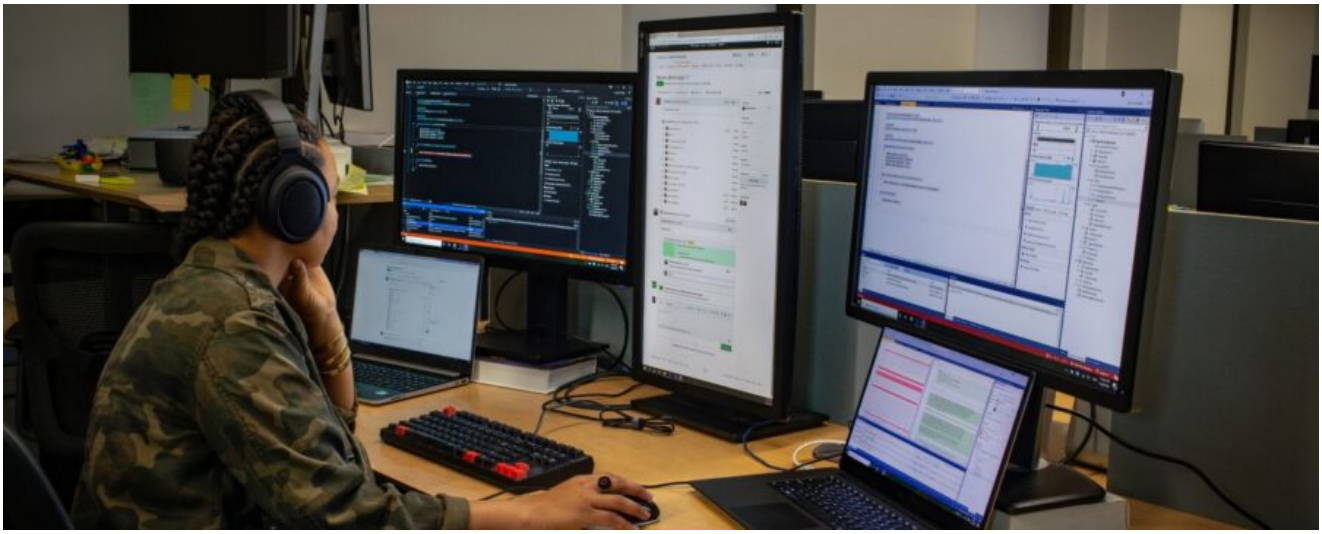
A guide to combatting human-operated ransomware: Part 1

microsoft.com/security/blog/2021/09/20/a-guide-to-combatting-human-operated-ransomware-part-1/

September 20, 2021



This blog is part one of a two-part series focused on how Microsoft DART helps customers with human-operated ransomware. For more guidance on human-operated ransomware and how to defend against these extortion-based attacks, refer to our human-operated ransomware docs page.

Microsoft's Detection and Response Team (DART) has helped customers of all sizes, across many industries and regions, investigate and remediate human-operated ransomware for over five years. This blog aims to explain the process and execution used in our customer engagements to provide perspective on the unique issues and challenges regarding human-operated ransomware. We will also discuss how DART leverages Microsoft solutions such as Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Cloud App Security (MCAS) within customer environments while collaborating with cross-functional threat intelligence teams across Microsoft who similarly track human-operated ransomware activities and behaviors.

Human-operated ransomware is not a malicious software problem—it's a human criminal problem. The solutions used to address commodity problems aren't enough to prevent a threat that more closely resembles a nation-state threat actor. It disables or uninstalls your antivirus software before encrypting files. They locate and corrupt or delete backups before sending a ransom demand. These actions are commonly done with legitimate programs that you might already have in your environment and are not considered malicious. In criminal hands, these tools are used maliciously to carry out attacks.

Responding to the increasing threat of ransomware requires a combination of modern enterprise configuration, up-to-date security products, and the vigilance of trained security staff to detect and respond to the threats before data is lost.

Key steps in DART's approach to conducting ransomware incident investigations

To maximize DART's efforts to restore business continuity while simultaneously analyzing the details of the incident, a careful and thorough investigation is coordinated with remediation measures to ensure that the root cause is determined. These efforts take place as we assist and advise customers with the task of getting the organization up and running again in a secure manner.

Every effort is made to determine how the adversary gained access to the customer's assets so that vulnerabilities can be remediated. Otherwise, it is highly likely that the same type of attack will take place again in the future. In some cases, the threat actor takes steps to "cover their tracks" and destroy evidence, so it is possible that the entire chain of events may not be evident.

The following are three key steps in our ransomware investigations:

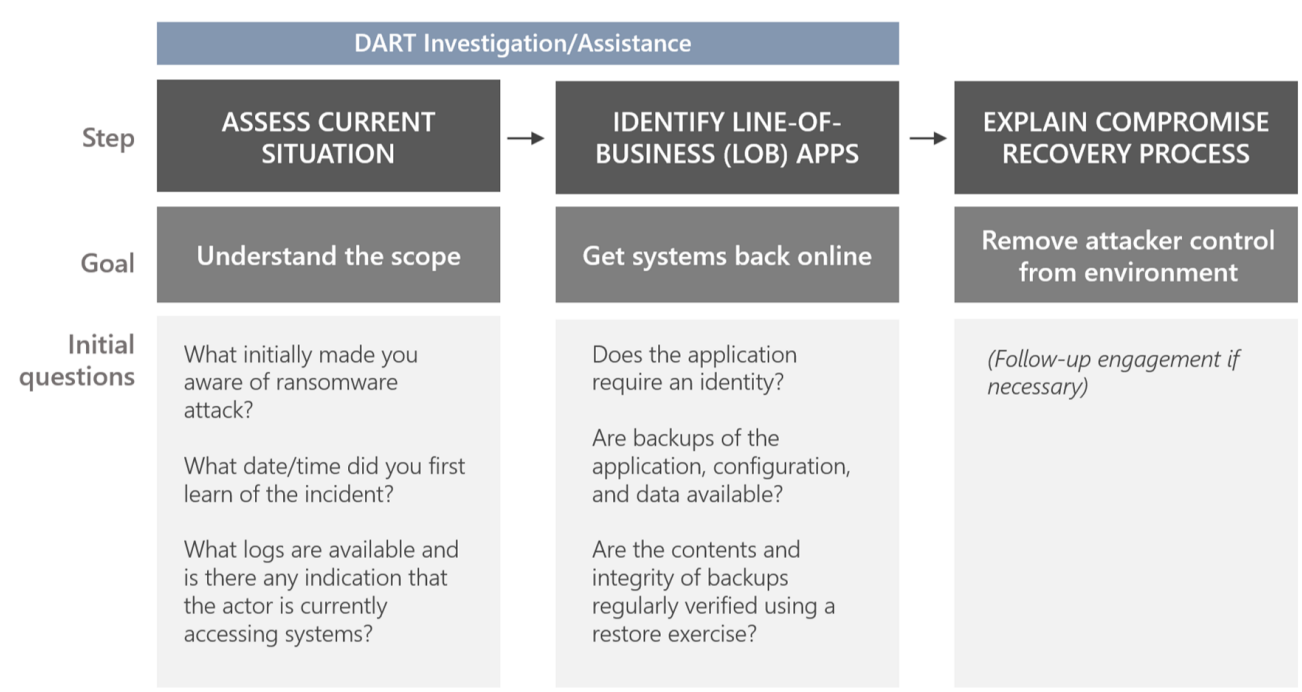


Figure 1. Key steps in DART's ransomware investigations.

1. Assess the current situation

This is critical to understanding the scope of the incident and for determining the best people to assist and to plan and scope the investigation and remediation tasks. Asking these initial questions is crucial in helping us determine the situation being dealt with:

What initially made you aware of the ransomware attack?

If the initial threat was identified by IT staff (like noticing backups being deleted, antivirus (AV) alert, endpoint detection and response (EDR) alert, suspicious system changes), it is often possible to take quick decisive measures to thwart the attack, typically by disabling all inbound and outbound internet communication. This may temporarily affect business operations, but that would typically be much less impactful than an adversary deploying ransomware.

If the threat was identified by a user call to the IT helpdesk, there may be enough advance warning to take defensive measures to prevent or minimize the effects of the attack. If the threat was identified by an external entity (like law enforcement or a financial institution), it is likely that the damage is already done, and you will see evidence in your environment that the threat actor has already gained administrative control of your network. This can range from ransomware notes, locked screens, or ransom demands.

What date/time did you first learn of the incident?

Establishing the initial activity date and time is important because it helps narrow the scope of the initial triage for "quick wins." Additional questions may include:

- What updates were missing on that date? This is important to understand what vulnerabilities may have been exploited by the adversary.
- What accounts were used on that date?
- What new accounts have been created since that date?

What logs (such as AV, EDR, and VPN) are available, and is there any indication that the actor is currently accessing systems?

Logs are an indicator of suspected compromise. Follow-up questions may include:

- Are logs being aggregated in a SIEM (like Microsoft Azure Sentinel, Splunk, ArcSight) and current? What is the retention period of this data?
- Are there any suspected compromised systems that are experiencing unusual activity?
- Are there any suspected compromised accounts that appear to be actively used by the adversary?
- Is there any evidence of active command and controls (C2s) in EDR, Firewall, VPN, Proxy, and other logs?

As part of assessing the current situation, DART may require a domain controller (DC) that was not ransomed, a recent backup of a DC, or a recent DC taken offline for maintenance/upgrades. We also ask our customers whether multifactor authentication (MFA) was required for everyone in the company and if Microsoft Azure Active Directory was used.

2. Identify line-of-business (LOB) apps that are unavailable due to the incident

This step is critical in figuring out the quickest way to get systems back online while obtaining the evidence required.

Does the application require an identity?

- How is authentication performed?
- How are credentials such as certificates or secrets stored and managed?

Are tested backups of the application, configuration, and data available?

Are the contents and integrity of backups regularly verified using a restore exercise? This is particularly important after configuration management changes or version upgrades.

3. Explain the compromise recovery (CR) process

This is a follow-up engagement that may be necessary if DART determines that the control plane (typically Active Directory) has been compromised.

DART's investigation always has a goal of providing output that feeds directly into the CR process. CR is the process by which we remove the nefarious attacker control from an environment and tactically increase security posture within a set period. CR takes place post-security breach. To learn more about CR, read the Microsoft Compromise Recovery Security Practice team's blog CRSP: The emergency team fighting cyber attacks beside customers.

Once we have gathered the responses to the questions above, we can build a list of tasks and assign owners. A key factor in a successful incident response engagement is thorough, detailed documentation of each work item (such as the owner, status, findings, date, and time), making the compilation of findings at the end of the engagement a straightforward process.

How DART leverages Microsoft security solutions to combat human-operated ransomware

DART leverages cross-functional teams, such as internal threat intelligence teams, who track adversary activities and behaviors, customer support, and product development teams behind Microsoft products and services. DART also collaborates with other incident response vendors the customer may have engaged and will share findings whenever possible.

DART relies heavily on data for all investigations. The team uses existing deployments of Microsoft solutions, such as Defender for Endpoint, Defender for Identity, and MCAS within customer environments along with custom forensic data collection for additional analysis. If these sensors are not deployed, DART also requests that the customer deploy these to gain deeper visibility into the environment, correlate against threat intelligence sources, and enable our analysts to scale in speed and agility.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is Microsoft's enterprise endpoint security platform designed to help enterprise network security analysts prevent, detect, investigate, and respond to advanced threats. As shown in the image below, Defender for Endpoint can detect attacks using advanced behavioral analytics and machine learning. DART analysts use Defender for Endpoint for attacker behavioral analytics.

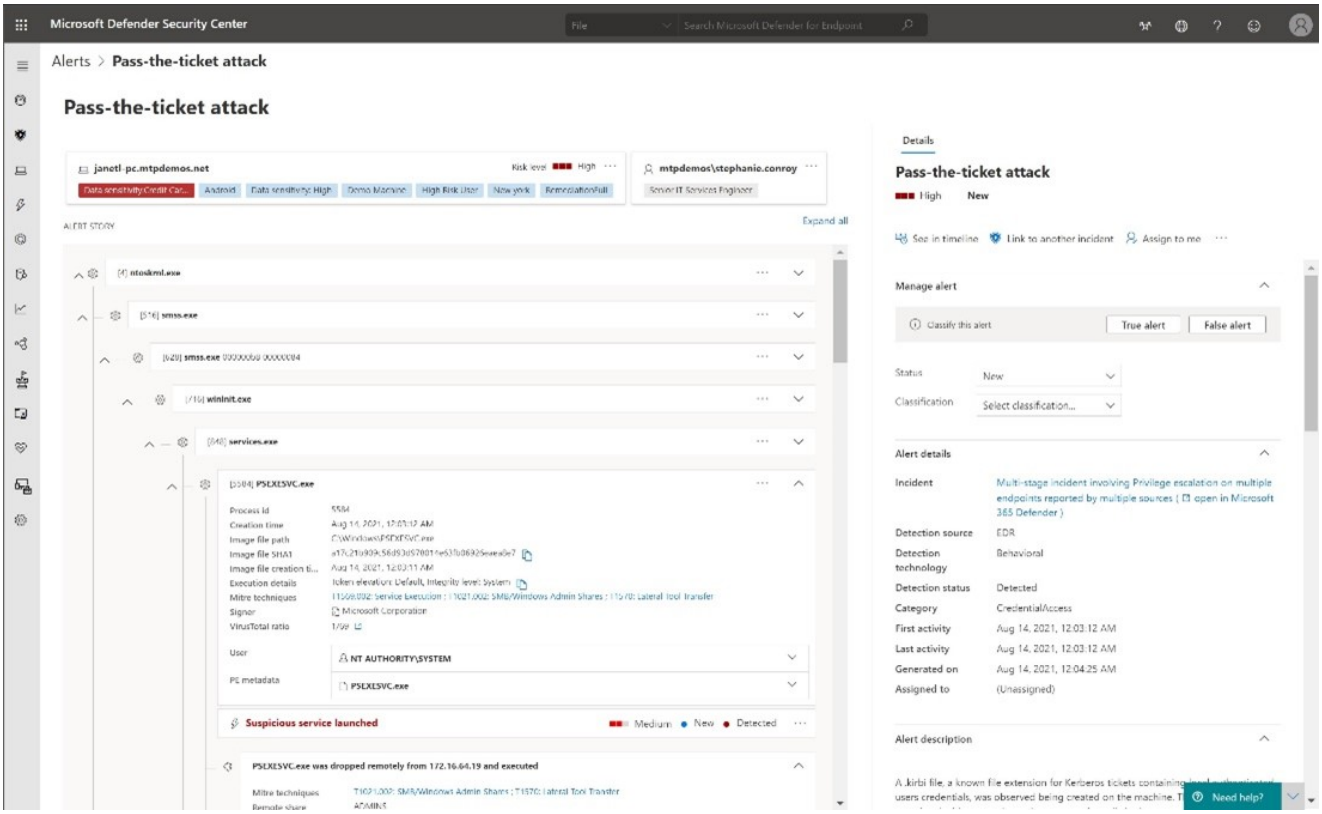


Figure 2. Sample alert in Microsoft Defender for Endpoint for a pass-the-ticket attack.

DART analysts can also perform advanced hunting queries to pivot off indicators of compromise (IOCs) or search for known behavior if a threat actor group is identified.

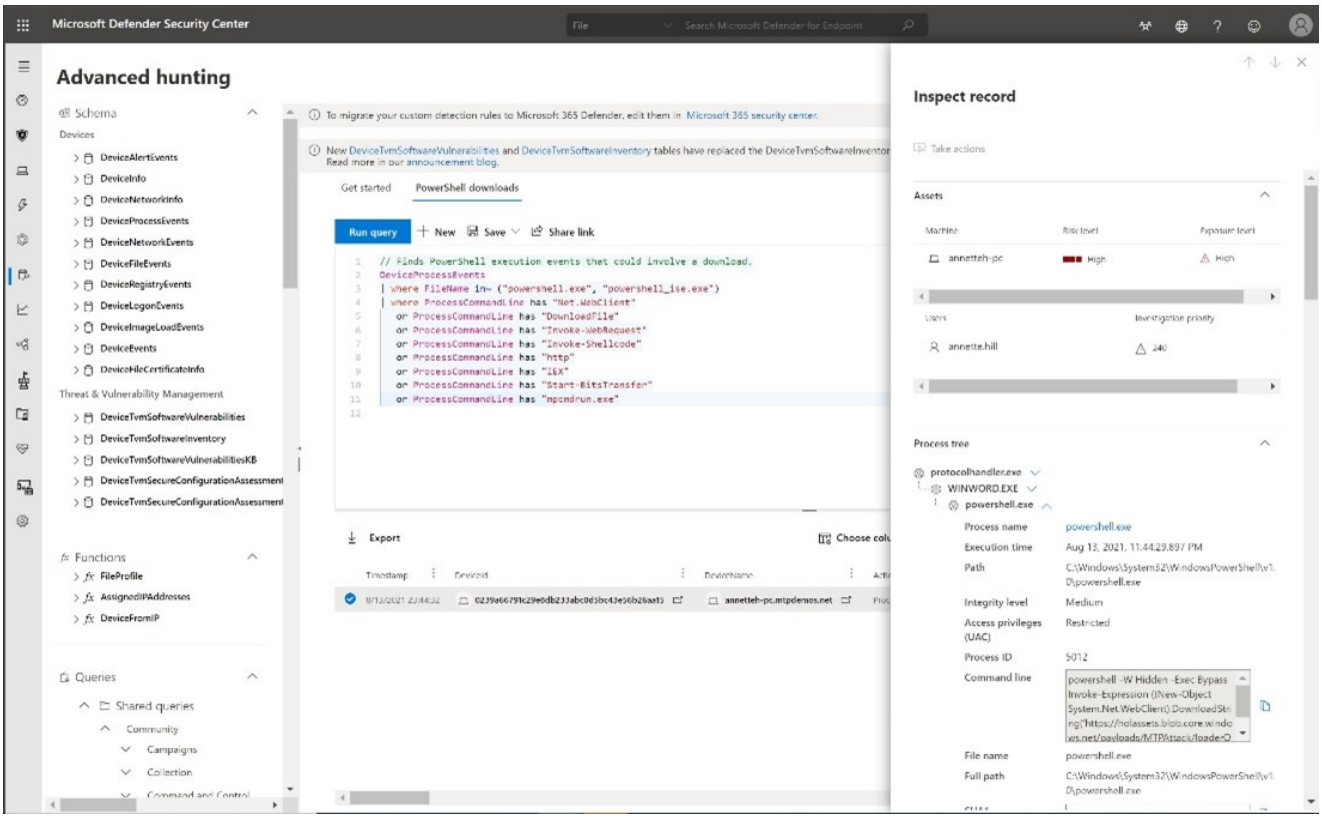


Figure 3. Advanced hunting queries to locate known attacker behavior.

In Defender for Endpoint, customers have access to a real-time expert-level monitoring and analysis service by Microsoft Threat Experts for ongoing suspected actor activity. Customers can also collaborate with experts on demand for additional insights into alerts and incidents.

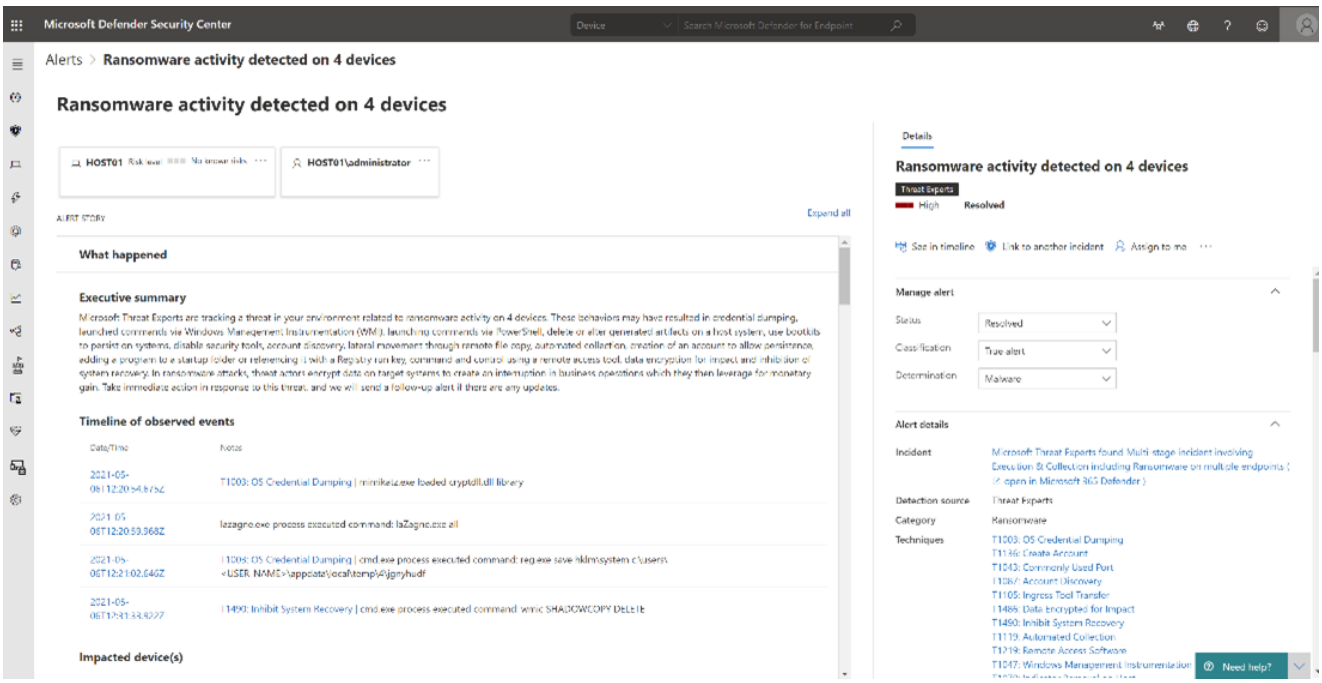


Figure 4. Defender for Endpoint shows detailed ransomware activity.

Microsoft Defender for Identity

DART leverages Microsoft Defender for Identity to investigate known compromised accounts and to find potentially compromised accounts in your organization. Defender for Identity sends alerts for known malicious activity that actors often use such as DCSync attacks, remote code execution attempts, and pass-the-hash attacks. Defender for Identity enables our team to pinpoint nefarious activity and accounts to narrow down our investigation.

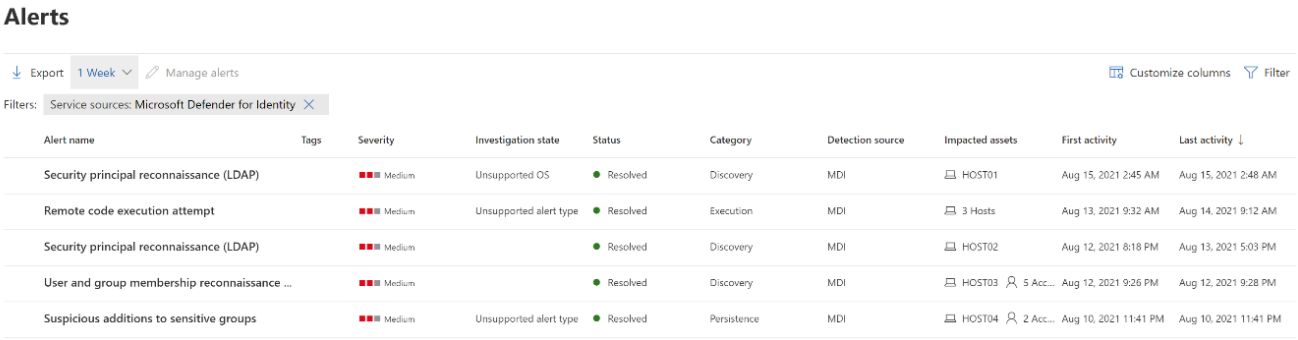


Figure 5. Defender for Identity sends alerts for known malicious activity related to ransomware attacks.

Microsoft Cloud App Security

MCAS allows DART analysts to detect unusual behavior across cloud apps to identify ransomware, compromised users, or rogue applications. MCAS is Microsoft's cloud access security broker (CASB) solution that allows for monitoring of cloud services and data access in cloud services by users.

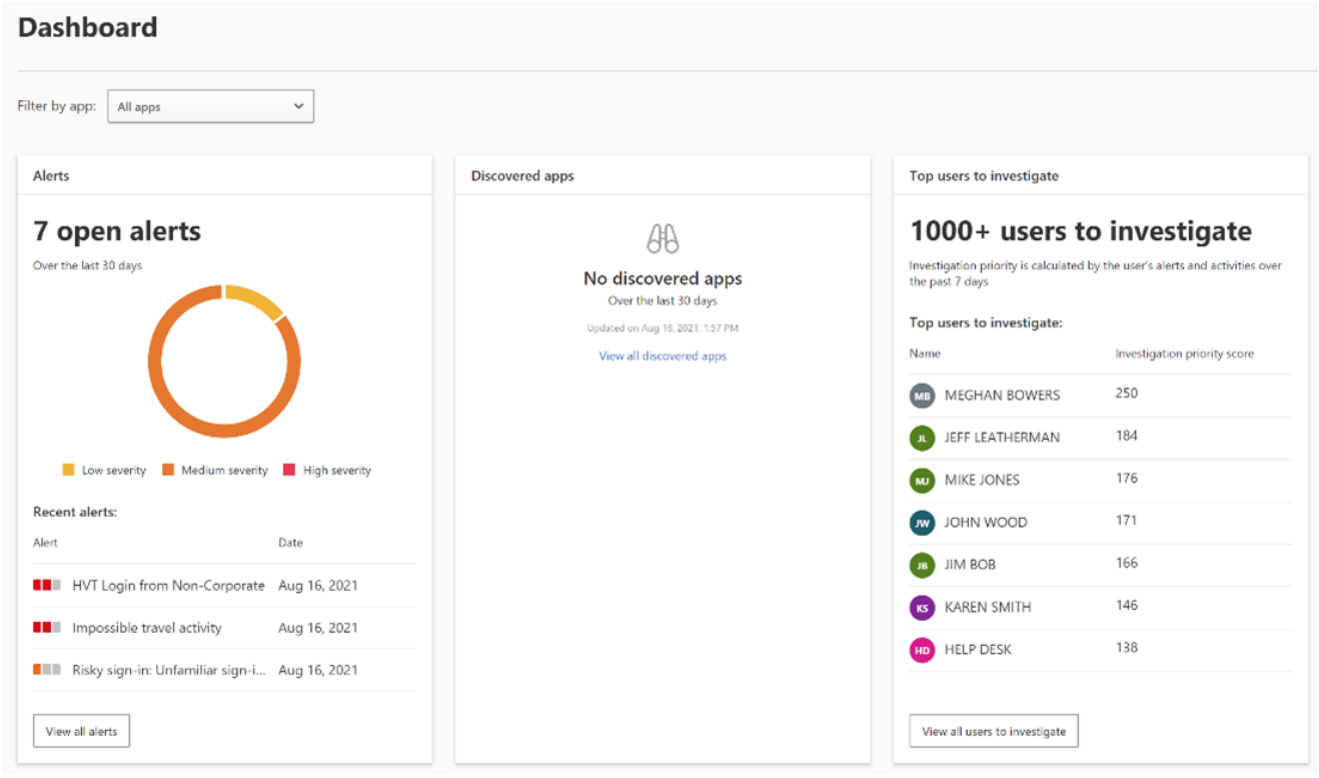


Figure 6. The Microsoft Cloud App Security dashboard allows DART analysis to detect unusual behavior across cloud apps.

Microsoft Secure Score

The Microsoft 365 Defender stack provides live remediation recommendations to reduce the attack surface. Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more improvement actions taken. Refer to our documentation to find out more about how your organization can leverage this feature to prioritize remediation actions that are based on their environment.

Understand your business risks

Beyond the immediate risk of encrypted files, understanding the disruption to business operations, data theft, extortion, follow-on attacks, regulatory and compliance reporting, and damage to reputation fall outside technical controls. Microsoft DART recommends each organization weigh these risks when determining the appropriate way to respond based on the organization's policies, risk appetite, and applicable regulatory requirements.

Microsoft Defender for Endpoint, Microsoft Defender for Identity, and MCAS all work seamlessly together to provide customers with enhanced visibility of the attacker's actions within and investigate attacks. Given our vast experience and expertise in investigating countless human-operated ransomware events over the past few years, we have shared what we consider best practices.

Learn more

Want to learn more about DART? Read our past blog posts.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us at @MSFTSecurity for the latest news and updates on cybersecurity.