Coro version 1.3 – Release Notes

Advanced Threat Control (ATC) events and control in Coro console

VSS automatic backup and protection

Box cloud service protection

Advanced Threat Control (ATC) events and control

Using behavioral process analysis to mitigate zero-day attacks

As new threats emerge and new malware is spread on a daily basis, it is important to overlay signature-based malware detection with heuristic process behavior analysis in order to overcome a potential gap between the time of new threat detection and the time its signatures are released and propagate.

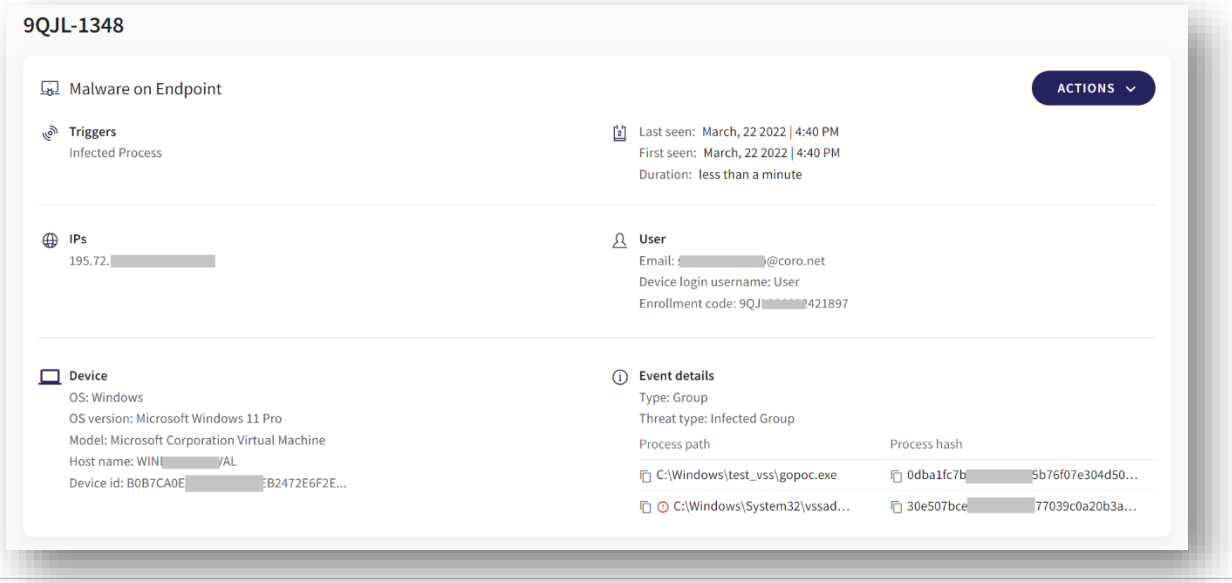
The Coro client analyses running processes and looks for anomalies in their behavior, such as impersonation, code injection and execution, etc.

Although not recommended, you can select to turn off the ATC from your Coro Console (Control Panel/Endpoint Devices/Settings)

Note: This feature is only available for Windows endpoints.

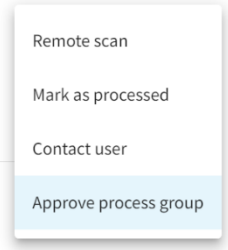
Immediate mitigation

When the behavior of a process running in the OS is assessed as potentially harmful, it is immediately terminated to isolate and remediate the threat and the detection is reported in the Coro Console as “Malware on Endpoint” event with “Infected Process” trigger.



Process approval

After you have examined the suspicious process, possibly consulting the end user, you can use “Approve process group” action to add this process group to the allow list and avoid triggering on this process for your endpoint devices.



VSS automatic backup and protection

Using snapshots to support business continuity in case of a ransomware attack

As a ransomware attack is typically corrupting or encrypting local files, making frequent copies of your files is essential to allow quick recovery and **minimize business impact**.

The Coro client now utilizes the Windows VSS (Volume Shadow Copy Service) mechanism to automatically save a snapshot of your files every 4 hours.

Use the Coro Console’s Control panel (Control Panel/Endpoint Devices/Settings) to enable or disable VSS protection.

Notes:

- This feature is only available for Windows endpoints.
- The number of saved copies depends on the disk size allocated in the Windows’ “System Protection” configuration

Backup copy protection

Attackers understand that snapshots make their attack futile, so they have learned to target the backups and delete or corrupt them.

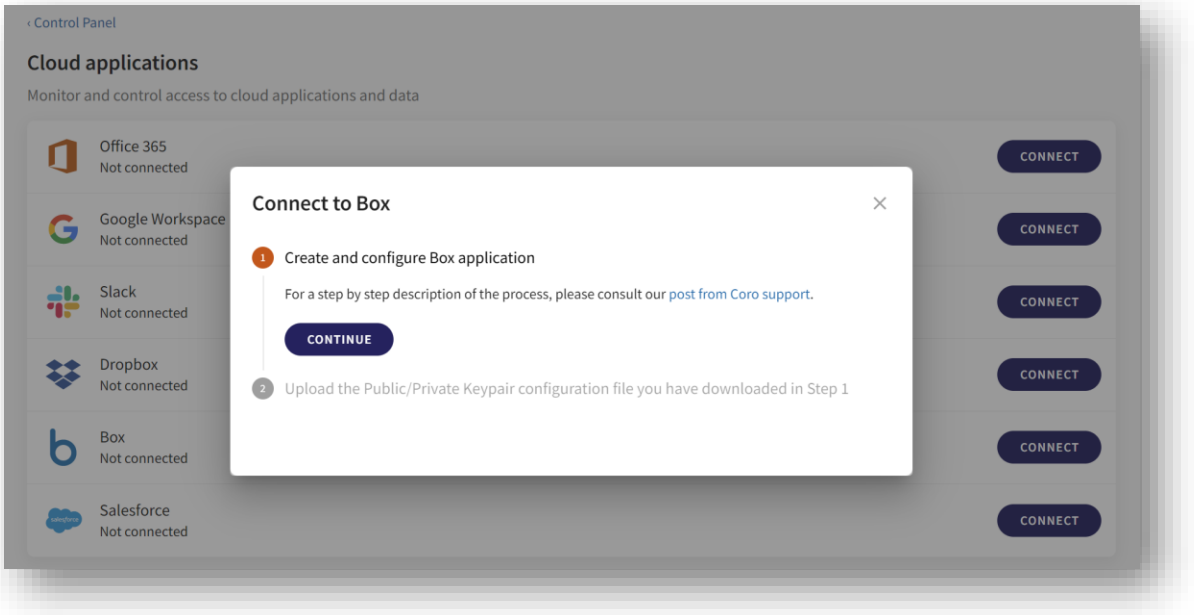
In order to overcome this threat, the Coro client monitors access to the VSS copies and utilizes the ATC mechanism to kill processes trying to tamper the backup.

Note: Backup protection might have a side effect of disrupting the operation of legit applications, in which case these processes need to be added to the allow list by using the “Approve process group” action.

Box cloud service support

You can now use Coro to monitor and protect your organizations' BOX service.

Coro monitors Box for unauthorized access, abnormal user activity, malware and ransomware in the Box file system and sensitive data leakage (DLP).

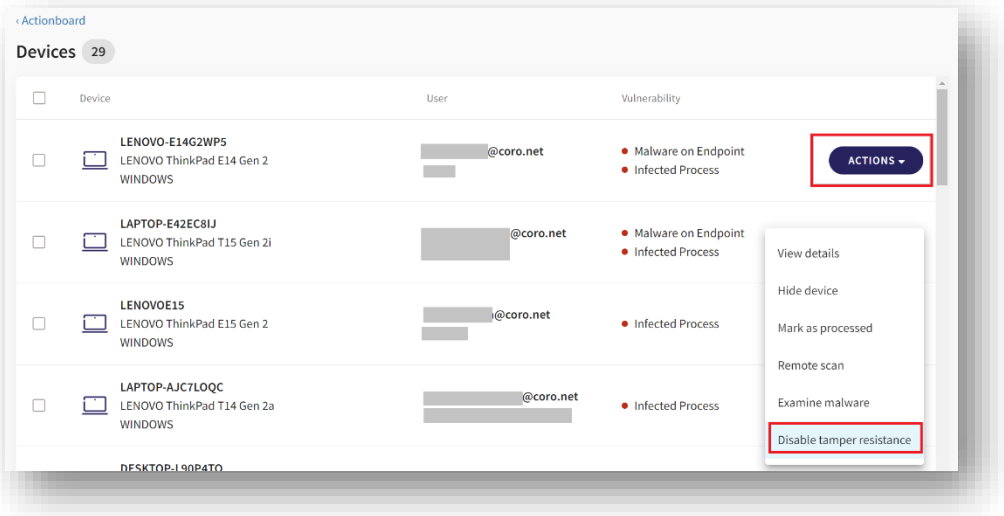


Other Changes

Improved anti-tampering

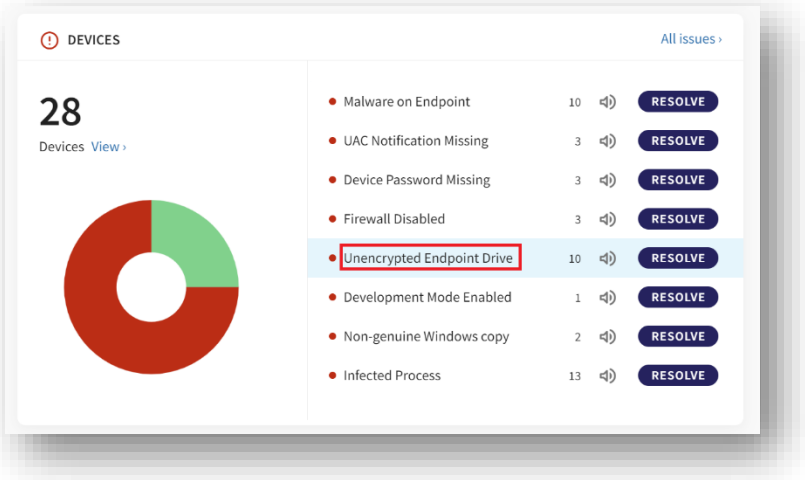
Additional layers of defense were added to prevent malware from killing the Coro agent process or disturbing its operation in any other way.

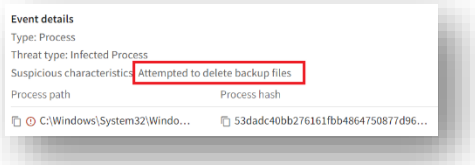
Note that anti-tampering also prevents uninstalling and updating the Coro client, so please use the Coro Console's Control panel (Control Panel/Endpoint Devices/Settings) to enable or disable Tampering Protection to all your Coro clients.
You can also enable/disable anti-tampering for individual devices from the Console's Devices screen.



Drive-level encryption vulnerability

To allow more flexibility in disk encryption policy, we will show missing encryption events at the drive level rather than the device level.

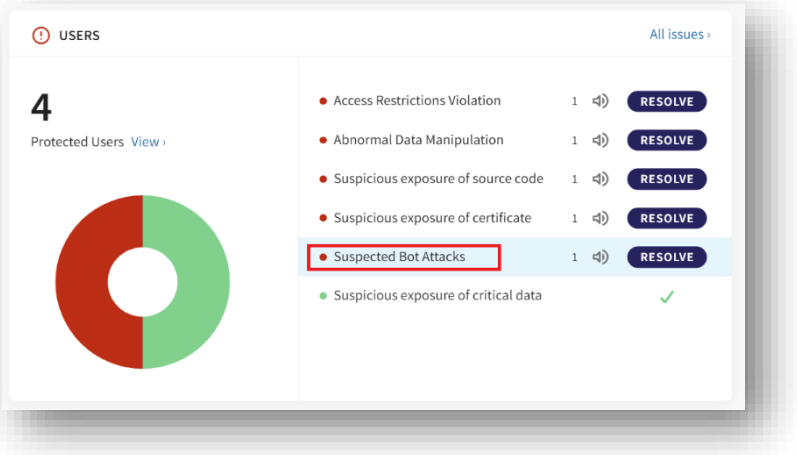




Suspected Bot Attack trigger

A new “Suspected Bot Attack” trigger had been added to the Users section of the action board to indicate customers whose email address might be known to attackers using it for credential theft attempts.

It is advised to make sure use a strong non-trivial password and apply a 2FA protection layer.



Exact keyword phrase search

To reduce potential confusion and clatter, keywords defined in the Data Governance settings (Control Panel/ Data Governance) are now treated as exact match search. Please use REGEX to implement a different match pattern.

Device IP and location for endpoint events

Endpoint events (malware, vulnerabilities) now include an indication of the device public IP and its location to enable better understanding of the threat.