Progress Flowmon

How to deploy a multi vector cyber defense solution

AT A GLANCE

superna eyeglass

SOLUTION ESSENTIALS

Superna

- ✓ Ransomware Defender
- ✓ Smart Airgap API license

Progress

- ✓ Flowmon Appliance with Anomaly Detection System installed
- ✓ Custom script actions to integrate Smart Airgap API

KEY ORGANIZATIONAL SECURITY CONSIDERATIONS

1. What is the security operational maturity level for monitoring and response to security events?

2. Are there critical application servers that your team has responsibility for protecting?

3. Do you have business critical file or object data that can be subject to compromise?

4. What is an acceptable Recovery Time Objective for your file and object data if and when breaches occur?

As with all organizational data, unstructured file and object storage is the target of threat actors and a growing number of cyber-attacks. The sophistication of today's evolving threats requires enterprise customer defense strategies to mature to protect corporate assets.

Business Challenge

With the volume of cyber-attacks on the increase, enterprise customers need to define a strategy that encompasses multiple detection vectors. A detection vector is a layer of the application stack that can identify and mitigate malicious activity. Examples include end point protection, email gateways, firewalls, network detection & response systems and storage devices.

Today's threats are shrinking the time between initial breach and attack launch. In order to reduce the time to detect, respond and remediate these attempts, a solution that can quickly and intelligently aggregate multiple inputs and automate resolution is required. For threats that sit idle for an extended period prior to the launch of an attack, solutions that can create a picture of disparate anomalies over weeks or months and identify them as a compromise is needed. In either case, the solution implemented must be multi-vector in nature.

The Power of integrating Network and Storage Defense

By integrating network detection with the storage layer defense, organizations can gain an upper hand on mitigating threat actors by providing early warning, detection and remediation of ransomware attempts. Ransomware Defender's combined solution with Flowmon means that business critical business data, is protected and enterprise recovery objective targets can be met and exceeded.

Solution Advantages

- **Early detection** attacks using network monitoring machine learning powered anomaly detection

- **Eliminates** time lag for SOC staff to read and process multi domain threat alarms and **automates** the **response in seconds**

- Combines threat knowledge across network and storage domains to **accelerate** and **automate** responses

- Integrates with Ransomware Defender Enterprise Cyber vault to **block replication of compromised data**

- **Quickly identifies root cause** of the source of the threat at the user, file/object level and network device to enable SecOps teams to scale

- **Reduces the recovery cost** resulting from a Ransomware attack with a protection solution that can **recover data in minutes** not days or weeks with backup only approach or dependence on a cyber vault for recovery.

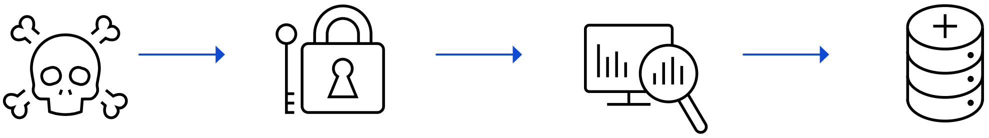
How multi vector cyber defense works?

The solution helps customers protect their critical data by combining intelligent network detection and response capabilities of the Progress Flowmon Anomaly Detection System with Superna's storage layer defense.

By leveraging the full network layer visibility of potential attacks that Flowmon provides, early detection and warnings can be leveraged to trigger data protection workflows in Superna Ransomware Defender.

For most attacks, a threat actor first maps the intended targets with a port scan or attempts a brute force login against application servers. Flowmon is designed to easily detect these early stage indicators and enable the integrated multi vector solution to take pre-emptive protection steps.

An attacker's ultimate goal in ransomware scenarios is to gain access to critical data to hold ransom and do harm to the business. Therefore,a storage centric approach to protecting your ecosystem is critical. Superna Ransomware Defender monitors client behavior at the I/O level to detect malicious activity in real time with a Zero Day detection engine. After a detection of suspicious activity by a potential bad actor, associated files are tracked, the suspect entity is locked out of the storage environment and immutable snapshots are created as a recovery point preventing early stage activities from progressing further through the attack chain.

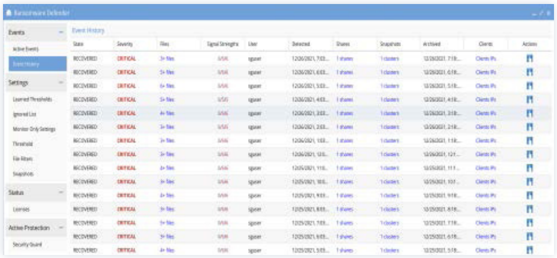


Hacker probes network defenses

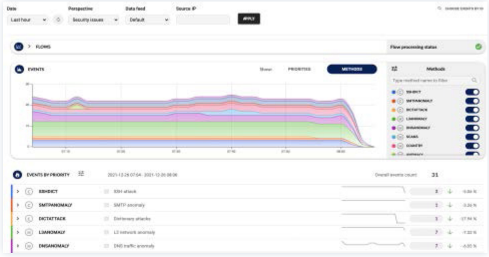
Network Security defenses detect suspicious activity

Smart Airgap API Request to inform storage layer of possible threat

Ransomware Defender applies proactive data snapshot and logs additional data provided by security layer.



Superna Ransomware Defender



Flowmon Anomaly Detection System

About Superna

Superna is a global leader in Managing, Protecting and Securing unstructured data. Superna operates in 5 countries and has over 2600 customers in all verticals that depend on our scalable simple and easy to use products to protect and secure billions of files stored on Scale out NAS.

Learn more about Progress Flowmon

About Progress

Dedicated to propelling business forward in a technology-driven world, Progress (NASDAQ: PRGS) helps businesses drive faster cycles of innovation, fuel momentum and accelerate their path to success. As the trusted provider of the best products to develop, deploy and manage high-impact applications, Progress enables customers to build the applications and experiences they need, deploy where and how they want and manage it all safely and securely. Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals—with confidence. Learn more at www.progress.com

/progresssw
/progresssw
/progresssw
/progress-software
/progress_sw_

Progress®