Beyond Firefighting:

Revolutionizing Endpoint Security with Integrated Risk Management

Andrew Morrisett
Qualys Product Management

Larry Lawrence
Director of Information Technology

What Are We Seeing

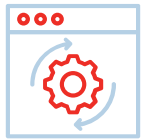
180% increase
in breaches initiated through vulnerability exploitation compared to the previous year

73 Days to contain breach

55 days to **patch 50%** of known to be exploited vulnerabilities after patches become available

Repeat Infections are the norm

Why 55-day Patching average?



Why repeat infections?

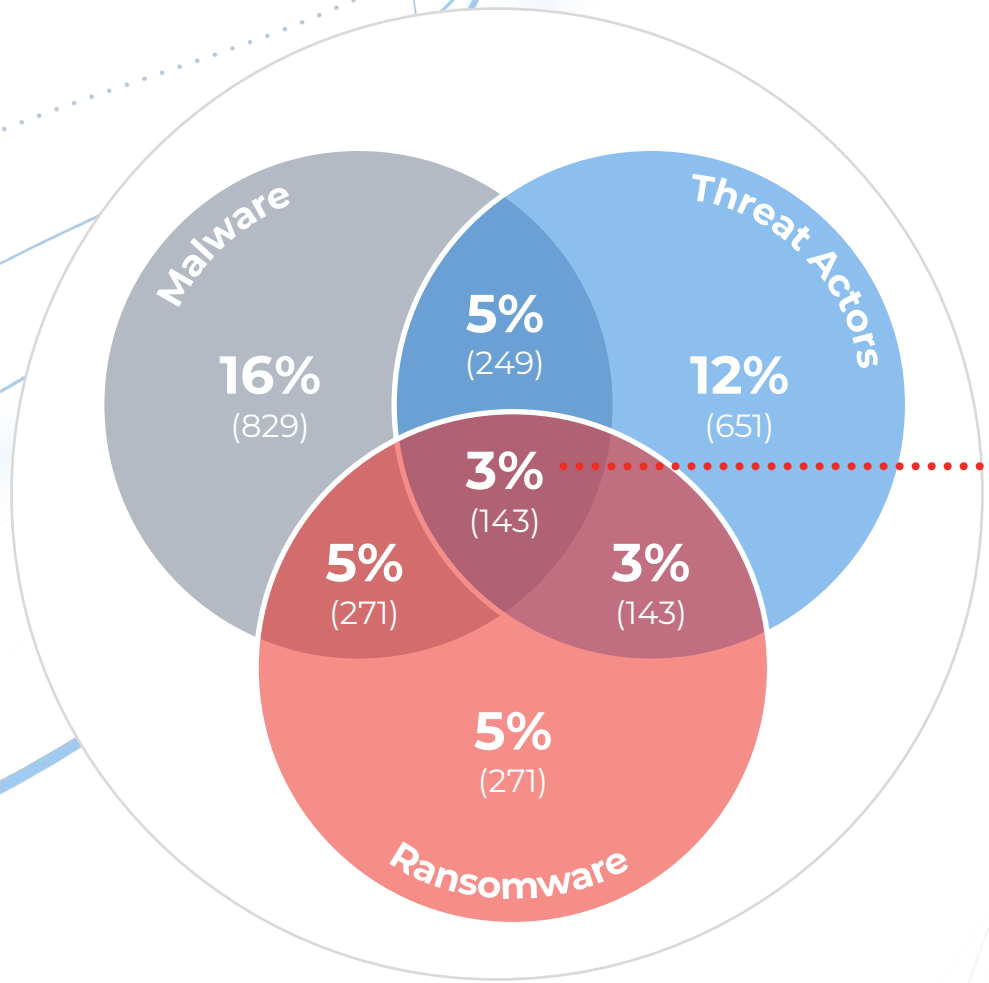
Where is the vulnerability intelligence for SOC Teams?

What about zero-day CVE's and malware?

Know Thy Enemy

Group Name	Cloud	Ransomware	Exploits CVEs
Candiru			✓
Luckycat		✓	✓
Operation Dragon Castling			✓
Ajax Security Team			✓
Sandworm Team		✓	✓
Wizard Spider		✓	✓
APT28	✓		✓
APT38		✓	✓
Dragonfly			✓
Fin7		✓	✓
FoxKitten	✓	✓	✓
Lazarus Group			✓
menuPass			✓
Threat Group 3390	✓	✓	✓
Tonto Team			✓

How Do You Measure Risk During an Attack?



Lack of vulnerability intelligence leads to exploitation, reinfection, expanded compromise.

Misconfigurations Leading to Ransomware

Falling Controls

Top Cloud Techniques

T1210:
Exploitation of Remote Services

T1485:
Data Destruction

T1530:
Data from Cloud Storage Object

Falling Controls

Top on Premise Techniques

T1110:
Brute Force

T1021.001:
Remote Desktop Protocol

T1548:
Abuse Elevation Control Mechanism

Impact of Unknown Assets

Not known to your SOC, but known to attackers

Case Study – Ransomhub

Initial Access

- Phishing Emails: Mass and spear-phishing campaigns
- Brute Force Attacks – password spraying
- CVE-2023-3519: Citrix ADC Remote Code Execution
- CVE-2023-27997: Fortinet FortiOS Buffer Overflow
- CVE-2023-46604: Apache ActiveMQ Remote Code Execution
- CVE-2023-22515: Atlassian Confluence Admin Account Creation
- CVE-2023-46747: F5 BIG-IP Authentication Bypass
- CVE-2023-48788: Fortinet FortiClientEMS SQL Injection
- CVE-2017-0144: Windows SMBv1 Remote Code Execution

Proof-of-concept exploits are obtained from sources like ExploitDB and GitHub

Privilege Escalation

- Mimikatz: Used for credential dumping and privilege escalation
- CVE-2020-1472: Netlogon Privilege Escalation
- CVE-2020-0787: Related to Zerologon

Persistence

- Account Creation
- Installing remote access software

Lateral Movement

- Remote Desktop Protocol (RDP): For moving within the network
- PsExec: Remote execution of commands
- Cobalt Strike: Post-exploitation tool

Defense Evasion

- Renaming Executables: To appear legitimate
- Clearing Logs: To avoid detection
- Disabling Security Tools: Using Windows Management Instrumentation (WMI)

Data Exfiltration

- PuTTY
- WinSCP
- Rclone
- Cloud Services: Misconfigured AWS S3 buckets

Encryption

- Curve 25519 Elliptic Curve: Used for file encryption

Endpoint Security With Qualys

Qualys®

Ransomhub vs Qualys

The threat actors target unpatched external facing system for initial compromise

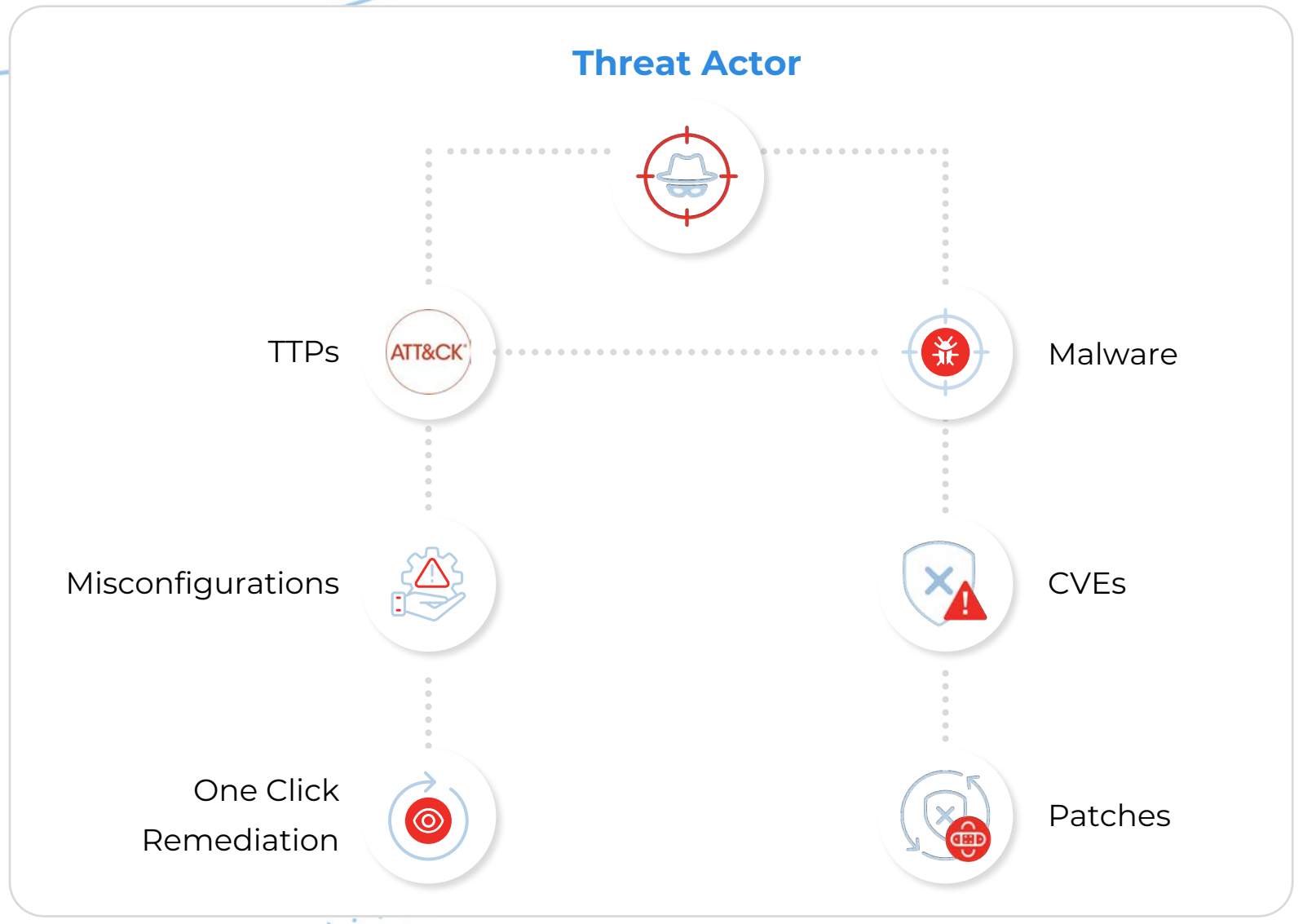
Brute Forced SSH on Linux servers but were blocked

100% of malware used were zero days blocked by our ML model

Qualys provided one click patching to reduce risk of both spread and continued attack

Persistence methods were identified and tagged as suspicious, then removed

Qualys Incident Response

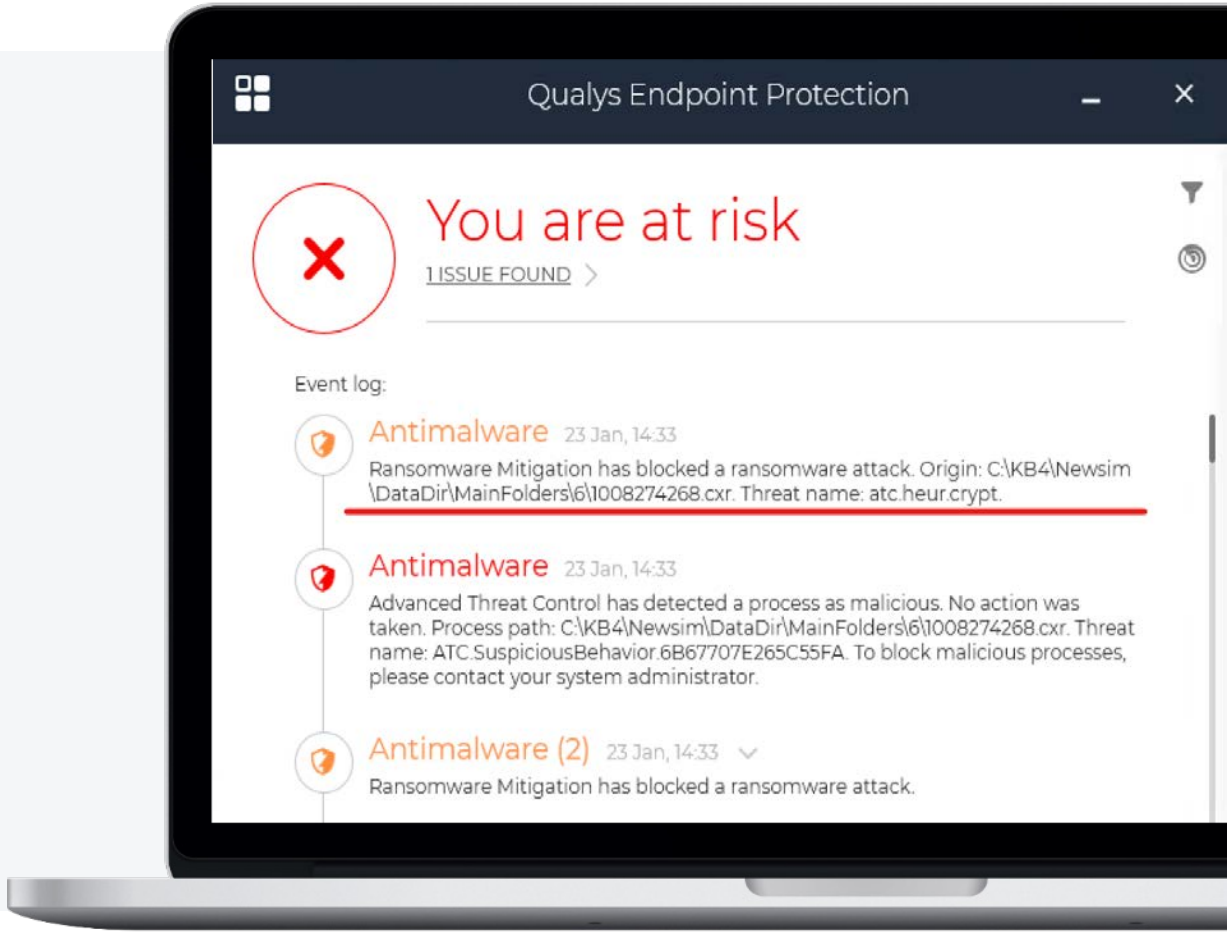


Need for Machine Learning Prevention

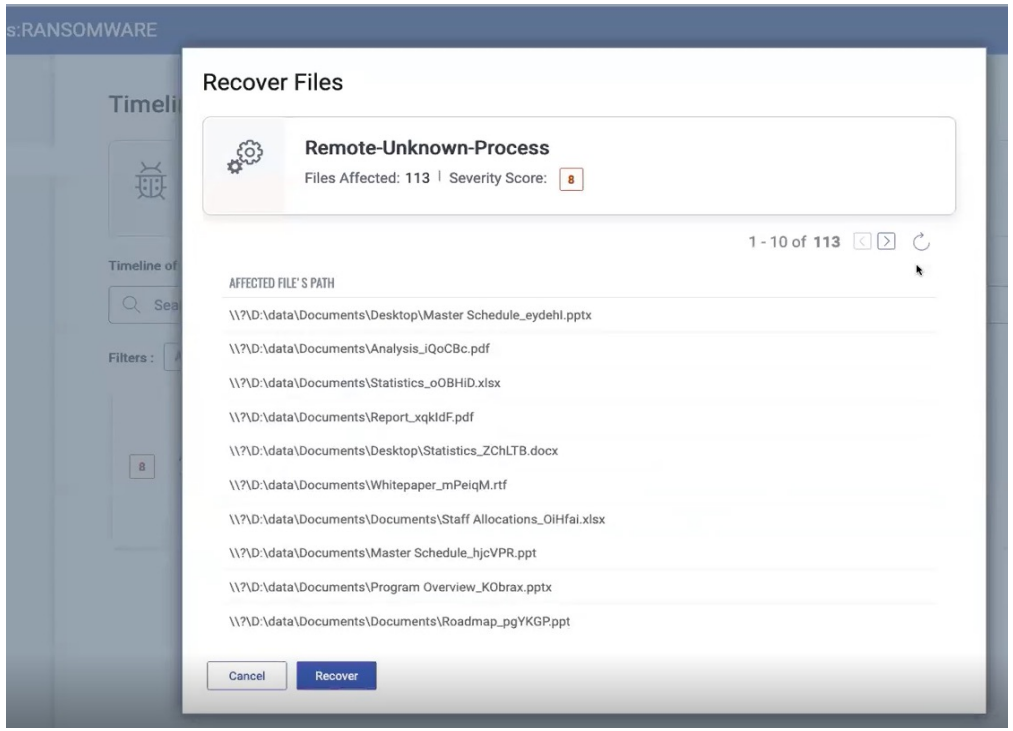
Threat actors rarely use malware that is detected by Anti-virus signatures anymore

Every new attack has custom binaries, hash always changing

ML based Prevention is a must, cannot be marketing fluff



Detect, Block and Recover With Same Agent



Qualys Endpoint Detection & Response will automatically block known and unknown ransomware attacks with multiple layers of technologies.

Ransomware Prevention detects and blocks ransomware attacks by monitoring encryption entropy.

This mitigation works against previously unseen ransomware variants.

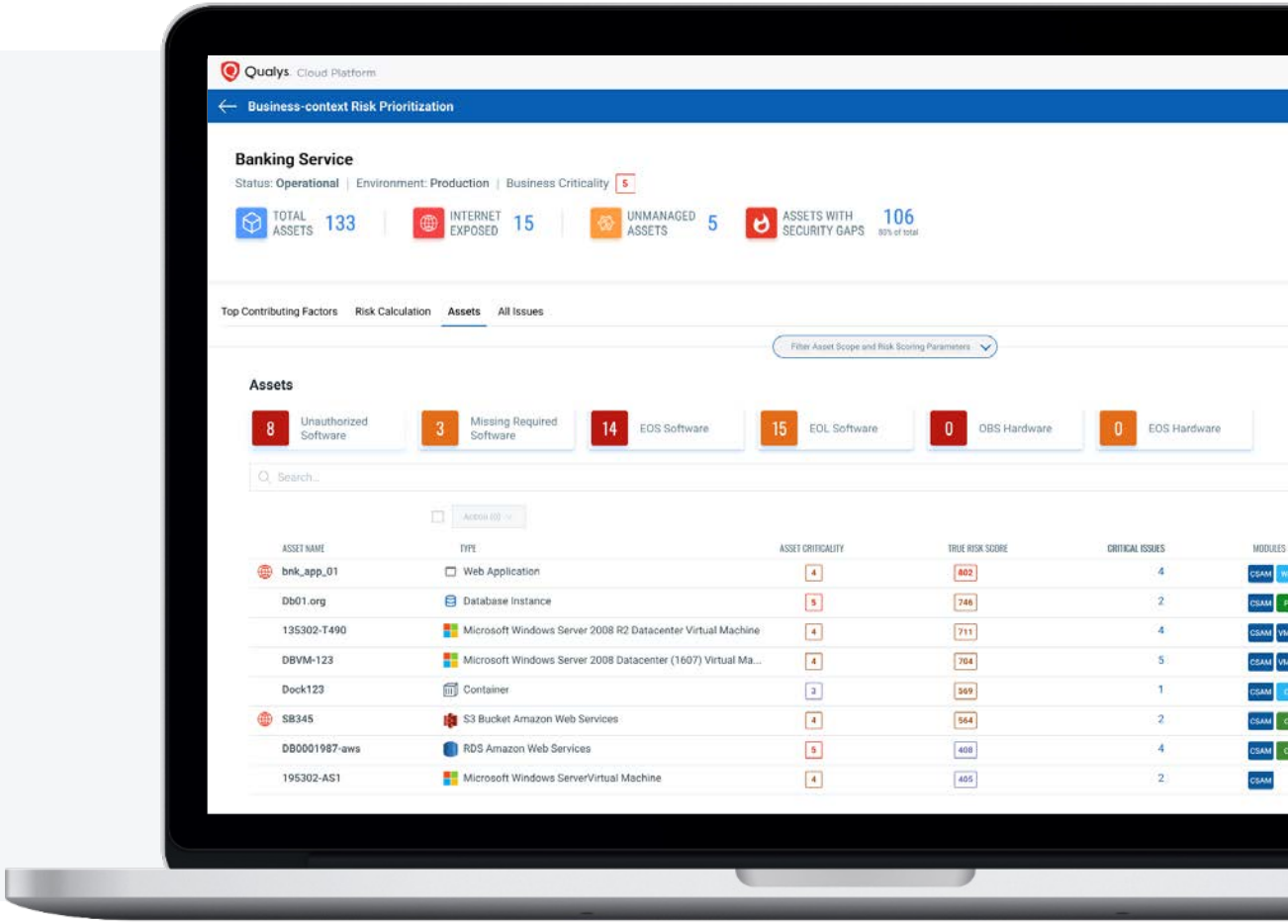
- **Automatically block** the latest ransomware tactics, techniques, IOC's, encryption methods, including phishing attacks.
- **Real time Anomalous Behavior Detection & intervention** when a request is made to encrypt a file (an increase of randomness over a certain limit), a temporary backup is created in memory and the original file is restored after the file changes are done.
- **Multi-layered Response** to remediate incidents and close-loop patching to eliminate the root-case.
- **File Recovery** can recover encrypted files, either automatically or on-demand.

Proactive Endpoint Security

01 Validate what assets are exposed externally to attacker's view

02 Automatically find things like missing agents, security tools, unsanctioned ports, expired SSL certs

03 Ensure no assets are missing required software or endpoint security



Demo

Qualys®

Larry Lawrence

Director of
Information Technology

Evansville, Indiana

9+ Years at MPF

Worked with Qualys
since 2019

A Summary

MIDWESTERN PET FOODS, INC.

Midwestern Pet Foods is **a fourth-generation family-owned** business that manufactures high-quality pet food and treats.

Founded in 1926 and is headquartered in Evansville, Indiana.

150+ employees, **7+ Brands**

4 Major manufacture facilities

8 Remote Locations

400+ devices

Qualys Products

CSAM | **VMDR** | **Patch** | **EDR** | **SaaSDR**

Q&A

Qualys®