Real-time Detection: Stay ahead of Ransomware – Jelgava Novads, Latvia

Tomas Cedermark Mikael Lange

Progress Nordics and Baltics

October, 2023

Intros – Progress Nordics

Tomas Cedermark

Enterprise Account Manager

Tomas.Cedermark@progress.com

+46 706 05 90 16

Flowmon

Nordics and Baltics

Mikael Lange

Enterprise Account Manager

Mikael.Lange@progress.com

+46 708 80 41 21

ECS Connection Manager

Nordics, Poland and Baltics

Progress

Who in the room knows What Progress does???

Progress AX Solutions help your IT organization to ensure that networks and applications are stable, compliant, highly available, optimized and performing above expectations. The AX portfolio delivers insights into the state of your applications and environment and the tools you need to proactively solve emerging issues.

Progress is the only vendor combining application delivery and the deepest network, infrastructure and security operations capabilities on the market:

Application Delivery

Improve availability and efficiency through advanced load balancing

- High-performance application delivery
- User authentication and threat protection

IT Infrastructure Monitoring

Monitor devices, servers, virtual machines, and more in cloud, hybrid cloud or on-premise

- Network discovery & mapping
- Resource utilization metrics

Application Performance Monitoring

Track the health and performance of applications to speed troubleshooting

- Insights on usage, capacity, error rate and SLA compliance
- Workflow automation

Network Traffic Visibility

Understand performance from a network perspective and pinpoint the source of an issue

- Comprehensive network performance monitoring
- Intelligent network traffic capture

Traffic Anomaly Detection

Apply behavior analysis algorithms to protect the network

- Early insights to malicious behavior and threats
- Automated response to security incidents

Progress

Welcome to Jelgava Novads

Total number of people 35,000

- Schools 22
- Libraries 29
- Municipal police of Jelgava region
- Jelgava County Property Administration
- Sports center of Jelgava region
- Social Department

Jelgava Novads IT – Central staff

- IT staff is 10 employees

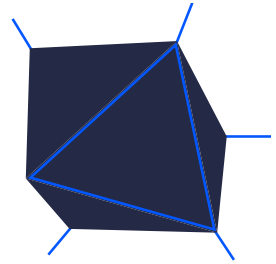
Latvia University of Life Sciences and Technologies

Jelgava Novads needed a solution for

- Identify network-related issues
  - Determine and indicate root cause analysis
- Needed reports that in detail described the reasons related to network problems
  - With demonstrable evidence to the management of the municipality of Jelgava.
- Improve overall network performance
- The institution has a distributed networks architecture, also historically with distributed networks
  - when the regions are coming together – goal is to get a centralized management and network visibility in one central location
- Mandatory to reducing costs to use already existing network peripheral devices such as MikroTik, Fortinet, to send data flows to one central location for analysis and monitoring
- Improve and to get the full visibility from the view of cybersecurity

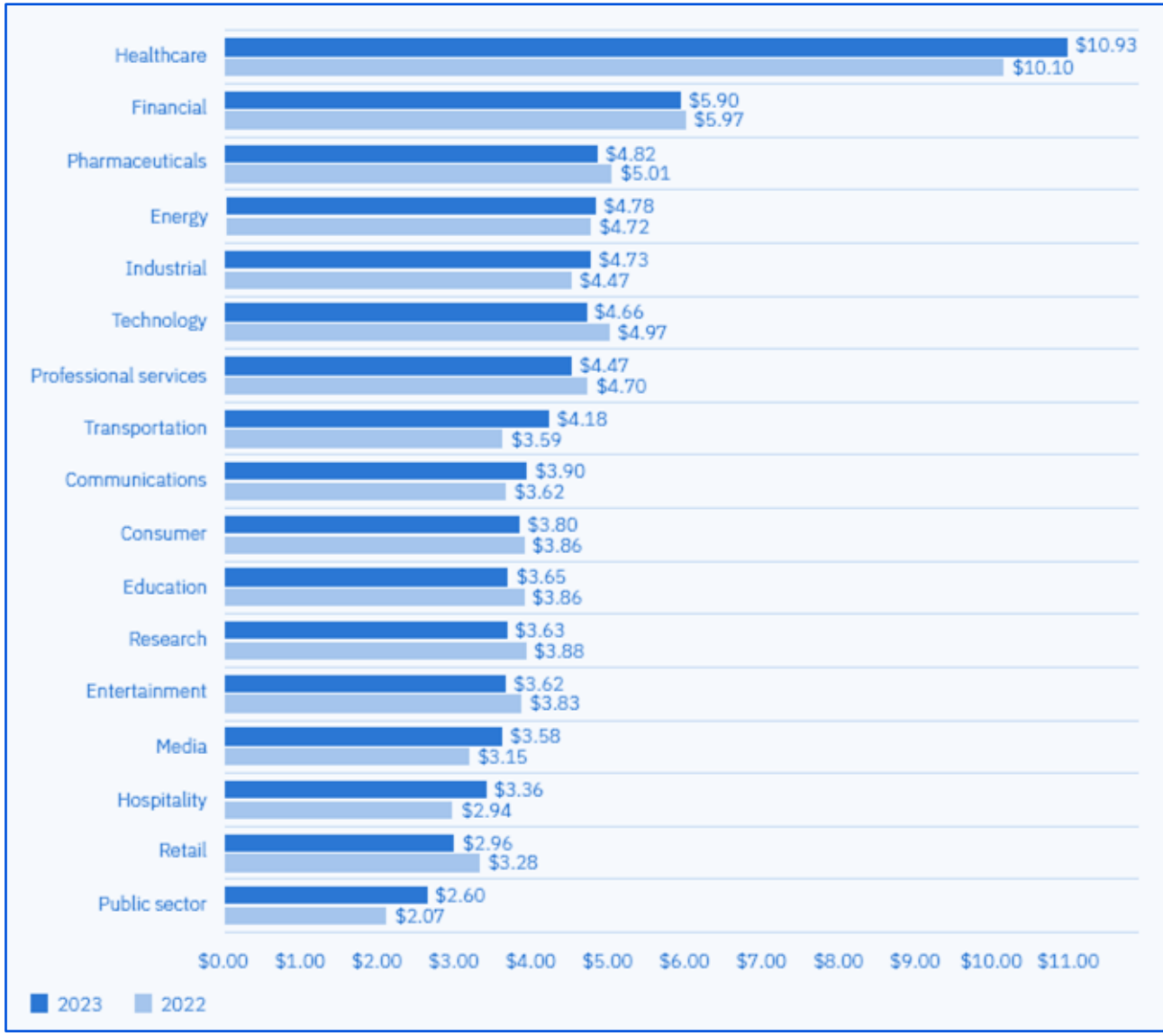

CYBER
is the new
DISASTER
DELL Technologies
PARTNER PROGRAM
DELL Technologies
PARTNER PROGRAM
DELL Technologies

Cost of a Data Breach Report 2023



83%	of organizations studied have had more than one data breach.
19%	of breaches occurred because of a compromise at a business partner.
277	Average time to identify and contain a data breach.
60%	of organizations' breaches led to increases in prices passed on to customers.
12 years	consecutive years the healthcare industry had the highest average cost of a breach.

Cost of a data breach



Progress®

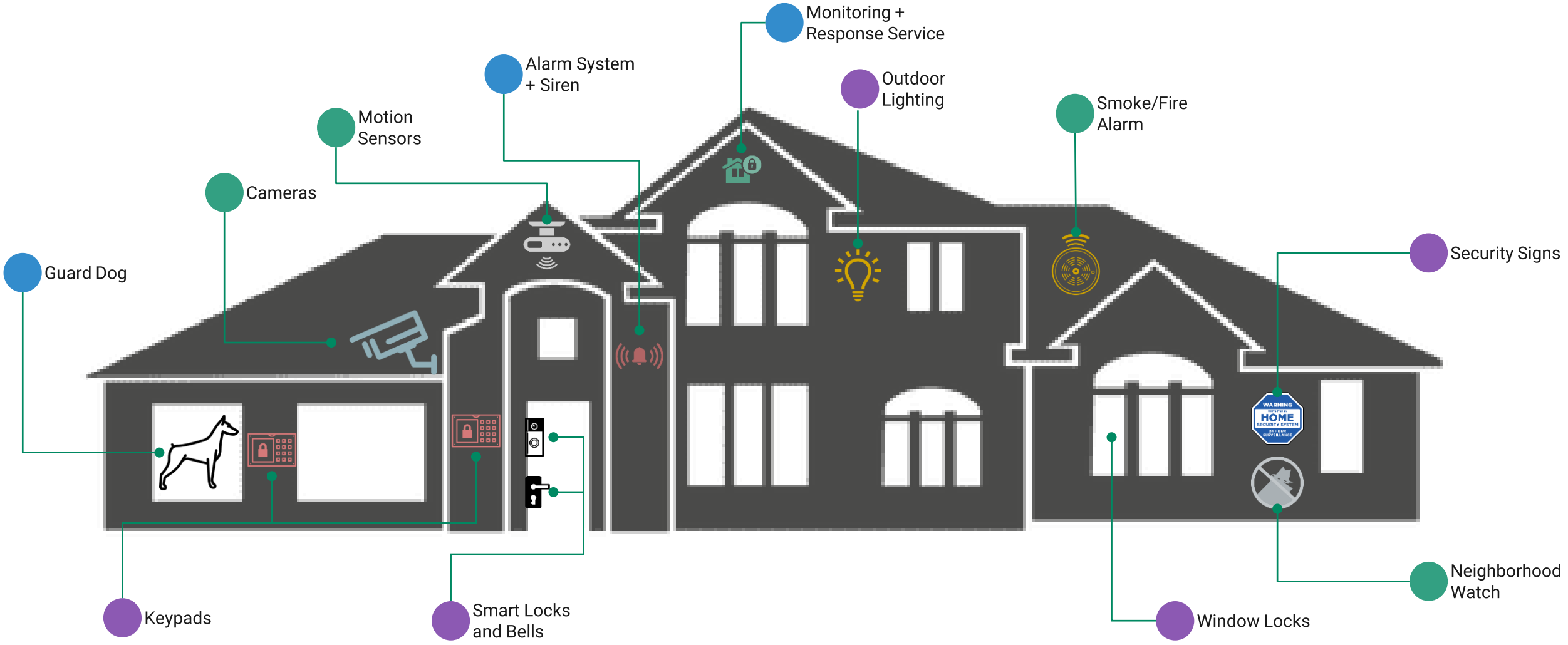
Flowmon is an early RansomWare and Breach detection solution.

Multi-Dimension Security Model

Deter threats and unauthorized access

Detect suspect behavior and access

Automatically respond and alert



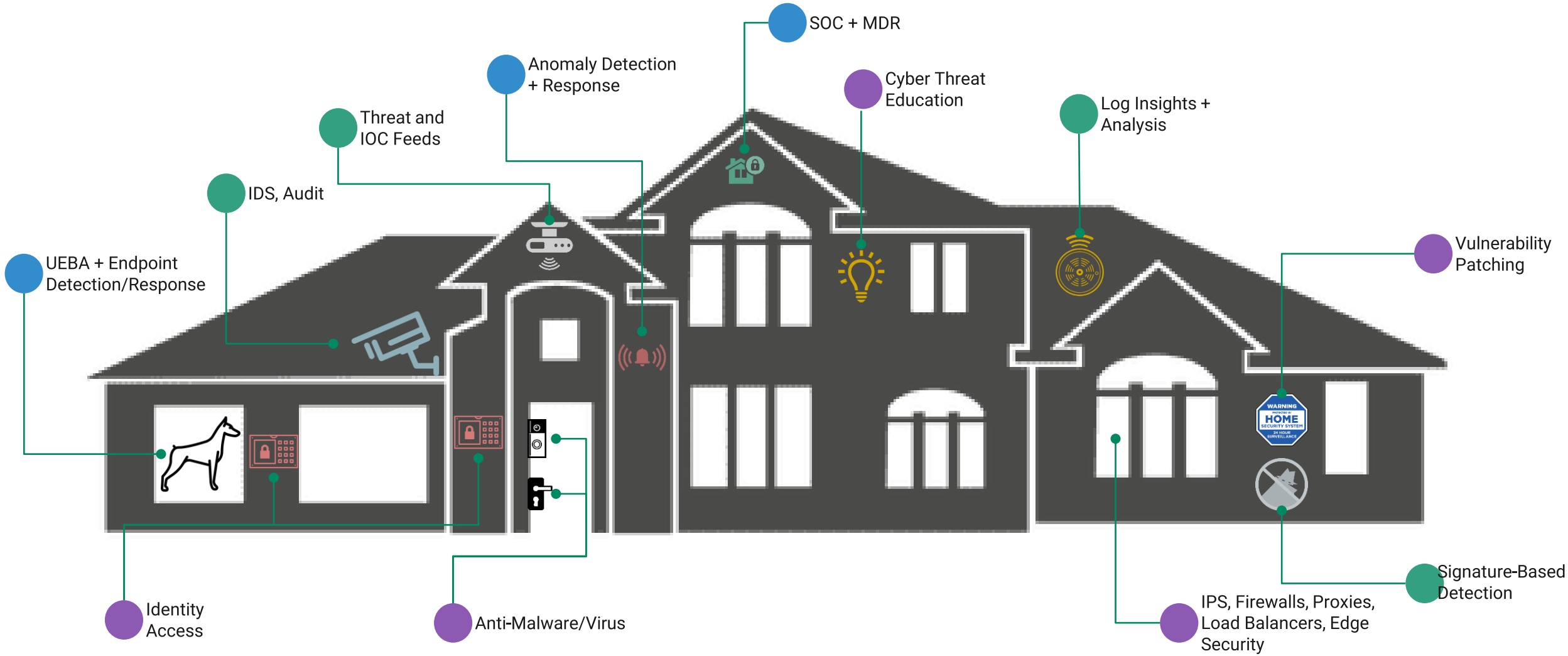
Progress

Multi-Dimension Security Model

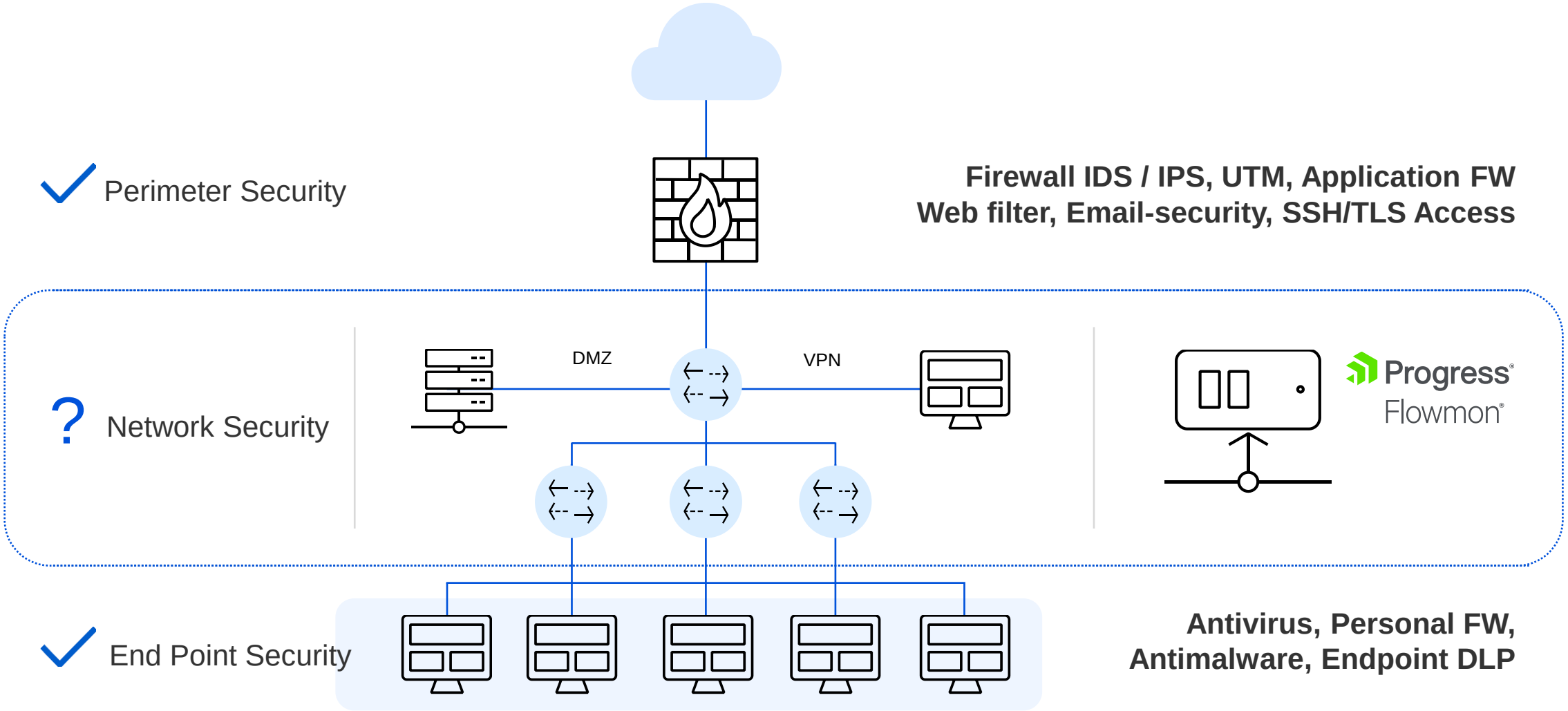
Deter threats and unauthorized access

Detect suspect behavior and access

Automatically respond and alert



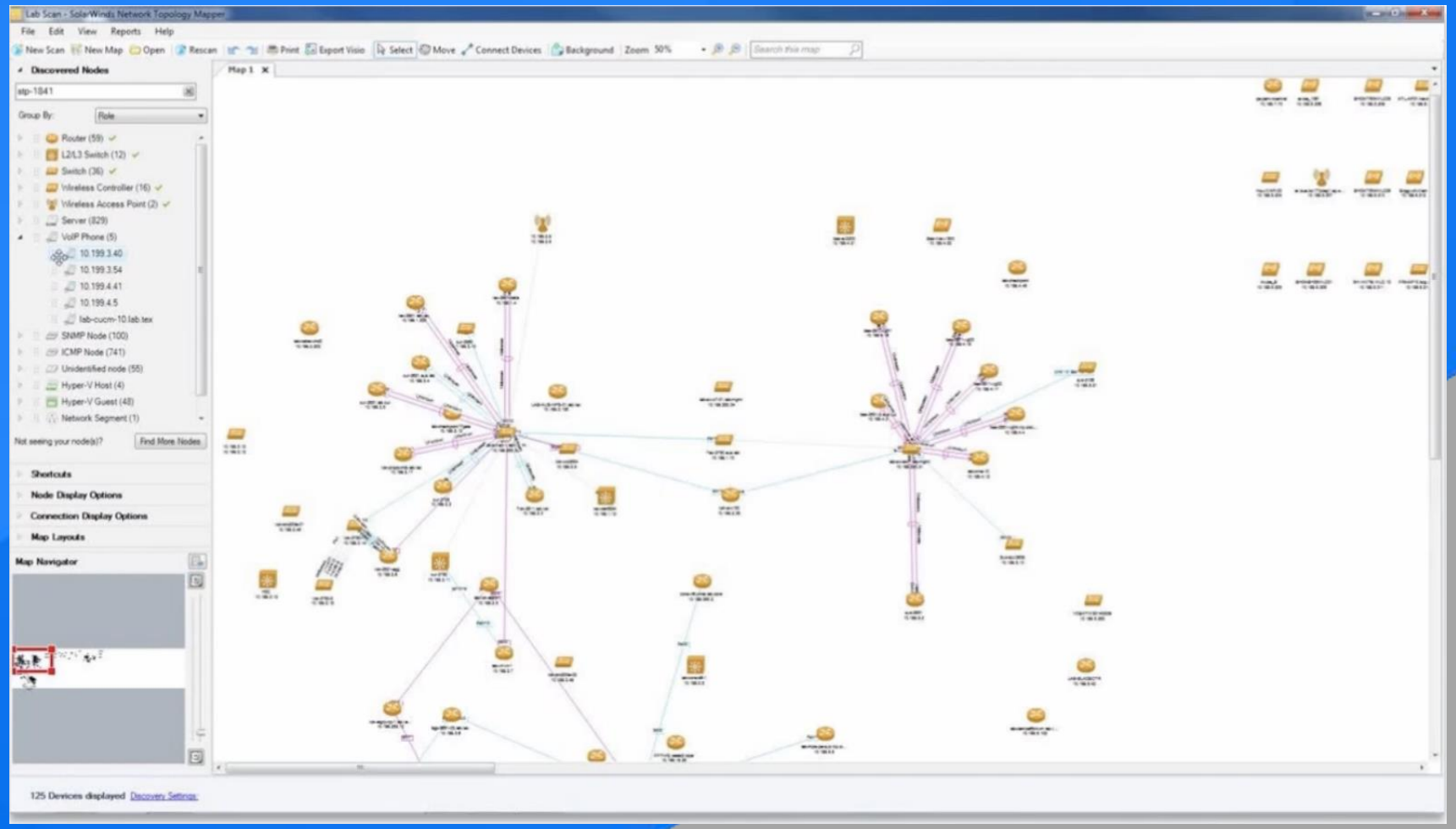
Flowmon Secures the Network



Ransomware Attack Step By Step Example

Progress Flowmon

- Discovery
- Credential Access
- Lateral Movement
- Collection
- Exfiltration
- Impact



Progress Flowmon

- Discovery
- Credential Access
- Lateral Movement
- Collection
- Exfiltration
- Impact

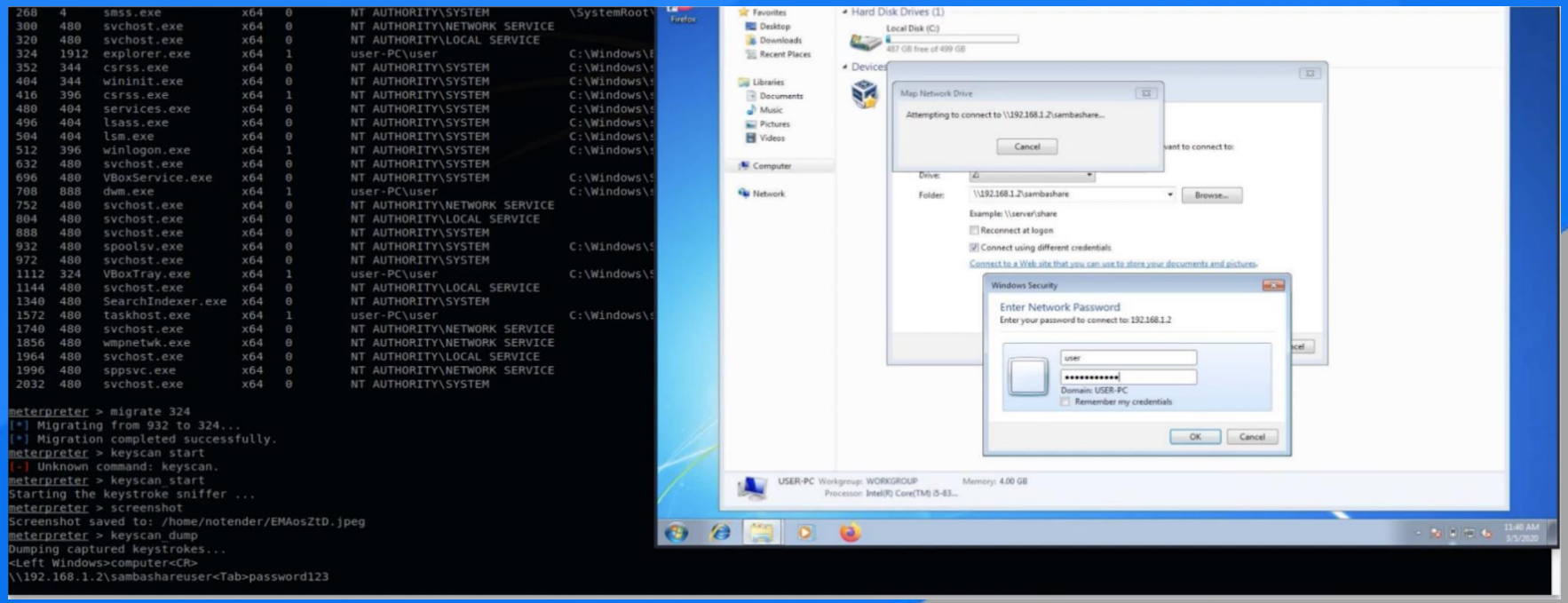
```
[-] ERROR: Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
[-] [redacted]\admin01:ik290skjs92 - LOGON FAILED
[-] ERROR: Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
[-] [redacted]\user01:ik290skjs92 - LOGON FAILED
[-] ERROR: Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
[-] [redacted]\user02:ik290skjs92 - LOGON FAILED
[+] Sleeping 2 seconds.
[+] [redacted]\admin01:[redacted] - LOGON SUCCESS
[+] [redacted]\admin01:[redacted] - ADMIN$ access SUCCESS!
[+] [redacted]\user01:[redacted] - LOGON SUCCESS
[+] [redacted]\user01:[redacted] - ADMIN$ access SUCCESS!
[+] [redacted]\user02:[redacted] - LOGON SUCCESS
```

Progress Flowmon

- Discovery
- Credential Access
- **Lateral Movement**
- Collection
- Exfiltration
- Impact

Progress Flowmon

- Discovery
- Credential Access
- Lateral Movement
- Collection
- Exfiltration
- Impact



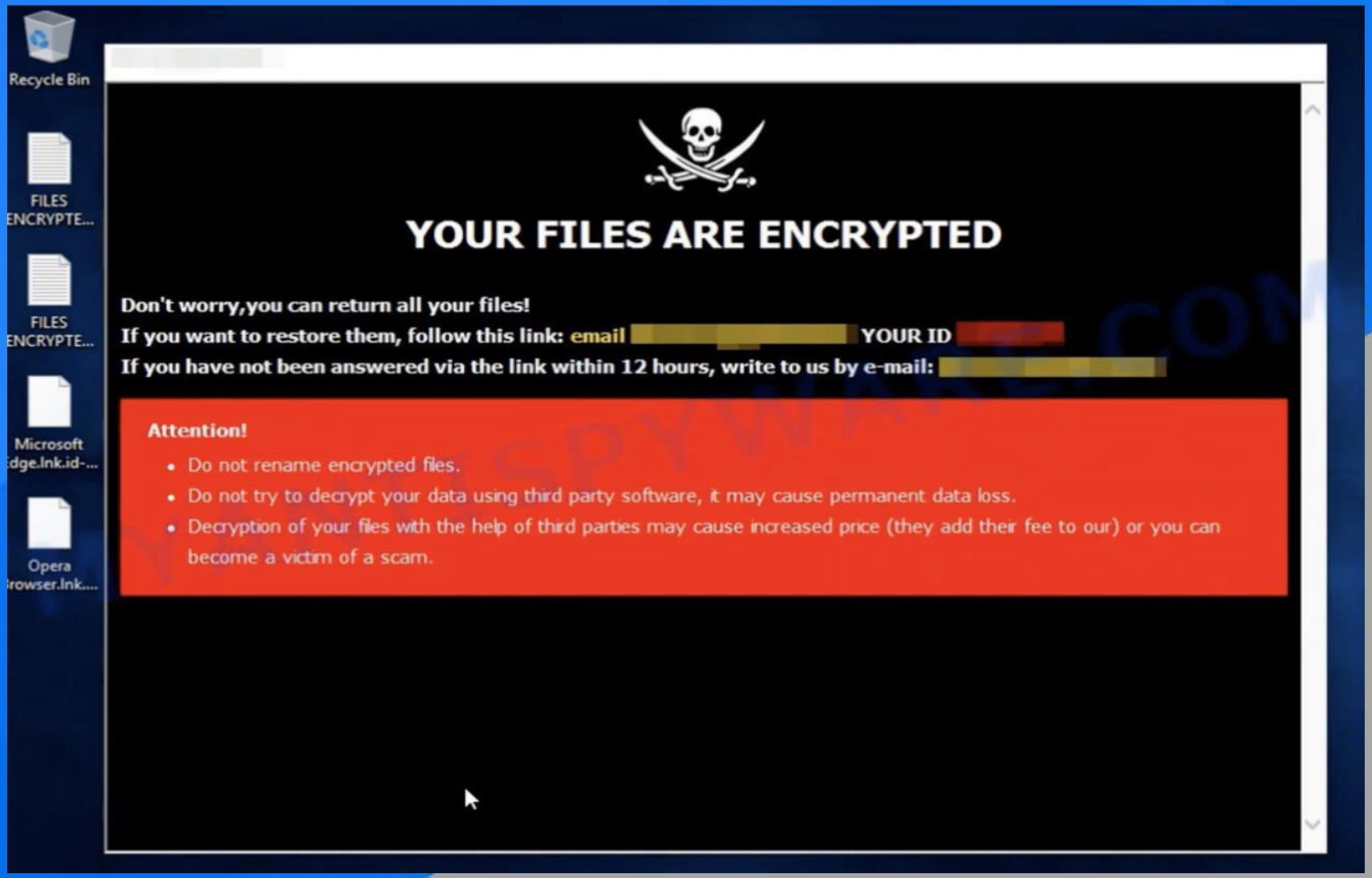
Progress Flowmon

- Discovery
- Credential Access
- Lateral Movement
- Collection
- Exfiltration
- Impact

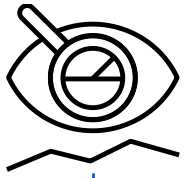
```
root@Chocolate-Crispy:~/DET# python det.py -c ./config.json -p icmp -L
[2016-03-08.16:07:27] CTRL+C to kill DET
[2016-03-08.16:07:27] [icmp] Listening for ICMP packets..
[2016-03-08.16:07:28] [icmp] Received ICMP packet from: 10.0.1.10 to 192.168.0.1
[2016-03-08.16:07:32] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:32] Received 67 bytes
[2016-03-08.16:07:32] Register packet for file /etc/passwd with checksum a7b8bda
05119f81ea199100df01bbfcb
[2016-03-08.16:07:35] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:35] Received 840 bytes
[2016-03-08.16:07:36] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:36] Received 994 bytes
[2016-03-08.16:07:37] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:37] Received 872 bytes
[2016-03-08.16:07:40] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:40] Received 820 bytes
[2016-03-08.16:07:43] [icmp] Received ICMP packet from: 10.0.1.10 to 10.0.1.10
[2016-03-08.16:07:43] Received 914 bytes
```

Progress Flowmon

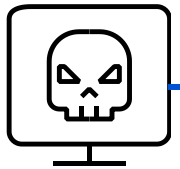
- Discovery
- Credential Access
- Lateral Movement
- Collection
- Exfiltration
- Impact



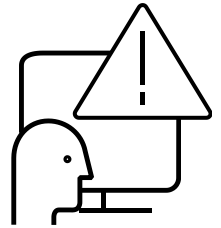
Progress® Flowmon®



5-30 days	1-5 days	30-180+ days	5-10 days	1 day	1 day

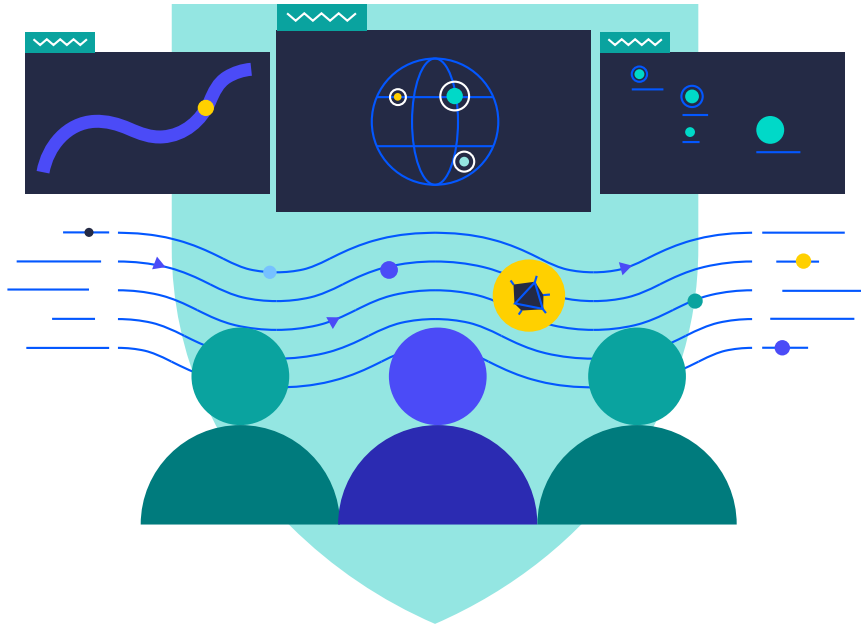


Ransomware Attack Stages



Discovery	Credential Access	Lateral Movement	Collection	Exfiltration	Impact
Attacker searches for vulnerabilities in the target system, network, or user to exploit them	Attacker gains access to user credentials to escalate its privileges and access sensitive information.	Attacker spreads to other systems or devices on the network, using the compromised credentials.	Attacker identifies and gathers valuable data or resources from the compromised systems.	Attacker sends the stolen data to a remote server or command and control center outside the victim's organization.	In the final stage attacker encrypts sensitive data and demands ransom payment to restore access.

Jelgava Novads NDR solution - Network Detection and Response



Internal Security

Viruses, Malware
Ransomware, Botnets
Crypto-mining
Insider Threat

Unwanted Apps

P2P networks, Instant Messaging
Anonymization services
Outdated security policies

Anomalies in Behavior

Profile of a device
Change in long-term behavior

Operational Problems

Delays
excessive load
unresponsive services
broken updates

Attacks

Port scanning
Dictionary attacks
DoS & DDoS
Telnet

Traffic Anomalies

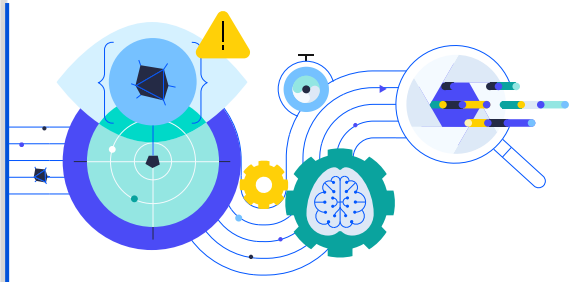
DNS, DHCP, ICMP
Multicast
TLS/SSL

What Flowmon can do outside NDR

Delivering the best Application Experience (AX) in three ways:

Network Performance Monitoring & Diagnostics (NPMD)

Intelligent network traffic capture, comprehensive network performance monitoring and automated root-cause analysis



Network Detection and Response (NDR)

AI-driven behavior analysis and anomaly detection to preemptively mitigate the most subtle exploits before they have a negative impact

Application Performance Monitoring (APM)

Insights on app and database performance combined with workflow automation for addressing sub-optimal AX

Flowmon Helps to Comply with NIS2 Regulation

Threat Detection

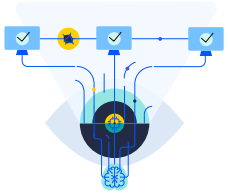
Threat Hunting

NIS 2 requires organizations to have an "early warning mechanism" to detect and respond to cyber threats.

Hybrid Cloud Monitoring

Encrypted Traffic Analysis

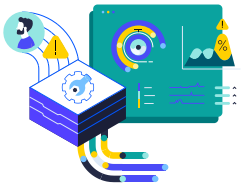
NIS 2 requires organizations to have "comprehensive monitoring" of their hybrid networks to analyze services availability and functionality.



Digital Forensics

Incident Response

NIS 2 requires organizations to have incident handling and management on place to minimize the impact of cyber security incidents.



Root Cause Analysis

Performance Monitoring

NIS 2 requires regulated entities to collect and analyze data when cyber incident occur.

Progress®

Summary

Next Steps

1

If - so far this sounds of interest

Tech Session

2

If after the Tech Session, you are still interested

PoC

3

If you are happy after verifying a good fit for the product

Check please!

Key Takeaways

Visibility is Key!

- Just because you can’t see it – doesn’t mean it doesn’t exist!
- It’s all about protecting YOUR data
- Cyber IS the new DISASTER

Management and Reporting

- Correlation of Reporting and Events
- Multi-Role Management Capabilities
- Identify, Analyse & Diagnose
- Policy Verification and Enforcement

Top Business Benefits

- Enhanced CyberSecurity Posture
- Root Cause Analysis
- Centralized Dashboard
- Reduction in Impact of Data Breaches


Progress®