Simplify your Microsoft Security Operations for Identity-Based Alerts

CRITICALSTART®

Abstract

Identity is the new security perimeter forcing many organizations to rethink security for their workforce to work from remote locations. This has introduced additional cybersecurity challenges because employees may not have the same level of security controls in place at home as they experience at work. To address these challenges, organizations have resorted to increased monitoring and detection of threats. However, existing approaches to monitor and respond to threats are proving to be inadequate. In this white paper, we will examine an approach to detect and address identity-based alerts in a Microsoft environment, and the measurable benefits from this approach.

Overview of Microsoft® Security Solutions

Microsoft provides a comprehensive set of tools for cybersecurity professionals to manage both their Microsoft and non-Microsoft applications and infrastructure.

The core focus of Microsoft products has been to protect Microsoft assets such as Sentinel, Windows and Microsoft 365 Defender. They have a large base of enterprise customers that acts as a source for deep threat intelligence. One of the core strengths of Microsoft has been identity management. For customers who have on-premises solutions, Active Directory acts as a source of truth for user identity. With the growth of Sentinel, many customers have built solutions using Active Directory (**AAD**) for managing user identities. With the adoption of Microsoft 365 Defender, many customers have leveraged Microsoft' Identity-as-a-Service (**IDaaS**) offering for managing identities. Additionally for protecting Office 365, Microsoft provides tools for securing email, documents and collaboration tools. Microsoft security solutions protect endpoints and mobile devices. With the strong adoption of Sentinel, Microsoft introduced the cloud security capabilities to gain visibility into cloud usage, to protect data in the cloud and to detect threats across clouds.

All of the above security tools are offered under the Microsoft 365 Defender umbrella as shown in the image below.

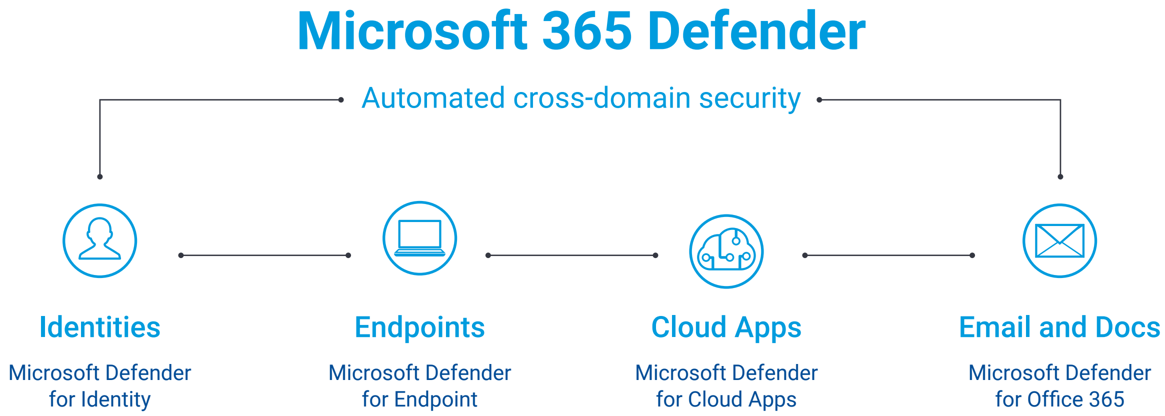

Microsoft 365 Defender
Automated cross-domain security
Identities
Microsoft Defender for Identity
Endpoints
Microsoft Defender for Endpoint
Cloud Apps
Microsoft Defender for Cloud Apps
Email and Docs
Microsoft Defender for Office 365

Figure 1: Microsoft 365 Defender Solutions

Overview of
Microsoft Security Solutions

While these solutions provide a high level of protection, many customers need to correlate the threat information from these solutions and view them along with the data obtained from other non-Microsoft applications. In order to provide the cross-domain and cross-application visibility and to help Security Operations Center (SOC) operators address threats, Microsoft has a solution called Sentinel, which is both a Security Information Event Management (SIEM) and a Security Orchestration Automated Response (SOAR) solution.

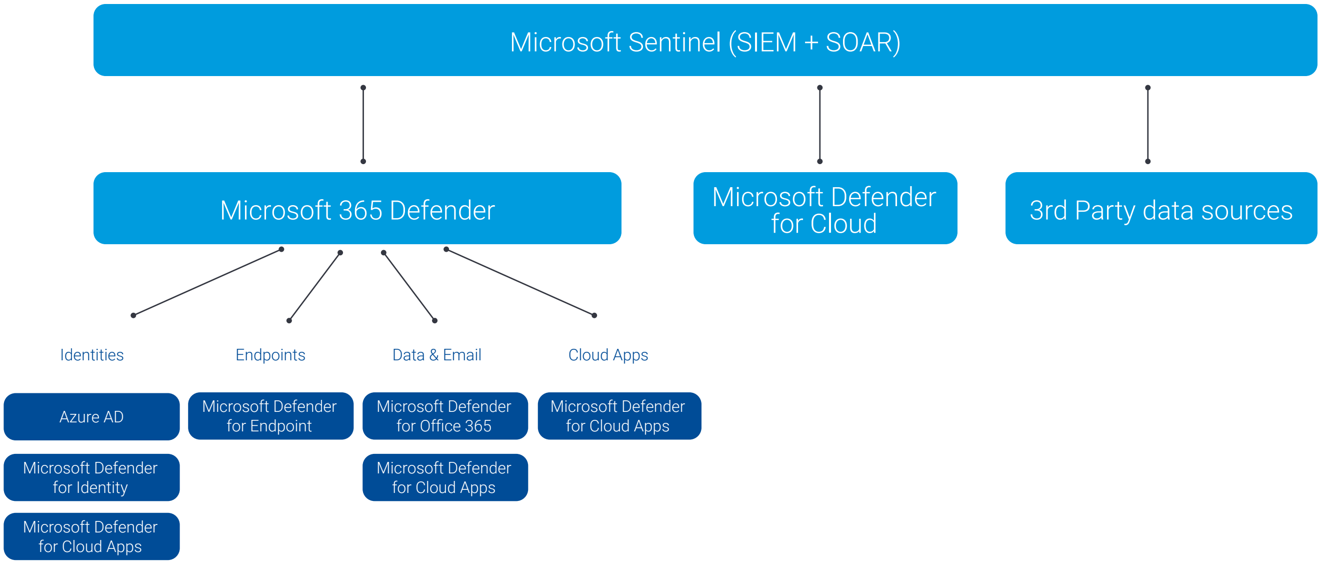

Microsoft Sentinel (SIEM + SOAR)
Microsoft 365 Defender
Microsoft Defender for Cloud
3rd Party data sources
Identities
Endpoints
Data & Email
Cloud Apps
Azure AD
Microsoft Defender for Endpoint
Microsoft Defender for Office 365
Microsoft Defender for Cloud Apps
Microsoft Defender for Identity
Microsoft Defender for Cloud Apps
Microsoft Defender for Cloud Apps

Figure 2: Microsoft Sentinel and Microsoft Defender

Importance of identity in threat detection and response

Over the past few years, with corporate network boundaries blurring, identity has become the new perimeter. Most attackers target identity solutions as a means to gain malicious access. In fact, according to the 2021 Verizon Data Breach report, phishing and credential abuse were the leading causes of data breach (60% of all breaches). Once an organization has been compromised, the average time to identify a breach was 228 days in 2020 according to IBM's Cost of Data Breach report. The same report also states that the average time to contain a breach was 80 days. Another report from Symantec also stated that nearly half of all malicious attachments were Microsoft Office files. Clearly a lot of data points towards identity being a key vector used in initiating and propagating data breaches.

Risk of days lost in a breach

For many organizations, it is a matter of when, rather than whether, they will be breached. Security operators have to work with two simultaneous questions in mind – how soon can I detect a breach and once detected, how quickly can I recover from it? Every day lost in detecting and in responding increases the cost and complexity of the breach and the recovery process. For example, The CRITICAL**START® SOC sees on average over 14,000 alerts per customer per day. Most organization security teams are understaffed, making it extremely difficult for all alerts to be addressed. There is significant alert fatigue and as a result most alerts will not be investigated and simply ignored. Additionally, SOC operators face a burgeoning backlog of alerts to process.**

When an attacker breaches the organization, each day that they go undetected presents additional risks. Typical attackers accumulate privileges as they dwell in the system. Once they have accumulated sufficient privileges and, in some instances, elevated access to certain applications, they launch their next steps – some form of data exfiltration or denial of access in exchange for ransomware. From an organization's perspective, they will have to ensure that they address all alerts they receive in a day. In order to do so, they can either:

- ✓ increase the staff on hand or
- ✓ automate the alert detection and some parts of the alert remediation process or
- ✓ a combination of the two

In order to automate the alert detection and remediation process, operators must be provided tools that will help automatically triage alerts. This will let the operators focus on specific alerts that need manual intervention. Secondly, the tools that are provided to the SOC operators must simplify the manual triage process.

Detecting and Responding to Identity-Based threats with Microsoft Security Tools

In a Microsoft environment, we discussed the various tools that are available as part of the Defender suite of products. The key flexibility offered by the Microsoft security suite to a SOC operator is also a drawback. Each of the Defender products have their own dashboards by virtue of Microsoft's flexible licensing options. Further, the products require specific expertise which make it hard to users to leverage unless they have gone through the requisite training. For example, let's consider that an operator receives an identity-based alert such as impossible time travel alert – a user logs in from one location and after 30 minutes logs in from a completely different part of the world. The first step would be to check who the user is. Once the user has been identified, it would be necessary to see which device the user used. From there you may want to determine if that device was compromised in any way. And additionally the operator may want to confirm if the user had accessed any other application in the same pattern. From a SOC operator's perspective, this would mean navigating from Defender for Identity, Defender for Endpoint, and Microsoft Sentinel at the very least. In each of these instances, it is important that the operator is well qualified and trained in all the products from Microsoft in order to address the threat. This requires significant time, money and effort.

Process of identity detection and response using Critical Start ZTAP® – a single portal

With the use of Critical Start Zero-Trust Analytics Platform® (ZTAP®) platform, many of these complexities are solved.

ZTAP provides two key functionalities:

1. Automates the detection process by addressing all the alerts – irrespective of whether they are Critical, High, Medium or Low.
2. Provides a consolidated view of the alert and the associated fields from other Microsoft products. For example, a SOC analyst will be able to obtain in-depth information about an impossible time travel alert, and view information from Defender for Endpoint, Defender for Identity and Microsoft Sentinel without having to navigate to each of their portals. These are also accessible via a mobile application.

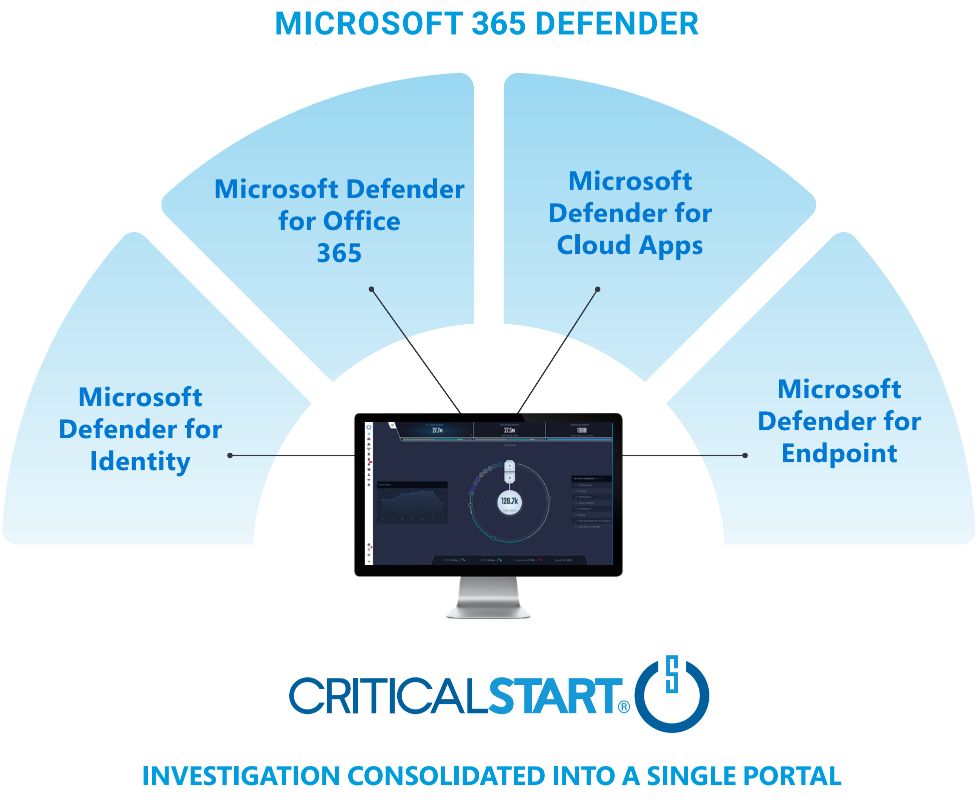

MICROSOFT 365 DEFENDER
Microsoft Defender for Office 365
Microsoft Defender for Cloud Apps
Microsoft Defender for Identity
Microsoft Defender for Endpoint
CRITICALSTART®
INVESTIGATION CONSOLIDATED INTO A SINGLE PORTAL

Figure 3: Consolidated View with Critical Start

Cost & Time Savings from Critical Start ZTAP

The process followed by Critical Start ZTAP provides both cost and time savings. It has been evident that the number of attacks are on the increase. This has resulted in more alerts:

- ✓ **real alerts generated as a result of anomalous activities and**
- ✓ **false positives and false negatives generated as a result of improperly tuned security controls and confidence levels**

In all of these cases, the burden on the SOC analyst increases. This burden can be quantified in both cost and time.

Time Savings

In the case of identity based alerts, Critical Start provides a single pane of glass across all Microsoft security solutions. This drastically reduces the time it takes to triage an alert. In the absence of Critical Start, an analyst spends at least 15 minutes to triage an alert. Lets take an example of an impossible time travel alert. An analyst will have to follow at least the following steps:

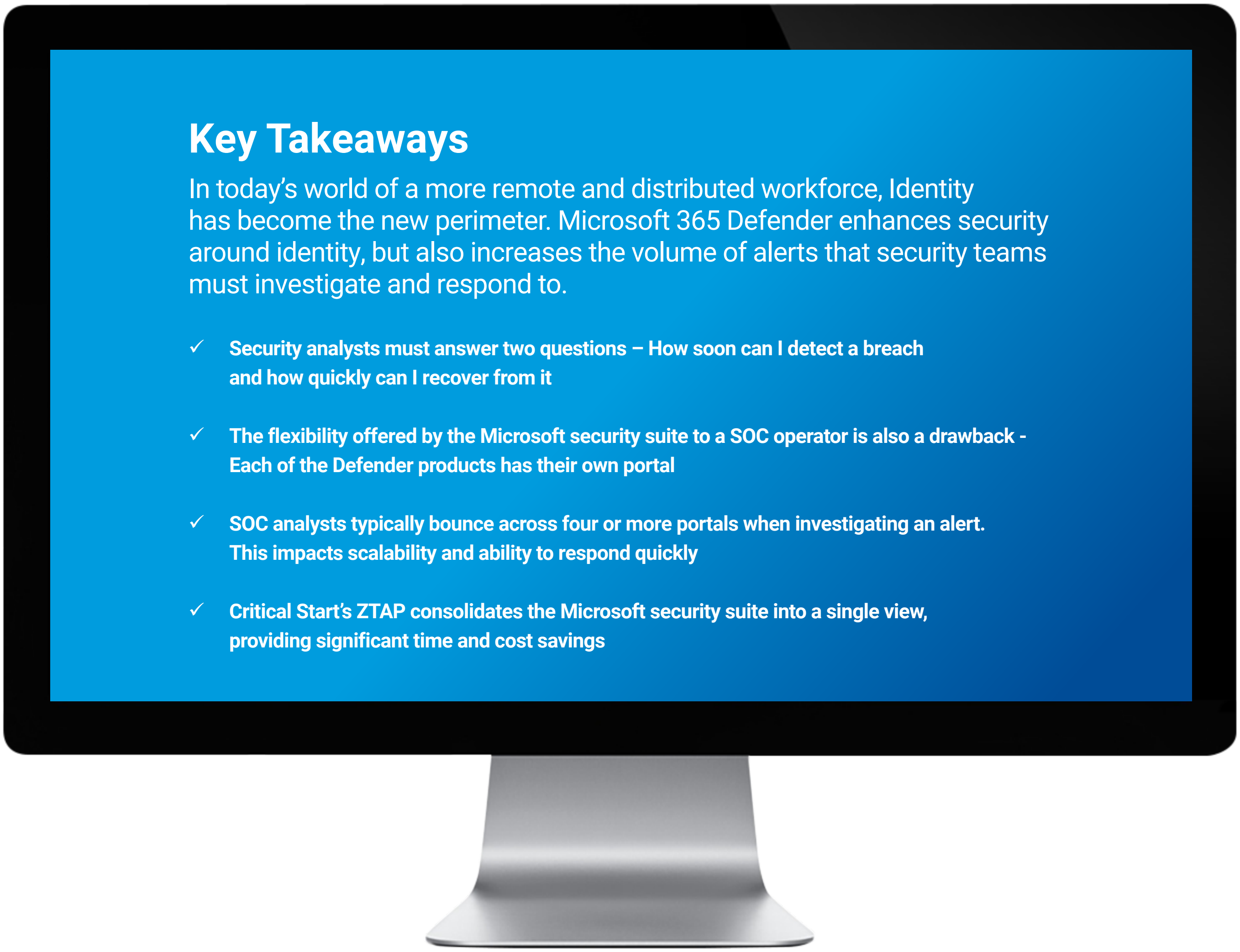
- ✓ **Log into Azure Active Directory Identity Protection and review the alert**
- ✓ **Log into Microsoft Sentinel (if licensed) to review other accesses by the user**
- ✓ **Log into Microsoft Defender for Endpoint to determine the status of the device from which the user logged in**
- ✓ **Verify the user's login activity in on-premises solutions in Defender for Identity**

For each of the steps above, the underlying assumption is that the analyst has enough knowledge about each of these solutions and knows exactly what information to look for and how to correlate the events in each solution.

With Critical Start, the customer just needs to review an event and all the corresponding events in the other Microsoft security solutions are automatically referenced. In analyzing past Critical Start customer data, we estimate that the time taken to triage an alert using Critical Start is less than 2 minutes. This represents an 87% time saving per alert.

Cost Savings

As ZTAP is completely automated and tuned based, it provides near 100% coverage of all alerts in a given day. Organizations no longer have to consider prioritizing only High and Critical alerts and can instead cover all categories of alerts in a day. Because ZTAP covers all alerts in a day, analyst resources can be leveraged in the most productive manner in an organization. Analysts can focus on true escalations and on other higher value activities. In the same example of an impossible time travel alert, a security analyst would save 13 minutes in triaging an alert. If an organization had 32 alerts a day to triage, that would result in one day's work for a full time SOC analyst without Critical Start. It would take a little over one hour for the same SOC analyst with Critical Start. As a result, an organization needs far fewer analyst hours to triage alerts can either be realized as a cost savings and an increase in productivity as the rest of the analyst time can be redeployed to more productive initiatives.



Key Takeaways

In today's world of a more remote and distributed workforce, Identity has become the new perimeter. Microsoft 365 Defender enhances security around identity, but also increases the volume of alerts that security teams must investigate and respond to.

- ✓ **Security analysts must answer two questions – How soon can I detect a breach and how quickly can I recover from it**
- ✓ **The flexibility offered by the Microsoft security suite to a SOC operator is also a drawback - Each of the Defender products has their own portal**
- ✓ **SOC analysts typically bounce across four or more portals when investigating an alert. This impacts scalability and ability to respond quickly**
- ✓ **Critical Start's ZTAP consolidates the Microsoft security suite into a single view, providing significant time and cost savings**

Visit **criticalstart.com** for more information.