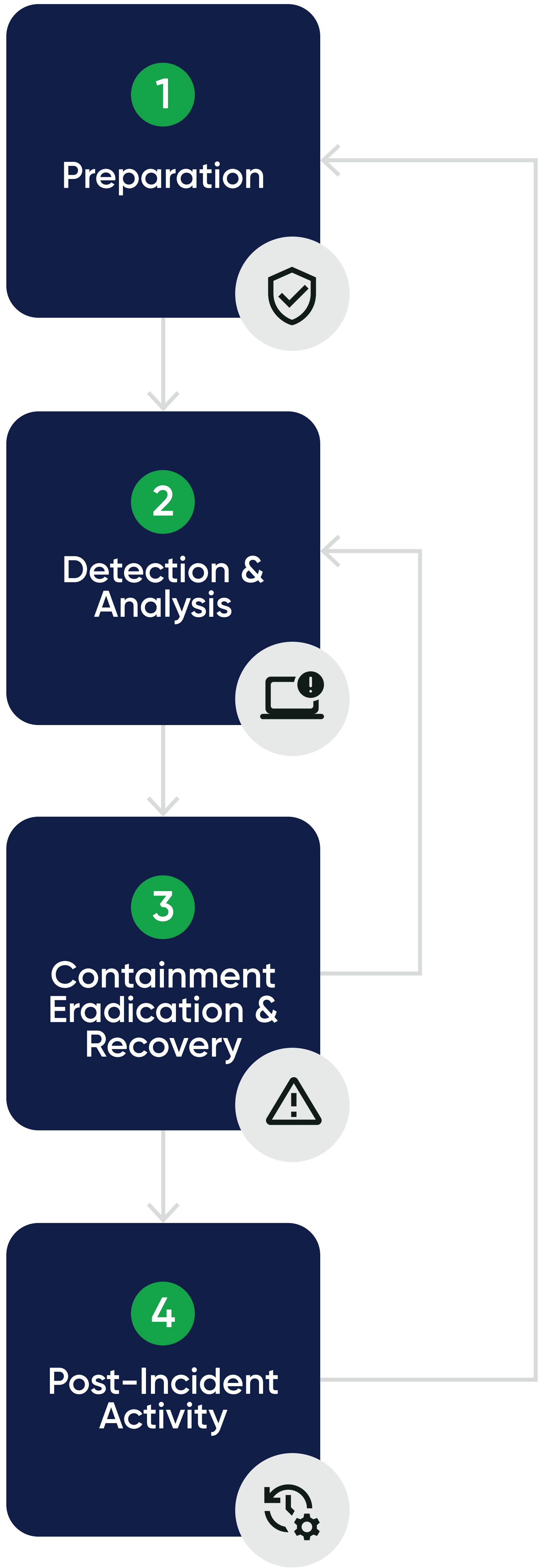
WHITE PAPER

Absolute Ransomware Response Playbook

Enable a Confident, Efficient, and Reliable Response in the Event of a Ransomware Attack

Unlike other security incidents, Ransomware puts organizations on a countdown timer. Decisions need to be made swiftly and in an orderly fashion. Any delay in the decision-making process can lead to devastating consequences such as public disclosure or permanent data loss. Thus, it is critical for organizations to prepare in advance by developing a Ransomware Response Playbook. This playbook can guide incident response activities and ensure they are carried out as efficiently and effectively as possible.



Introduction

This Absolute Ransomware Response Playbook document is structured based on the four-phase Incident Response Lifecycle defined in **NIST SP800-61 rev2**:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity

This document explains how to apply the Absolute Ransomware Response offering to each phase of the Incident Response Lifecycle, with a specific focus on endpoint recovery. The goal is to strengthen an organization's pre-incident readiness and to enable a confident, efficient, and reliable response in the event of a ransomware attack. By following a step-by-step process, endpoint recovery becomes a more straightforward and streamlined procedure, rather than an ad-hoc improvisation, allowing organizations to recover more quickly from a ransomware attack than they might otherwise be able to.

Scope and Purpose

The scope of the Playbook is pre-incident preparedness and in-incident response for an organization's Windows endpoints. Thus, it is intended to augment, not replace, the organization's broader Incident Response Plan (IRP), which would address additional endpoint types and other systems and services (e.g., Active Directory, business applications).

For each phase of the Incident Response Lifecycle, this Playbook describes a combination of capabilities and services provided by Absolute under its Ransomware Response offering that help ensure an organization's overall playbook may be executed as intended. This applies in particular to attacks that employ one or more of the following MITRE ATT&CK techniques in order to thwart an organization's execution of the 'Detection and Analysis' as well as 'Containment, Eradication, and Response' phases:

- T1562 Impair Defenses
- TA003 Persistence
- T1027 Obfuscated Files or Information
- TA008 Lateral Movement

Absolute Ransomware Response is uniquely able to remediate attacks employing these techniques because it is based on Absolute's unique and patented Persistence™ technology, which is embedded in the firmware of more than 600 million devices of leading system manufacturers worldwide. Leveraging this technology, our endpoint security agent (the "Absolute Agent") may always be restored to operation, even if an attacker or malware attempts to remove or disrupt its intended operation. The Absolute Agent begins its execution at the earliest possible point in the operating system boot cycle – earlier than other security and management tools or ransomware itself. As a result, Absolute can execute critical tasks uninterrupted, such as identifying affected endpoints, applying containment, restoring and updating impaired defenses and OS services, and removing infected files. This ensures that an organization's overall playbook may be successfully executed as expeditiously as possible.

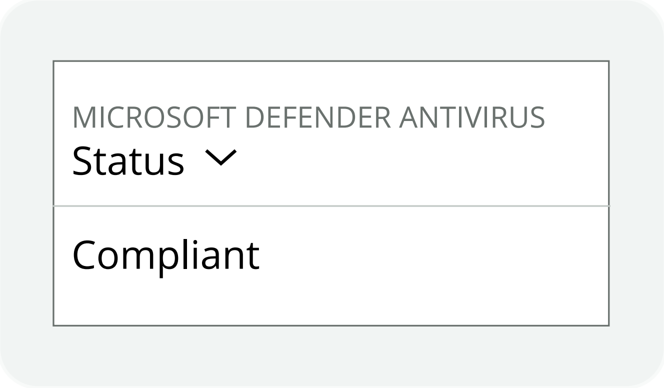
Four Phases of Ransomware Incident Response Lifecyle

As outlined above, there are four phases in the Incident Response Lifecycle — *Preparation; Detection and Analysis; Containment, Eradication, and Recovery*; and *Post-Incident Activity*. The following sections outline where and how capabilities and services enabled by the Absolute Ransomware Response offering may be applied in each phase.

1. Preparation

During the Preparation phase, Absolute offers assessment services to help organizations prepare for potential incidents. The assessment aims to ensure that organizations not only reduce their likelihood of experiencing an incident but also develop the capability to respond quickly and effectively if they are attacked. The Preparation phase is critical to enhancing an organization's security posture. Preparation steps where Absolute's service and product capabilities may be employed are described below.

Enabling Absolute Application Resilience

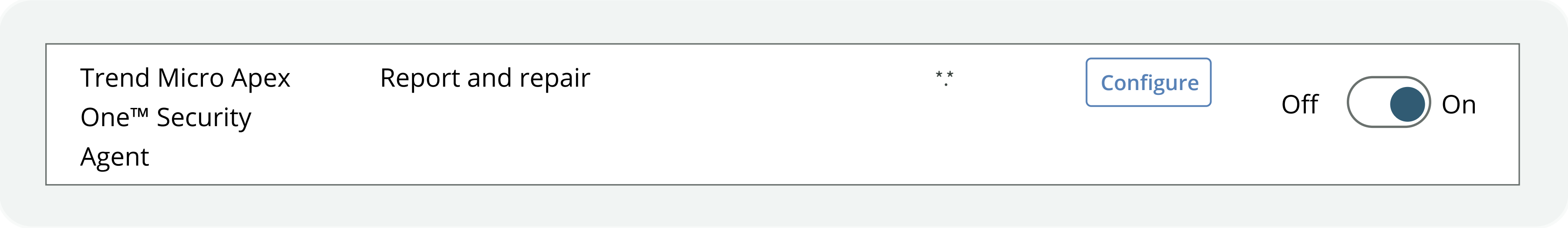


MICROSOFT DEFENDER ANTIVIRUS
Status

Compliant

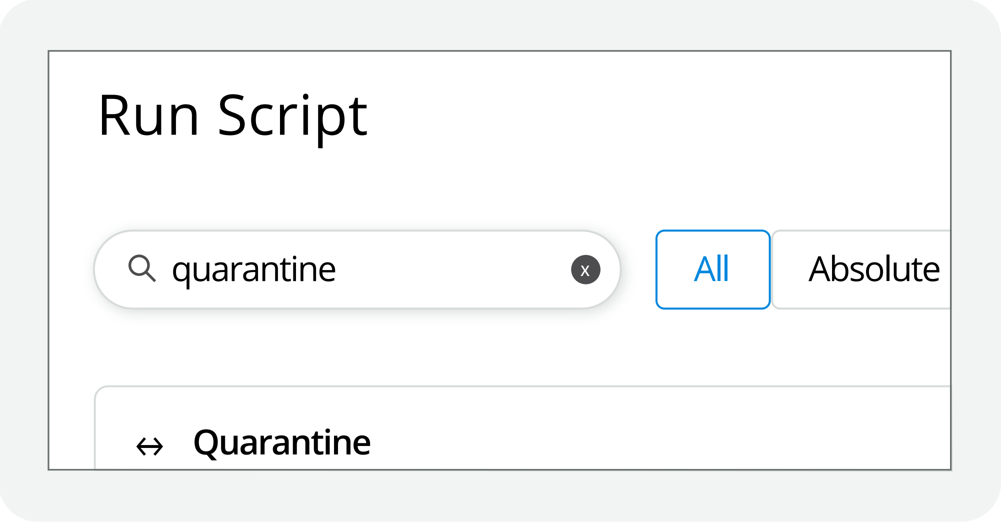
Absolute Ransomware Response includes Absolute Application Resilience™, a capability that monitors application health and automatically repairs and/or re-installs unhealthy third-party applications listed in the Application Resilience catalog to restore them to healthy operations. In the event that an organization's Unified Endpoint Management (UEM), Endpoint Protection Platform (EPP), and Endpoint Detection and Response (EDR) tool is not present, not updated to the latest version, or not running correctly, Absolute Application Resilience repairs or re-installs the applications. This key capability of Absolute Ransomware Response decreases the probability that malware enters an organization's environment through an endpoint where its EPP/EDR tools were offline, and therefore unable to respond to a threat they could normally detect and contain.

During the assessment phase, Absolute's Professional Services team will work with the organization to identify critical Unified Endpoint Management and EPP/EDR tools and activate Absolute Application Resilience to enable automatic health reporting, repair, and re-installation.



Trend Micro Apex One™ Security Agent	Report and repair	Configure	Off ● On

Testing Quarantine Script

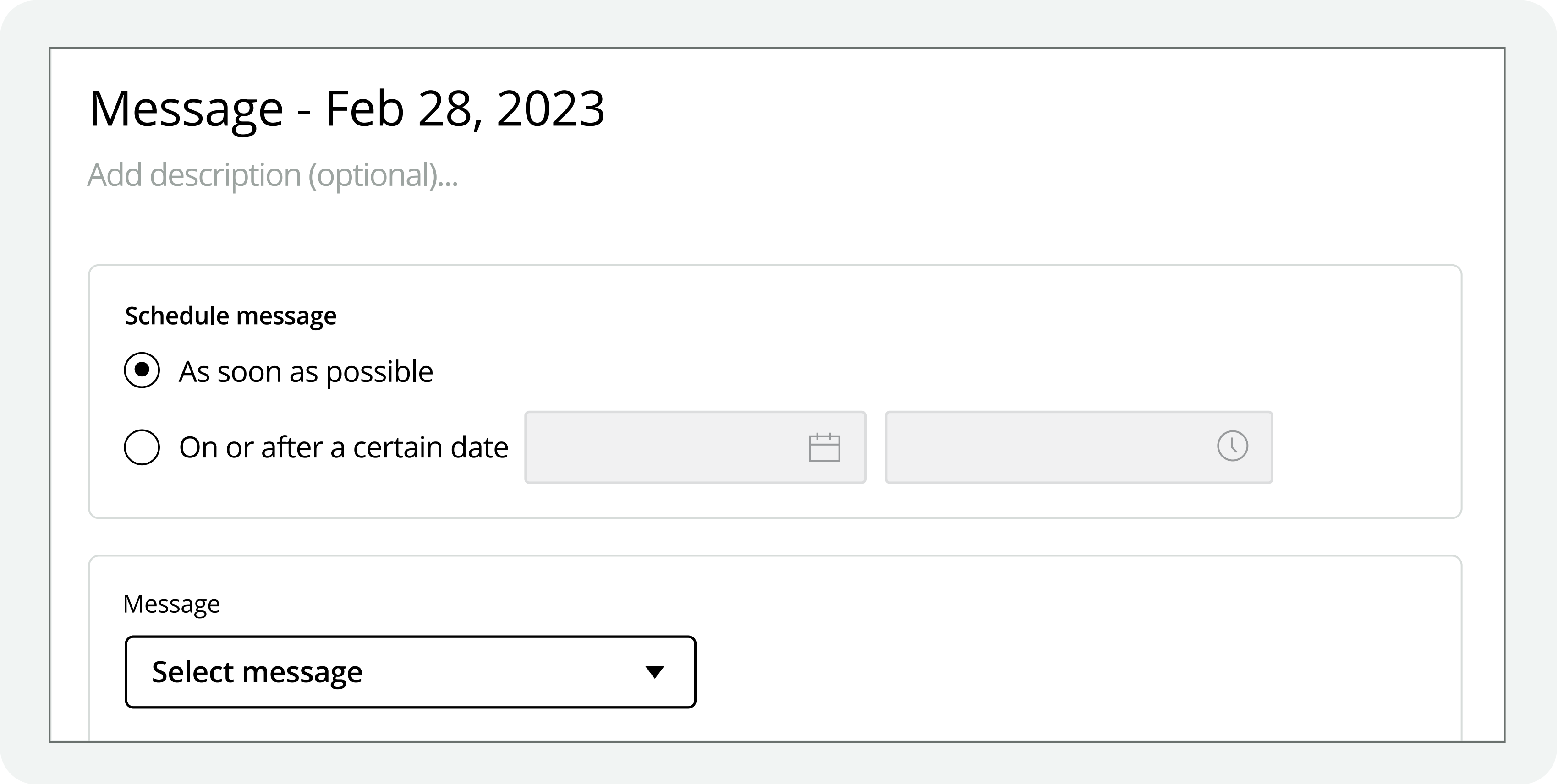


The Absolute Reach capability is used to remotely execute scripts on endpoints, individually or at scale. Among the hundreds of pre-defined scripts that Absolute has available for customers through its Reach library and knowledgebase is a quarantine script. This script locks down the network on a Windows endpoint, allowing access only for the Absolute Service and for any additional network addresses and ports required for remediation purposes. This blocks network access, while providing access to an organization's UEM, EPP/EDR, Data Recovery, or other tools utilized by its playbook. Having these scripts ready and configured with the desired list of exceptions is an important preparation step. It ensures that time is not lost obtaining the necessary networking details, building the correct exception list, and configuring the quarantine script accordingly. Finally, it is important to test the quarantine script to make sure that both the activation and deactivation work as expected.

```
<#
Extractable Script Comments
.SYNOPSIS This Quarantine script is designed to backup & encrypt the firewall settings, and lock down
```

Testing 'Discovery' Script Templates

The Absolute Reach capability may also be used to execute discovery scripts that identify infected endpoints through file hashes or other Indicators of Compromise (IoC), as determined in the 'Detection and Analysis' phase. Like the quarantine script, it is important to create and test templated versions of discovery scripts in advance of an actual incident to confirm that execution and collection procedures run as expected and at scale across the environment. During incident response, these scripts would need to be modified to reflect the particulars of the incident, such as by updating file hashes or locations, for example. However, it is easier and faster to do so if the script template has already been defined and the script is known to execute rapidly and at scale within the environment. Absolute's Assessment Services may be employed to assist in the definition and testing of templates specific to an organization's environment.



Message - Feb 28, 2023

Add description (optional)...

Schedule message

● As soon as possible

○ On or after a certain date

Message

Select message ▾

Preparing 'End User Messaging' Templates

Communicating with end users is an important part of incident response. Unfortunately, messaging and communications services like email, instant messaging, and team collaboration tools are often rendered inoperable because they are either a direct target or because they have been impacted by other outages. As further described below, the Absolute End User Messaging (EUM) capability maintains always-on communications with end users directly on their device. Absolute EUM can be used to inform users that an attack has occurred, that their endpoint(s) are or may have been compromised, and that their device may be subject to Device Freeze and other remediating actions. It is important to have message templates pre-defined and approved so that no time is lost in drafting or obtaining content approval prior to their use.

2. Detection and Analysis

The Detection and Analysis process aims to identify the ransomware variant and determine how it entered the network. Information gathered in this phase needs to be preserved and will be used in all following phases. A typical output of this phase would be identification of file signatures or other Indicator(s) of Compromise (IoC) associated with the now-known malware.

3. Containment, Eradication, and Recovery

These stages in the response lifecycle have the following objectives:

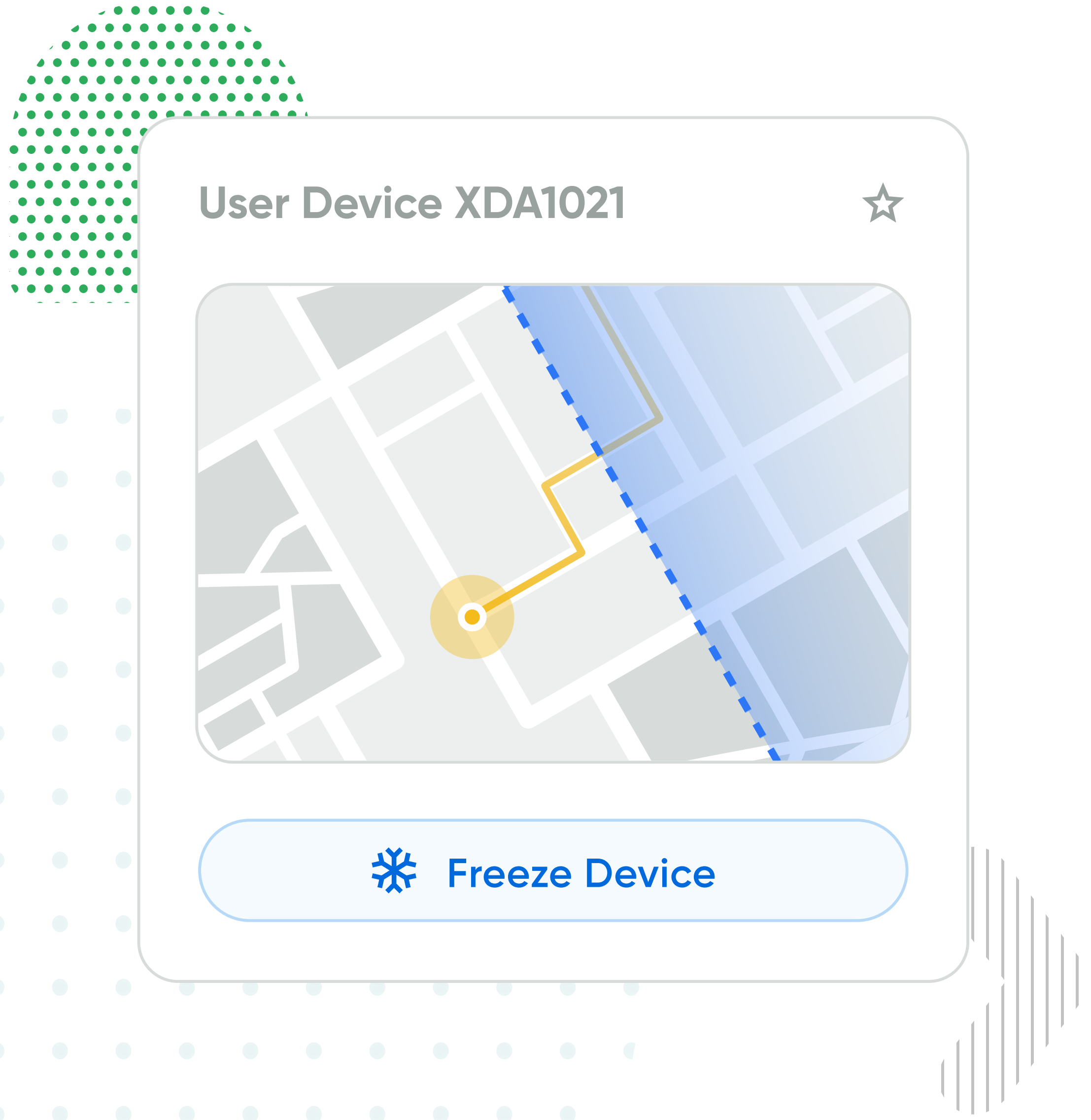
- **Containment** – focuses on stopping any further propagation of the attacker and/or malware throughout the network. Additional assistance from the infrastructure, network, and/or storage teams may be required. Any additional disruptions to operations required during the containment process must be communicated to the appropriate business groups via the communications lead.
- **Eradication** – focuses on eradicating all malicious actors and artifacts from the environment. It involves full system scans (including integrity of system configuration files), patching vulnerabilities, updates to threat intelligence tools, and submission of IoC to relevant third parties (e.g., MSSP/MDR provider).
- **Recovery** – focuses on recovery from the effects of the incident and a return to normal business operations.

The following sections describe how Absolute can assist in each of these phases, enabling a rapid and efficient response and return to normal business operations.

Containment

Identify Affected Hosts

A first critical step is to understand the scope of the infection across host types – e.g., endpoints, servers, and services – and the infection boundary (i.e., the extent of lateral sprawl). With respect to endpoint hosts, this step would involve identifying those with specific file signatures or other IoCs such as a combination of file location, file name, file hash, executing processes, and registry key-value pairs (or absence thereof) that were identified by incident responders during the ‘Detection and Analysis’ phase. Once a specific file signature or other IoCs have been determined, responders may modify previously tested and templatized Reach ‘Discovery’ scripts with specific discovery criteria to identify endpoints that have been infected by the ransomware and report back. **Once appropriate modifications have been made to the applicable ‘Discovery’ scripts, the time it takes to deploy a script to enrolled endpoints and collect data regarding the affected endpoints is typically on the order of 30 minutes.**



Isolate Affected Hosts

Upon successful identification of an affected endpoint host, an incident response team member should immediately isolate it. Simultaneously, other members can continue analysis of the particular strain, other IoCs, and the full extent of attack. As described above, the Reach 'Quarantine' script may be executed to isolate affected endpoints. Responders may also choose to approach the containment phase with an abundance of caution and proactively quarantine all enrolled endpoints, even before specific IoCs have been found. **Whether deploying on a targeted basis or to all endpoints, once the quarantine script is launched, it will take at most 15 minutes for online devices to execute the script and implement the quarantine. Offline devices will execute the script when they come online.**

*****IMPORTANT*****

Do NOT power off or restore machines without guidance from forensic investigators. Doing so may destroy valuable forensic data residing in memory or executing on disk. As outlined below, this instruction may be sent to users even if the endpoint has been frozen to prevent user interaction, or if other communications tools have been impacted by the attack and are not available for use.

Remove User Interaction

When an affected endpoint is successfully identified, it is crucial for a response team member to take immediate action by using the Absolute Device Freeze capability to freeze the device. This preserves the device's state and prevents the user from accidentally blemishing evidence or disrupting the recovery process. It's important to note that even well-meaning users can unintentionally cause harm by using the device, creating files, rebooting, or taking other actions.

Apart from preserving forensic evidence, the Device Freeze capability also provides a communication channel to the user. This is particularly useful when other communication tools are compromised or unavailable. With Device Freeze, a message can be displayed to the user, informing them of the ransomware attack, providing updates on progress, or giving other relevant instructions.

If user interaction can be permitted, the Absolute End User Messaging capability is an alternative that can be used to display a message to an end user without freezing the device. Like Device Freeze, this communications channel is invaluable when other communications tools have been disrupted.

Device Freeze actions and End User Messaging will execute on the target devices within 15 minutes after they are initiated by the incident response team.

*****IMPORTANT*****

Do NOT assume that tools such as email or Slack will be spared and available for communications to users. It is not unusual for servers or for related services to be compromised or impaired during the attack-cycle. Have the message templates and content already defined and approved in advance as part of the Incident Response Plan so time is not lost in creation, review, and approval cycles – especially since stakeholders may not be easy to reach as the attack unfolds.

Reset Impacted User/Host Credentials

At this stage, it may not be clear if data has been exfiltrated or to what extent, and it is possible that exfiltration may be ongoing as part of a multi-stage, multi-faceted campaign. To minimize the risk to the business, it may be necessary to remove existing user and device accounts and create new ones as needed. Absolute Ransomware Response includes Reach scripts that can effectively execute this remediation.

This step can be completed in 15 minutes across the entire fleet of endpoints.

Update Endpoint Protection (EPP) / Endpoint Detection and Response (EDR) Tools and Execute Anti-Virus/Anti-Malware Scan

After the ‘Detection and Analysis’ phase identifies file signatures or other, now-known IoCs, EPP/EDR tools will need to be updated to prevent recurrent infection. However, if the malware attempts to Impair Defenses, successfully deploying updates can become a challenge. Fortunately, through the combination of Absolute Application Resilience and Reach script capabilities, Absolute Ransomware Response can repair or re-install EPP/EDR tools, even when the malware uses defense evasion techniques. Absolute Ransomware Response can also support the deployment of a new EPP/EDR solution, if the organization determines that is required as part of the overall response and recovery.

In scenarios where EPP/EDR tools are disabled or require updates to prevent re-infection, Absolute Ransomware Response will ensure that the EPP/EDR tools are repaired, re-installed, or updated as applicable within 30 minutes. This ensures that a full scan can be completed on affected endpoints to remove the malware variant and prevent further reinfection.

Recovery

*****IMPORTANT*****

Do not restore an image on an infected asset without confirmation from the investigation team. Doing so may destroy valuable forensic data that may be necessary in the investigation of root cause.

Restore Infected Hosts to Known Good State

Restoring affected endpoints to a known good state may require either a complete rebuild of physical hardware or a system restoration from snapshots. This process can be very time-consuming. Depending on the effectiveness of the remediation step, the cyber security incident response team may need to determine if a reimage or a complete change in physical hardware is required.

Absolute Ransomware Response provides Reach scripts that assist with restoring devices. The time it takes to reimage a machine will vary.

Patch Known Vulnerabilities

Where possible, update all known critical and high vulnerabilities (hardware and software) on existing endpoints. This needs to be done whether using existing devices or deploying new devices. **In many cases, the IT tools required for patching known vulnerabilities will have been disabled or impaired by the attacker. In such scenarios, Absolute Ransomware Response will ensure that tools such as Microsoft Endpoint Manager (including Microsoft System Center Configuration Manager and Microsoft Intune) and Tanium are repaired or re-installed within 30 minutes so that vulnerabilities can be patched as soon as possible. Typically, business applications will require testing and verification after several patching cycles may be performed.**

Restoration of Affected Files From Backups

Once the Incident Response team confirms the availability of backups during the 'Analysis' stage, the next step is to connect newly restored hosts to the backup system and initiate the file restoration process. However, it is important to exercise caution. Attempting to initiate too many restores simultaneously may lead to negative performance outcomes, further delaying the recovery time.

It is equally important to identify critical systems and assets that need to be restored and define the order in which those systems need to be restored. **As can be seen from the steps above, Absolute Ransomware Response can assist with restoring devices, to ensure that they are ready to return to service within a few hours.**

Restore Normal Operations

The last step is to restore normal operations. This can only be performed once all the endpoints in the environment have been restored. In order to restore full operations, the incident handler should unfreeze all endpoints, remove them from quarantine, and inform users via Absolute End User Messaging that restoration is complete. **From the time the actions are initiated, they will take up to 15 minutes to complete.**

4. Post-incident Recovery

The importance of learning and improving in incident response is often overlooked. Holding a "lessons learned" meeting after a ransomware incident can help to improve security measures and the incident handling process. This meeting should be held within several days of the incident and should involve all parties. Questions should include what happened, how well staff and management performed, what information was needed sooner, what actions inhibited recovery, and what can be done differently in the future.

The success of such meetings depends on inviting the right people, establishing rules of order, documenting major points of agreement, and creating follow-up reports. These reports provide a reference for handling similar incidents and can be used for training new team members. Updating incident response policies and procedures is also important, as well as reviewing all related documentation and procedures for handling incidents at designated intervals. A formal chronology of events and a monetary estimate of the damage caused should also be created for legal reasons.

Absolute Ransomware Response maintains an audit log that includes when device actions were initiated and when the actions were executed on endpoints. This information can help with creating a chronology.

Execution Timeline

Here is a timeline that shows the different steps and how long each of those steps will take, leveraging either the Absolute Ransomware Response or Absolute Resilience product.

Containment

- Update discovery scripts
- Identify affected hosts (30 mins)
- Isolate affected hosts (15 mins)
- Remove user interaction (15 mins)
- Reset credentials (15 mins)

Remediation

- Obtain updated EPP/EDR installer
- Repair/re-install EPP/EDR tool with Application Resilience (30 mins)

Recovery

- Restore files from backup
- Patch known vulnerabilities
- Restore normal operations (15 mins)

Many of the steps listed above can be done in parallel to reduce the timeline; however, when done sequentially, the overall timeline is longer. Please note that the timeline is derived from testing within the environment defined below and from Absolute's long-established experience with the use and operation of the underlying capabilities at scale and in non-ransomware-response use cases; specific metrics may vary within a customer's own environment.

Test Environment and Assumptions

The test environment used to verify, validate, and measure the time-to-completion for different steps in the Playbook outlined above was a self-contained environment with multiple endpoints enabled with the Absolute Ransomware Response license and enrolled in the Absolute Service. Measurements were taken to determine successful execution of the Playbook and associated time-to-completion.

Since all the underlying capabilities employed by Absolute Ransomware Response (e.g., Application Repair and Reinstall, Device Freeze, End User Messaging, and Reach script deployment) are part of the core Absolute Secure Endpoint solution and are routinely employed at scale for non-ransomware-related endpoint resilience, security, and compliance purposes, Absolute knows they can be executed reliably and within the specified timeframes not only within the ransomware test environment but also at scale in production environments that include hundreds of thousands of endpoints.

ABSOLUTE®

Trusted by nearly 21,000 customers, Absolute Software is the only provider of self-healing, intelligent security solutions. Embedded in more than 600 million devices, Absolute is the only platform offering a permanent digital connection that intelligently and dynamically applies visibility, control and self-healing capabilities to endpoints, applications, and network connections — helping customers to strengthen cyber resilience against the escalating threat of ransomware and malicious attacks.

Request a Demo

Nasdaq | ABST   TSX | ABST