CRITICALSTART® Managed Detection and Response services with Microsoft Security solutions to extend protection and performance



# Table of Contents

---

03

Are you keeping pace with the volume and sophistication of today's threats?

---

11

Protect it all

---

04

Extend your Microsoft Security investments

---

12

Case study: Global leadership advisory and search firm

---

06

Act on the right knowledge

---

15

Make the most of your Microsoft Security investments

---

09

Control the uncontrollable

# Are you keeping pace with the volume and sophistication of today's threats?

## Cybersecurity is a board-level issue

Corporate leaders are increasingly elevating the importance of cybersecurity. But recent high-profile attacks reveal how much more needs to be done in the years ahead. Though the COVID-19 pandemic has accelerated technological adoption through the explosion of remote work, it has also exposed some of the most complex cyber vulnerabilities that have made cybersecurity risk an international concern.

- Ransomware attacks cost an average of \$4.62M – more expensive than the average data breach, which costs \$4.24M.<sup>1</sup>
- A new IDC survey found that more than one third of organizations worldwide have experienced a ransomware attack or breach that blocked access to systems or data in the previous 12 months. The Manufacturing and Finance industries reported the highest ransomware incident rates while the Transportation, Communication, and Utilities/Media industries reported the lowest.<sup>2</sup>
- 82% of security leaders have been surprised by a security event, incident, or breach that evaded a control they thought was in place.<sup>3</sup>

Microsoft Security has developed bold new tools to combat the most sophisticated threats known to the digital world. This is in large part due to the cloud provider's extensive visibility into the global threat landscape, analyzing over 24 trillion security signals every 24 hours to track the evolution of cybercrime. But while these products offer the right capabilities needed to extend a company's security perimeter, most organizations struggle to find the right talent and resources to manage the technologies and understand their output.



# Extend your Microsoft Security investments

It's one thing to know how critical security and risk management is to the integrity of your brand. That's why many security executives have already invested in leading platforms like Microsoft 365 Defender, Microsoft Sentinel, and Microsoft Defender for Endpoint. It's entirely another thing, however, to operate, optimize, and maintain those products – especially when the average enterprise security environment includes more than 76 different security tools, each generating hundreds of alerts that take up hours of a security analyst's time.<sup>3</sup>

To derive real value from your security investments, a company needs the expertise and methodology to make sense of Microsoft's cross-enterprise visibility threat detection and auto-investigation capabilities to radically reduce alerts and actively respond to threats. That's where Critical Start Managed Detection and Response (MDR) for Microsoft Security is driving the most impact. Critical Start simplifies breach prevention by delivering the most effective MDR services powered by a proprietary Zero Trust Analytics Platform™ (ZTAP™) and one of the industry's only Trusted Behavior Registry™ (TBR) and MOBILESOC®. Providing 24x7x365 access to expert security analysts and the Critical Start Cyber Research Unit (CRU), Critical Start is uniquely equipped to monitor, investigate, and remediate alerts swiftly and effectively with 100% transparency into the process.



## Maximize value with Critical Start MDR services for Microsoft Security

### Act on the right knowledge

Don't let the skills gap impede your ability to operationalize security controls for maximum protection.

[Learn More](#)

### Control the uncontrollable

Anticipate the risks associated with today's hyper-complex security environment and respond faster.

[Learn More](#)

### Protect it all

Defeat the alert fatigue while ensuring every single activity is monitored to prevent a breach.

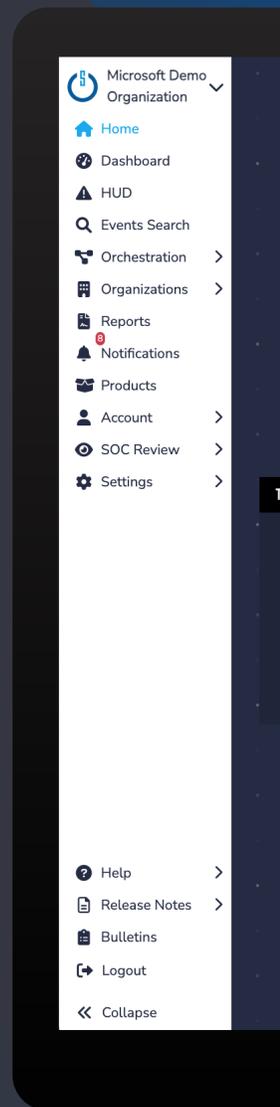
[Learn More](#)

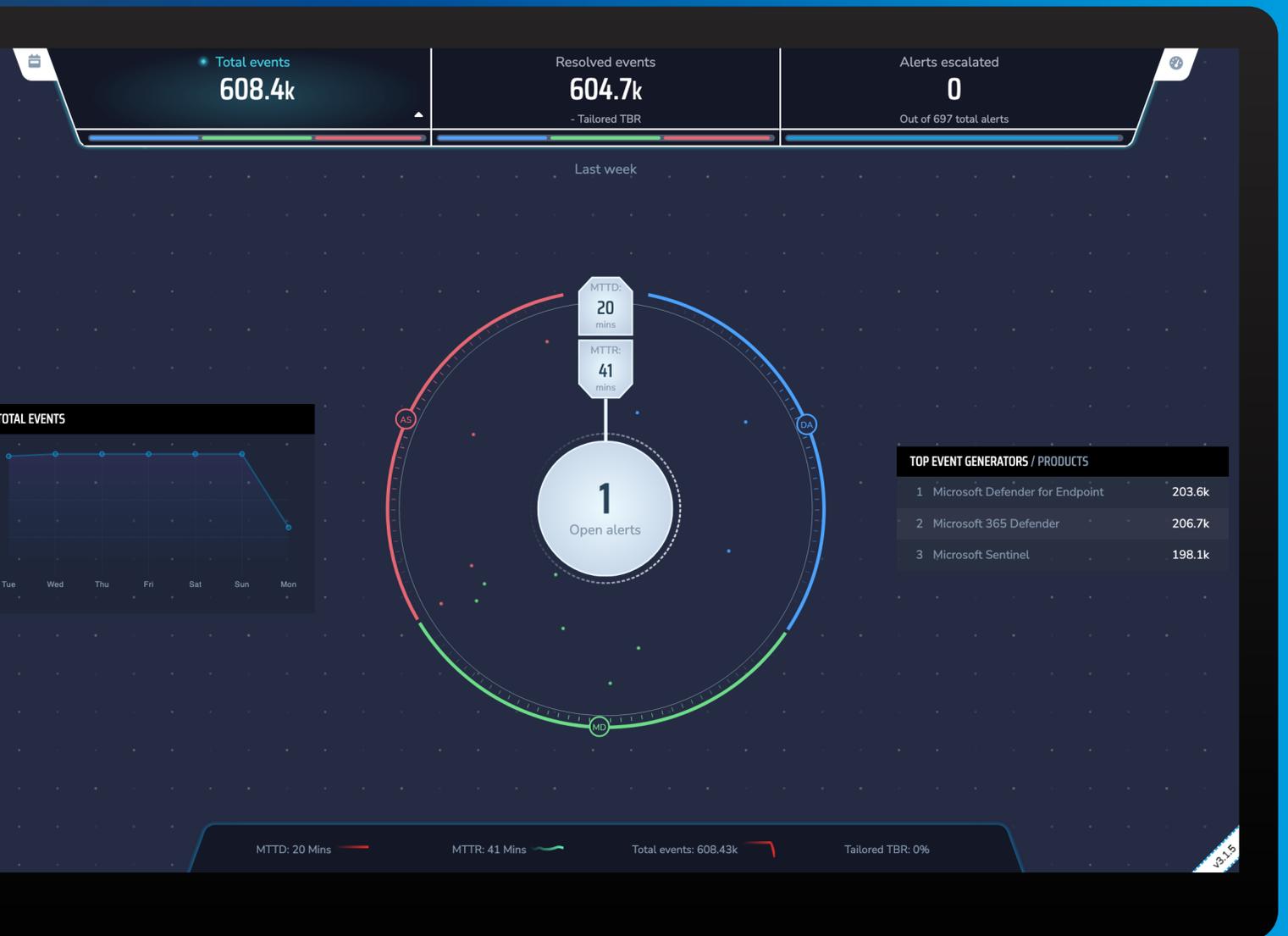
# Act on the right knowledge

Access to the right expertise and strategy is non-negotiable

Only 40% of security leaders are confident in their ability to check that security controls are working as intended.<sup>3</sup> Most security gaps among companies deploying Microsoft Security products are around configuration and maintenance. Not every security analyst is going to know it all, let alone have time to deviate from their day-to-day responsibilities to learn how to optimize Microsoft Security controls while maintaining hundreds of threat detections.

MDR is the latest evolutionary step in protecting organizations from a highly diverse, multifaceted threat environment. It offers a way for companies to access the latest security expertise without hiring internally. And its effectiveness has not gone unnoticed – by 2025, 50% of organizations will be using MDR services for threat monitoring, detection, and response functions that offer threat containment and mitigation capabilities. Where MDR services are undoubtedly useful, Critical Start takes these benefits even further by leveraging the power of their ZTAP and Trusted Behavior Registry, which eliminates false positives at scale. Combining a depth and breadth of Microsoft security expertise and best practices, the Critical Start team is skilled at maturing an enterprise's Security Operations (SecOps) by capitalizing on the full potential of their investments in Microsoft 365 Defender, Microsoft Defender for Endpoint, and Microsoft Sentinel.





## Optimize your security team's time and budget

- Reduce security team workload with ZTAP auto-resolution of false positives.
- Reduce the number of alerts escalated to your analysis and let Critical Start investigate and resolve on your behalf.
- Benefit from fast and effective resolution with a 1-hour SLA for Time to Detect (TTD) and Median Time to Resolution (MTTR).
- Get support for managing out-of-the-box Microsoft detections and Indicators of Compromise (IOCs).

[← Back](#)

## Alert Details

ID 219332



Created: 08/23/22, 7:01 AM

### 'Emotet' Malware Was Detected on WIN-1PvjlbKn

Reviewing

Microsoft Defender for Endpoint (Production)

Windows Defender for Endpoint Demo

Assigned to me

CAT 6 - Investigation

0 - NONE

+ Add Tag

Comments

7 >

Show previous events



Triggers

5 >

Observations

3 >

Whitelisted

0 >

# Control the uncontrollable

The attack surface will continue to change, so don't let your defenses falter

With an attack surface that is constantly changing, where access roles are dynamic, and devices and applications request and keep more data, it's no wonder enterprises are struggling to protect their people, assets, and infrastructure. It's not enough to deploy tools to improve one's security posture. You need to know how to use the information generated with reassurances that what you're seeing is an accurate reflection of your risk.

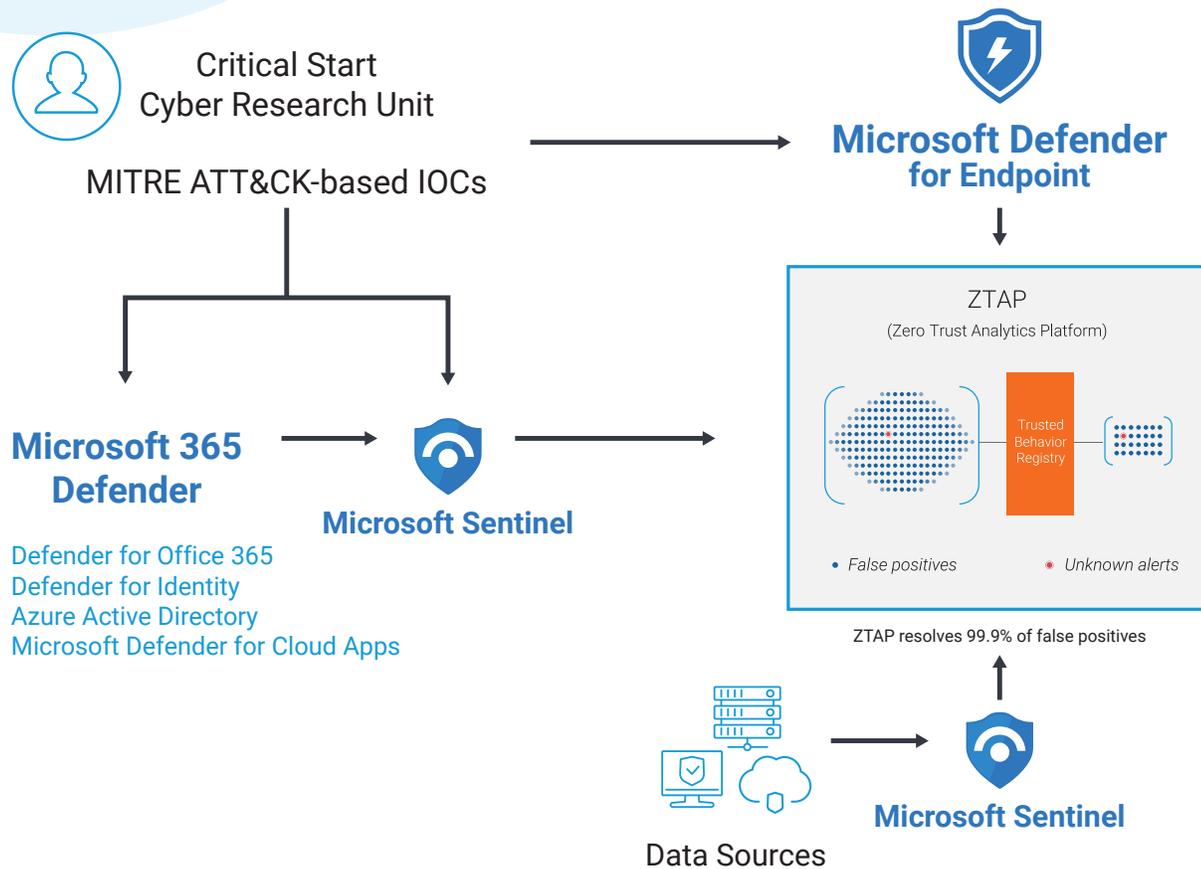
Compared to other MDR partners, Critical Start knows that a comprehensive integration with the Microsoft Security product portfolio is key to helping you consolidate visibility and speed up investigation and response times. Critical Start takes an all-in security approach with a focus on least privilege. All-in security is baked into every layer of the Critical Start MDR Services for Microsoft Security, helping security leaders distill the noise of alerts and take the right actions to prevent breaches. Security teams can better understand attacks across hybrid device types and can quickly investigate the context and remediate true positives.

## You have a right to see what's going on

- Gain 100% visibility into every Microsoft data point collected via the web or MobileSOC application.
- Triage, escalate, and isolate incidents anytime and anywhere via the MobileSOC application.
- Gain complete threat detection visibility and coverage across your security tools and MDR services to improve outcomes and accelerate time to response.
- Benefit from a native API integration to connect Microsoft security tools into a single pane of glass.

# Don't let a single threat go uninvestigated

## Critical Start – Enterprise-wide Detection and Response

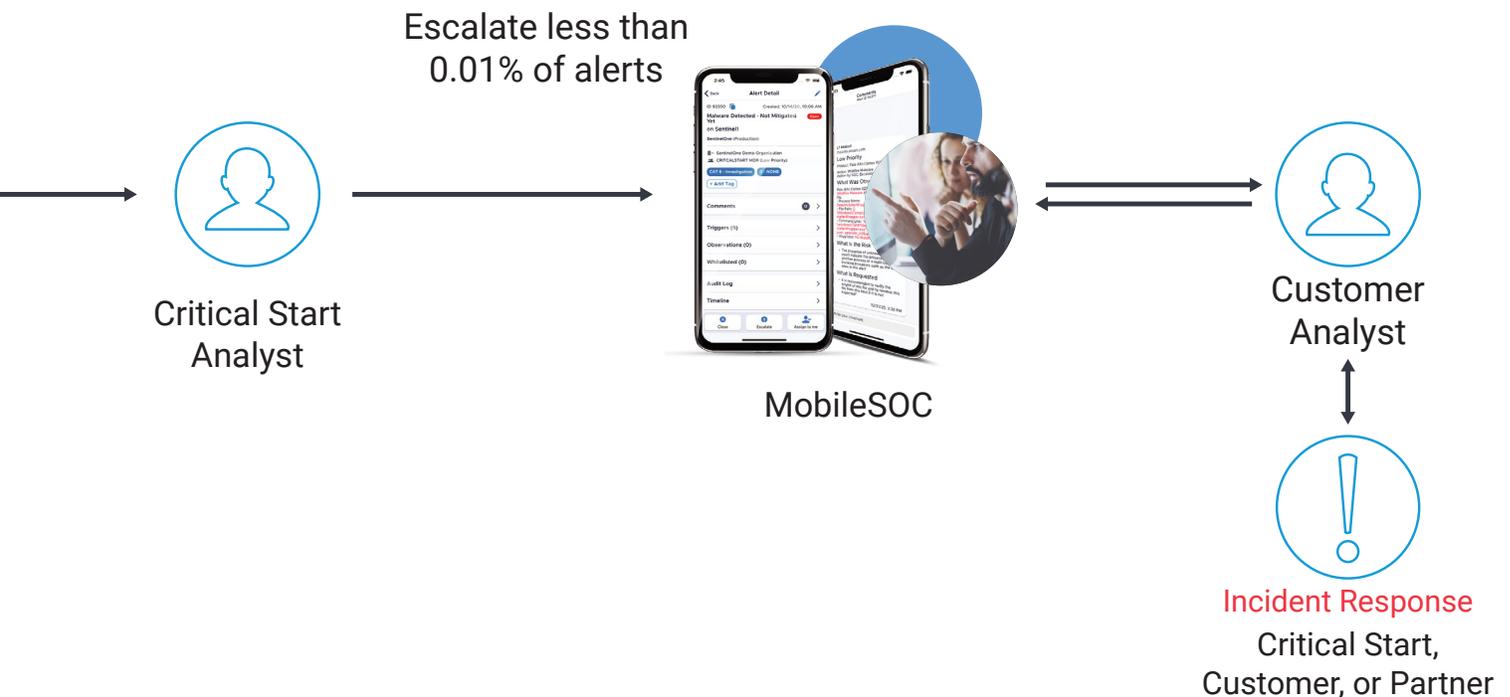


# Protect it all

The best way to reduce risk is to monitor and resolve every alert

Alert fatigue is a real issue among security analysts. With so many integrated security tools, analysts are tasked with sifting through hundreds of thousands of alerts to uncover possible threats to the business. Unfortunately, given the volume, most security alerts are not being analyzed and resolved – analysts simply don't have the time and resources, a situation that makes the business still more vulnerable to attack.

Where the vast majority of MDR partners would help augment a company's security operations center by helping distill the noise and investigating the bad alerts, Critical Start takes a different approach. Critical Start MDR for Microsoft Security doesn't just focus on the bad – it accounts for the good too and takes note of every false positive to better understand the typical behaviors of different systems. The Trusted Behavior Registry (TBR) within ZTAP is built to resolve all alerts, triaging information and passing along complicated unresolved incidents to well-trained, seasoned security analysts for closer investigation. That means no alert is left behind – an approach that effectively prevents security breaches.



## CASE STUDY

# Global leadership advisory and search firm

## Situation

It took over 50 years for one global executive talent leader to enable businesses across 10 sectors to connect with tomorrow's leaders. Today, this client now offers up to 40 different services, touching everything from board and CEO advisory services to cultural transformation and succession planning. With such a broad portfolio, the only way the organization can gain its signature insight is through data – massive amounts of data.

## Challenge

With so much data to sift through and a database that spans three redundant datacenters with connections to 48 offices in 23 countries, the company knew they needed a stronger security posture. Their current security provider did not give them the confidence they were looking for when it came to monitoring and securing endpoints and critical assets. This prompted them to start searching for a dedicated Managed Detection and Response Provider that met their business needs.

## Result

Critical Start stepped in to address the client's immediate challenges. The Critical Start team worked with the organization to deploy Microsoft Defender for Endpoint for enhanced threat monitoring and detection capabilities. After a 6–8-week deployment, the company was able to reduce false positive alerts by 90–95%. 45 days later, false positives were almost eliminated entirely.

The organization was especially impressed with what they coined the “secret sauce” of Critical Start: Rather than focusing investigation exclusively on critical or high threat alerts, Critical Start believes all alerts should be treated equally. This has given the company greater reassurance around their security posture.







<sup>1</sup> Cost of a Data Breach Report 2021 | Ponemon Institute/IBM Security

<sup>2</sup> IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach | Business Wire

<sup>3</sup> Security Leaders Peer Report | Panaseer

# Make the most of your Microsoft Security investments

When it comes to threat detection and response, today's reality is daunting. But Critical Start can help your SecOps team step up to meet the cybersecurity challenges of today by providing MDR services for the powerful Microsoft solutions you've already invested in.

Learn more about how Critical Start can help your security team simplify breach protection with MDR services that flex to your business objectives and cybersecurity vision – regardless of complexity.

## Managed Detection and Response Services for Microsoft 365 Defender

[Learn More](#)

## Managed Detection and Response Services for Microsoft Defender for Endpoint

[Learn More](#)

## Managed Detection and Response Services for Microsoft Sentinel

[Learn More](#)



[Help me simplify my breach prevention | Contact](#)

[Learn more | MDR for Microsoft Security](#)

