



The ThreatLocker®

## Testing Environment

ThreatLocker's Allowlisting is a powerful solution that simplifies onboarding with our Learning Mode and audit assistance. In dynamic environments, Allowlisting is not a set-and-forget solution. When users request to run new applications after the endpoints have been secured, administrators need to make a decision whether to allow or deny these requests. This requires specific knowledge about the requested application or a heavy research lift to investigate and verify whether an application meets the organization's safety requirements. **Until Now.**

### What is the ThreatLocker® Testing Environment?

ThreatLocker's new Testing Environment uses a Virtual Desktop Infrastructure (VDI) to enable administrators to evaluate an approval request quickly. Without taking the risk of running an unknown/untrusted application in a production environment, the VDI creates a temporary testing environment in which to run the requested application. Businesses can now safely evaluate applications in a cloud-based environment to examine how they behave and decide, based on real-time information, the best course of action for their organization.



## How Does The Testing Environment Work?

Without impacting your production environment, a Virtual Desktop Infrastructure (VDI) test environment is dynamically created to enable the requested application to run. When the application runs, ThreatLocker's Risk Center opens and performs the following evaluations:

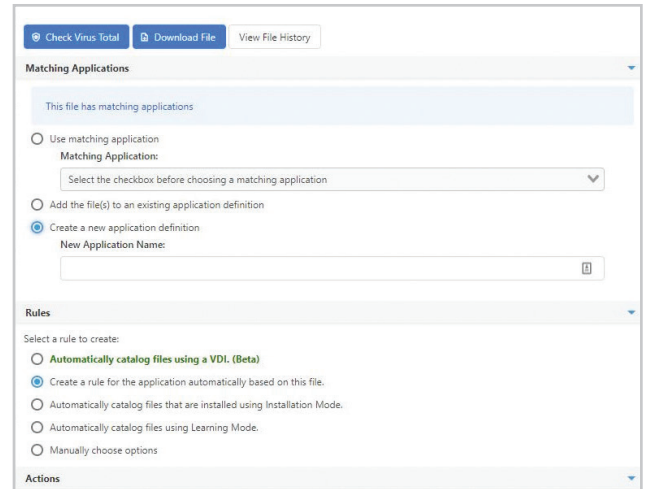
- Checks the application in VirusTotal to see if any AV vendors have flagged it as malicious or suspicious.
- Checks to see if the application attempts to access data storage locations using canary files.
- Checks to see if the application made changes at the System level (e.g., inserting itself into the startup folder).
- Checks to see if the application accesses the internet.
- Checks to see if the application makes changes to the registry.
- Checks the signatures of the application and its dependencies.
- Shows all new files that have been installed.
- Shows an audit of the activity in real-time.

## Real-Time Audit

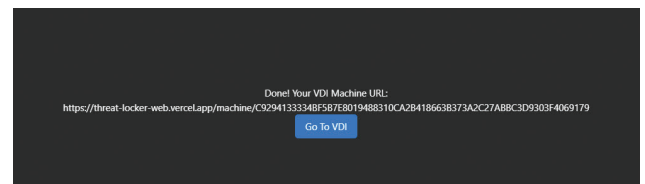
Red alerts on these parameters will give the administrator additional information, and all data is logged in real-time, giving you the critical information needed to understand the risk before allowing a user to install new software

Each of those checkpoints alerts in red for risks, and the tabs provide full details of the impact in a single click. This allows the administrator to quickly and confidently act upon an application install request.

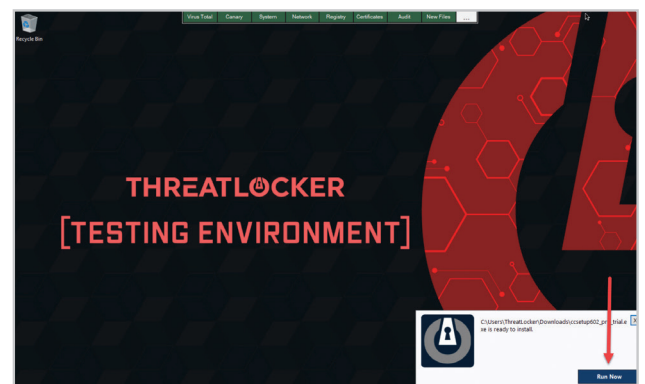
The ThreatLocker® Testing Environment™ is a powerful tool for rapid installation decision-making, keeping you moving at the speed of business.



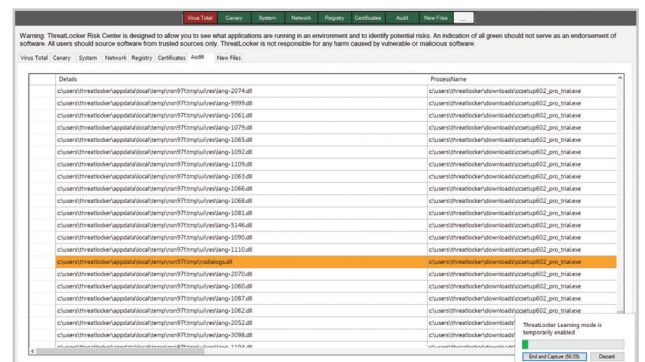
The image above shows the ThreatLocker™ Approval request.



Once you click 'Save', you will receive a URL for the VDI. Click 'Go To VDI' to be taken to the VDI.



Approval will automatically be downloaded onto the VDI. Click 'Run Now' to begin installation.



Details	ProcessName
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-2074.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-9999.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1061.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1079.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1065.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1095.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1109.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1063.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1066.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1068.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1081.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1090.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1110.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1110.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-2070.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1060.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1067.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-1062.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-2052.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe
C:\Users\threatlocker\appdata\local\temp\inst70\mpu\instang-3098.ab	C:\Users\threatlocker\download\os\osup602_pnc_3ml.exe