Progress Flowmon

Protect Your Data on PowerScale

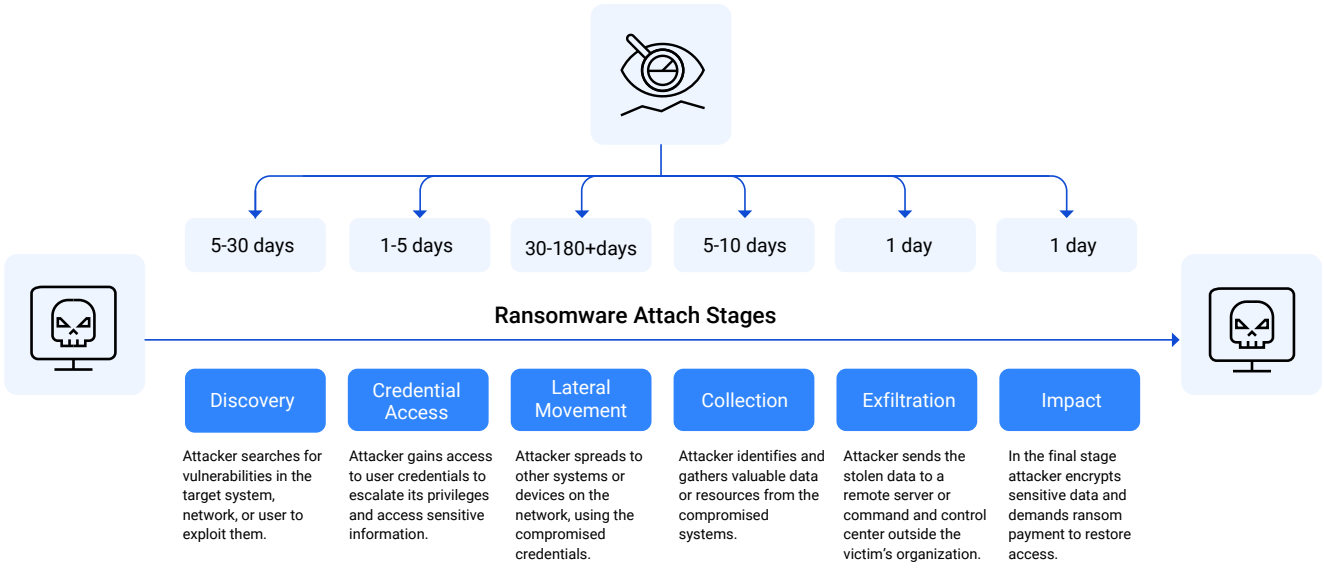
Proactively Detect Ransomware Threats

DATA SHEET

Protecting data is key. In 2022, organizations all around the world detected 493.33 million ransomware attempts. This translates to 15 ransomware attacks every second. This is why it is paramount for Dell Technologies to provide its PowerScale customers the solutions needed to proactively detect, protect and recover from such attacks.

Dell Technologies has a range of tools that will detect a bad actor at the Data layer, by looking at audit information: who does what with files (open, close, delete, rename, ...) when and where on PowerScale. However, this may be too late, as Data has already been exposed to a real Ransomware risk. This approach is:

- Reactive, similar to fire fighting
- Taking place during the „Collection" stage of an attack as per below picture
- Aiming to minimize damage and ensure there is valid copy of the Data for recovery purposes



Detect a ransomware attack at every stage - powered by Progress

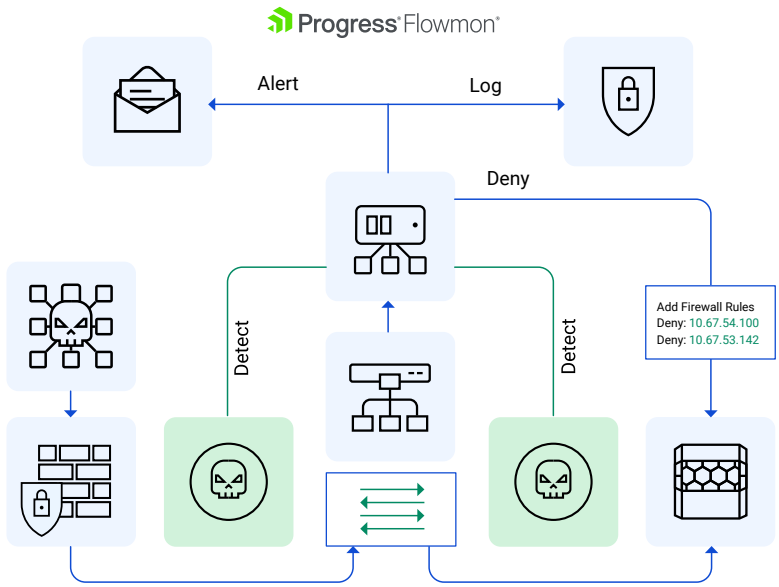
Dell Technologies can now offer its PowerScale customers a much more proactive solution that is able to detect suspicious activity at the „Discovery" stage -- long before bad actors on the Network gain any access to Data.

Dell Technologies has completed an integration for PowerScale and Progress Flowmon, a Network Detection and Response (NDR) solution that:

- Identifes threats before they reach endpoints and critical Data
- Detects threats that bypass the perimeter defenses
- Provides insights into overall network and security posture
- Leverages Machine Learning, AI and multiple other functions to detect network anomalies including Zero-Day attacks

Integrating PowerScale and Flowmon

Flowmon monitors networks that access PowerScale and can directly alert PowerScale to block potentially harmful IP(s) by utilizing firewall rules - once the suspicious activity has been detected.



Flowmon ADS + PowerScale Integration Flow

As an example:

1. Flowmon detects a host conducting network discovery port scans. Port scanning is often used by attackers to map the network environment and identify potential hosts to compromise as well as target victims of subsequent attacks.
2. Flowmon dynamically updates PowerScale's firewall policy with a new firewall deny rule including anomaly event details within the firewall rule description.
3. The bad actor is being blocked at the very start of a Ransomware attack.

For further information please refer to the documentation Flowmon and Dell PowerScale Integration.

The Flowmon integration with PowerScale also ensures Dell customers comply with various Cybersecurity regulations such as NIS2, DORA, HIPAA, PCI-DSS, etc.

If you want to see a demo, please contact your Dell Representative, or reach out to Progress Flowmon:

- EMEA team - dell.emea@progress.com
- APJ team - dell.apj@progress.com
- Americas team - dell.us@progress.com

Try Flowmon Guided Demo

About Progress

Progress (Nasdaq: PRGS) provides software that enables organizations to develop and deploy their mission-critical applications and experiences, as well as effectively manage their data platforms, cloud and IT infrastructure.

As an experienced, trusted provider, we make the lives of technology professionals easier. Over 4 million developers and technologists at hundreds of thousands of enterprises depend on Progress. Learn more at www.progress.com

Worldwide Headquarters

Progress Software Corporation
15 Wayside Rd, Suite 400, Burlington, MA01803, USA
Tel: +1-800-477-6473

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software
progress_sw_

Progress