NeuShield®
How much is your data worth?

CARISEC GLOBAL

Ultimate Anti-Data Compromise Defense

RECOVER INSTANTLY FROM ANY RANSOMWARE ATTACK or OPERATIONAL INCIDENTS

June 2024

Confidential and private document. Not for distribution

SECTION

Challenges in Cybersecurity

Challenges in Cybersecurity

ECONOMIC DISADVANTAGE

The economics are on the side of the attacker.

PRECISION MATTERS

Organizations must be right 100% of the time whereas attackers only need to succeed once.

ADAPTIVE THREATS

Ransomware algorithms are continually evading existing security solutions.

SOPHISTICATED ADVERSARIES

Ransomware gangs are outpacing IT security teams.

EVOLUTION OF TACTICS

The latest wave of attacks operate without traditional malware. Examples:

- LOLBINs
- Volt / Flax Typhoon

This evolution makes detection more challenging than ever.

Sources:
Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft Security Blog

Playing by the rules – You always lose

- Blanket zero trust / lock down is the only solution
  - You will have no functional business
- Malware engines will never stop every attack
  - Every product has multiple engines and still miss hidden vectors and patterns
- Human’s will always be a constant
  - Errors will always be a constant
- Budgets and belief will constrain your capability

When an attack has evaded your security boundaries

- You don’t have anymore mallets
- You will get budget to rebuild
- You will deploy the same again, but more restrictive

Ransomware Infection Challenges

Why it takes weeks to recover from an attack with competing solutions

INFECTION AND DAMAGE

BACKUP SYSTEMS:

- Backup data gets damaged
- Incomplete backups

WORKSTATIONS AND SERVERS:

- 1000’s of devices infected
- Security software disabled
- Applications stop working
- User data gets encrypted

DIFFICULT RECOVERY

DATA CANNOT BE RESTORED ON INFECTED DEVICES:

- Servers and workstations need reimaging
- Email and apps need to be reconfigured
- Clean devices need to be moved to an isolated network

RECOVERY CHALLENGES

LIMITED # DEVICES CAN BE RESTORED CONCURRENTLY:

- Limited IT staff
- Limited network capacity
- Limited backup and storage I/O

FINANCE:

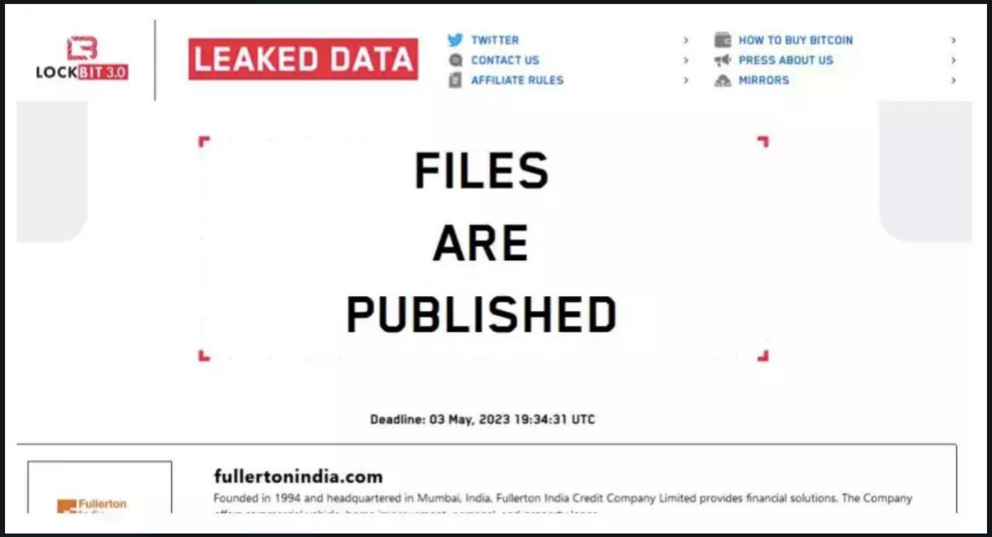
- Unbudgeted Costs for:
  - Incident Response Resources
  - Infrastructure
- Revenue and Reputation losses

Case Study

LockBit 3.0 Encrypted and Stole Data

600GB - PII, Banking, RTGS, NEFT, etc.

Ransom - Rs. 24 crore



FILES ARE PUBLISHED

Deadline: 03 May, 2023 19:34:31 UTC

fullertonindia.com

Founded in 1994 and headquartered in Mumbai, India. Fullerton India Credit Company Limited provides financial solutions. The Company

Fullerton India

- April 2023 Fullerton India, a NBFC, was targeted by a ransomware attack. Fullerton India refused to pay the ransom, and the attackers released over 600 GB of data from Fullerton India onto the dark web. The data included customer information, financial data and intellectual property. The attack had a significant impact on Fullerton India, and the company took over 3 months to recover.

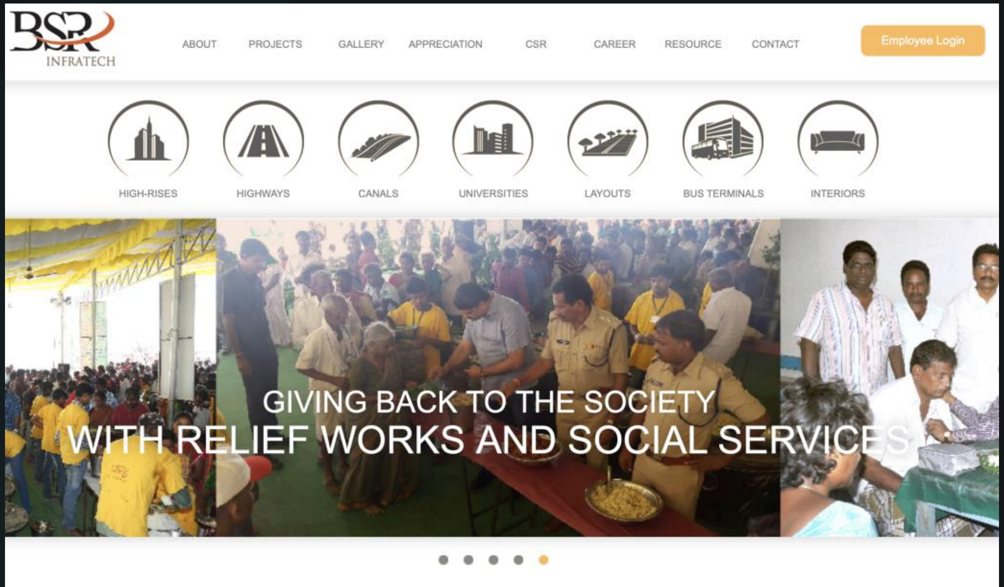
Sources:
https://ciso.economictimes.indiatimes.com/news/data-breaches/breaking-over-600-gb-of-fullerton-indias-data-published-on-dark-web/100057322

Case Study

Encrypted and Stole Data

01 10 PII, Business, Customer Data

Ransom - Rs 66.70 lakh



BSR INFRATECH INDIA LTD.
A firm located in Yelahanka offering construction services, were hacked on Feb 27, 2024. The incident came to light on March 28 after a police complaint was filed on behalf of BSR Infratech. The hacker gained access to details of employees, clients, customers, business details and others. The data files were then encrypted. Servers were still down in April as data was still being copied.

Sources:
https://www.deccanherald.com/india/karnataka/bengaluru/ransomware-attack-hits-b-luru-firm-criminals-demand-80-000-2958894

Case Study

LockBit, Himalaya, Blackbyte, CLOP, 8Base, etc.

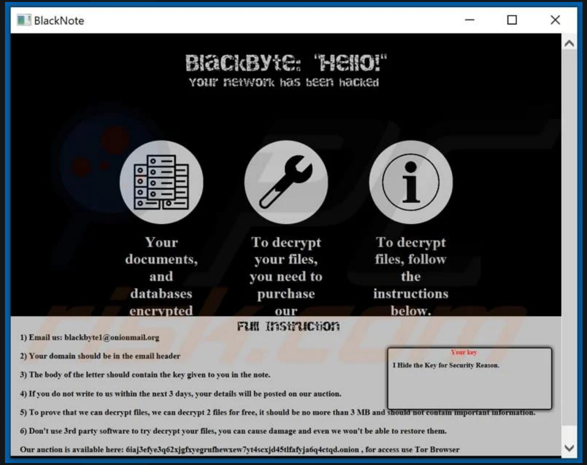
01
10

Ransom payment is only one penalty – ransomware disruption creates business instability.

Non-regulated sectors lack stringent disclosure laws. Consumers are vulnerable to breaches without adequate notifications.

MULTI-INDUSTRY

India is a growth target for ransomware



BlackByte: "Hello!"
Your network has been hacked

Your documents, and databases encrypted

To decrypt your files, you need to purchase our

To decrypt files, follow the instructions below.

Full Instruction

1) Email us: blackbyte1@onionmail.org

2) Your domain should be in the email header

3) The body of the letter should contain the key given to you in the note.

4) If you do not write to us within the next 3 days, your details will be posted on our auction.

5) To prove that we can decrypt files, we can decrypt 2 files for free, it should be no more than 3 MB and should not contain important information.

6) Don't use 3rd party software to try decrypt your files, you can cause damage and even we won't be able to restore them.

Our auction is available here: 6iaj3efye3q62xjgfxyegrufhewxew7yt4scxjd45tlfafyja6q4ctqd.onion , for access use Tor Browser

Your key

I Hide the Key for Security Reason.

2024 - EVERY INDUSTRY IS A RANSOMWARE TARGET

- **Polycab India** - Wire and cable manufacturing - March
- **Motilal Oswal** – Brokerage - February
- **BIRA 91** – Craft beer – March
- In 2023, median ransom demands increased from ₹5.42 Crore to ₹5.79 Crore (up 3%) but median payouts decreased from ₹2.91 to ₹1.98 Crore (down 32%).
- Around 44 per cent of impacted computers were encrypted in attacks against Indian victims, with 34 per cent of attacks involving data theft in addition to encryption.

Sources:
https://regtechtimes.com/ransomware-attacks-2024/
https://economictimes.indiatimes.com/tech/technology/manufacturing-sector-worst-hit-by-ransomware-in-india-palo-alto-networks-report/articleshow/108795601.cms?from=mdr
https://www.business-standard.com/industry/news/64-firms-report-ransomware-attacks-in-india-65-opt-to-pay-ransom-report-124051400881_1.html

WHY

NeuShield

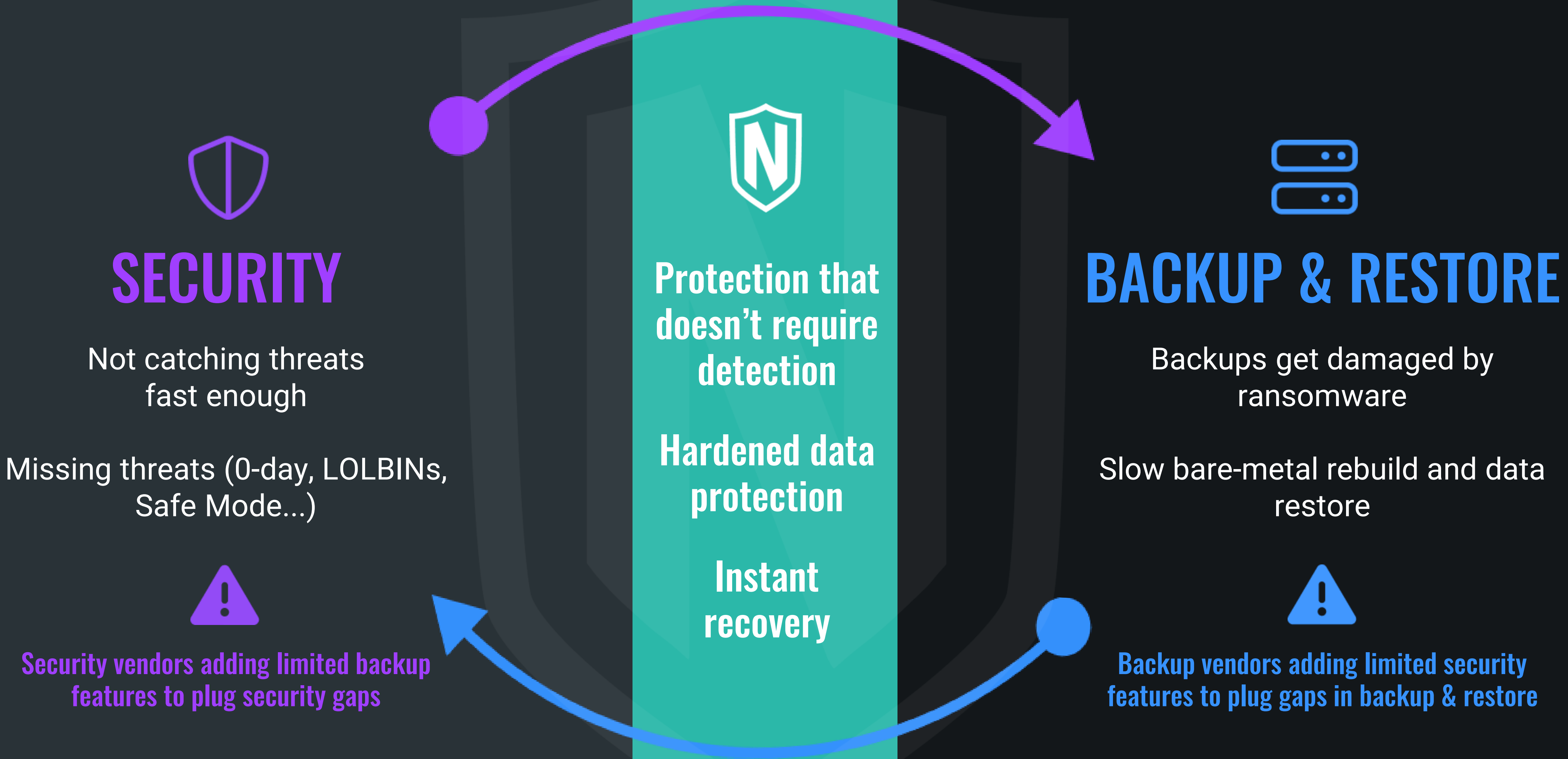
NeuShield Overview

- Multi-layered endpoint solution with SaaS management
- Recovers from undetectable attacks
- Removes all known, unknown, and zero-day malware
- Rapidly restores the entire environment

THE CHANNEL CO. CRN CHANNEL CHIEFS 2024
THE CHANNEL CO. CRN PARTNER PROGRAM GUIDE 2023
THE CHANNEL CO. CRN STELLAR STARTUPS 2023
THE CHANNEL CO. CRN PARTNER PROGRAM GUIDE 2023
ASTORS AMERICAN SECURITY TODAY 2023 GOLD AWARD WINNER HOMELAND SECURITY AWARDS
THE CHANNEL CO. CRN EMERGING VENDORS 2022
Info Security Products Guide 2019 GLOBAL EXCELLENCE GOLD ★★★★★
ASTORS AMERICAN SECURITY TODAY 2019 SILVER AWARD WINNER HOMELAND SECURITY AWARDS

WHATS UNIQUE

- INDUSTRY'S BEST RTO & TCO
- RESTORES WITHOUT A BACKUP
- REPAIRS WITHOUT DETECTION



SECURITY

Not catching threats fast enough

Missing threats (0-day, LOLBINs, Safe Mode...)

Security vendors adding limited backup features to plug security gaps

Protection that doesn't require detection

Hardened data protection

Instant recovery

BACKUP & RESTORE

Backups get damaged by ransomware

Slow bare-metal rebuild and data restore

Backup vendors adding limited security features to plug gaps in backup & restore

Who is NeuShield?

FOUNDED
2017

HEADQUARTERS
SILICON VALLEY

COMPANY FOCUS
RANSOMWARE PROTECTION

Yuen Pin Yeap

CEO, CO-FOUNDER

- 30+ years industry experience
- Created foundation of Symantec Endpoint Protection
- 16 patents

Elisha Riedlinger

COO

- 20+ years in Product Management
- Managed industry leading FireEye/Mandiant endpoint solution
- Launched Symantec's flagship endpoint product

Fei (Philip) Qi

CTO & ARCHITECT, CO-FOUNDER

- 20+ years' experience in cybersecurity engineering and architecture
- Architect of Websense / Forcepoint endpoint products
- Created Symantec Network Access Control

SYGATE   Symantec   websense ESSENTIAL INFORMATION PROTECTION   Forcepoint   FIREEYE   MANDIANT

NeuShield Value

COMPREHENSIVE RECOVERY

- Rapid recovery of entire environment in minutes
- Addresses limitations imposed by rollback and Shadow Copy

EXFILTRATION PROTECTION

- Prevent key data from leaving the corporation

DETECTION & PROTECTION

- Actionable early warning of ransomware
- Prevent malware from damaging or encrypting data

COST SAVINGS

- Reduce TCO for backups and incident response
- Fastest time to value

Layers of Protection

FILE PROTECTION

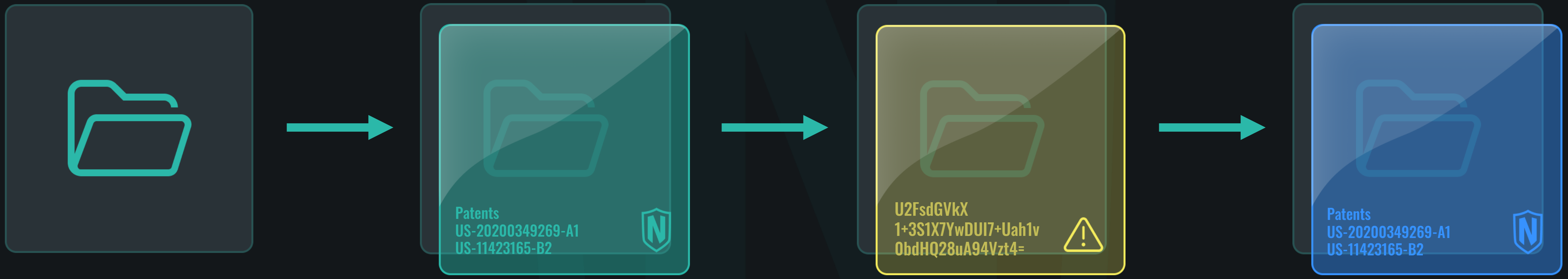
OS RESTORE

DATABASE EXFILTRATION PROTECTION

DEVICE HARDENING & PROTECTION

Mirror Shielding™

Instant Data Recovery & File Protection



ALL DATA

All files on disk and cloud storage

NEUSHIELD DATA SENTINEL OVERLAY

NeuShield adds an impenetrable protective overlay

RANSOMWARE ENCRYPTS FILES

Encryption is contained to the protective overlay,
actual files are never modified

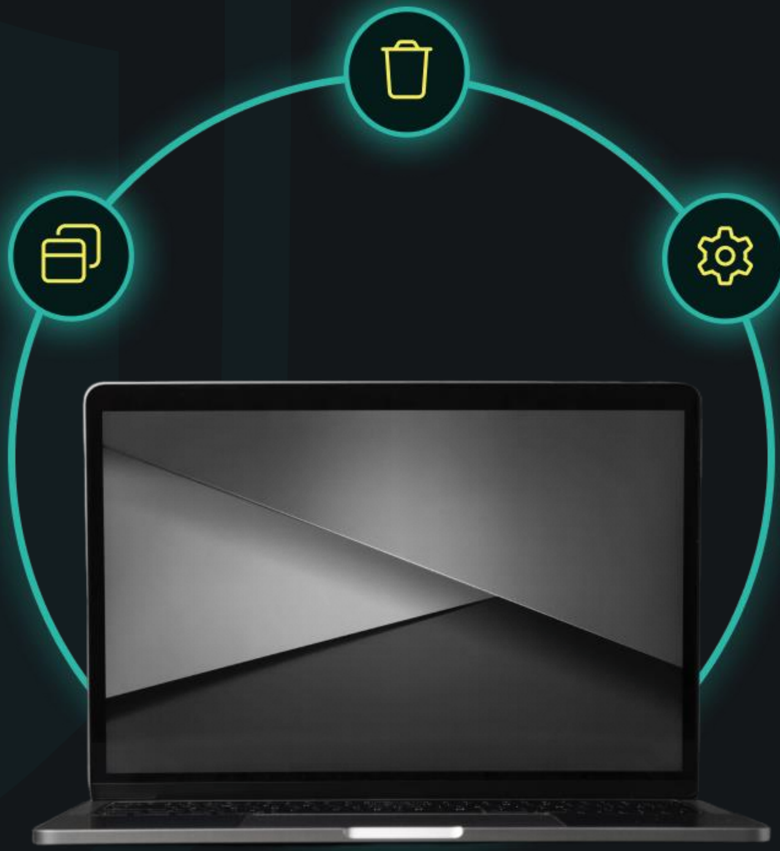
NEUSHIELD WIPES OVERLAY CLEAN

Original unmodified files are instantly exposed

One-Click Restore™

Operating System Recovery

- ✓ Restores entire operating system within minutes
  - User accounts, drivers, services, tasks, registry keys
  - Applications including desktop & browser settings
- ✓ Removes fully undetectable (FUD) malware
- ✓ Works offline and when backups fail



Database Guardian

Database Encryption and Exfiltration Prevention

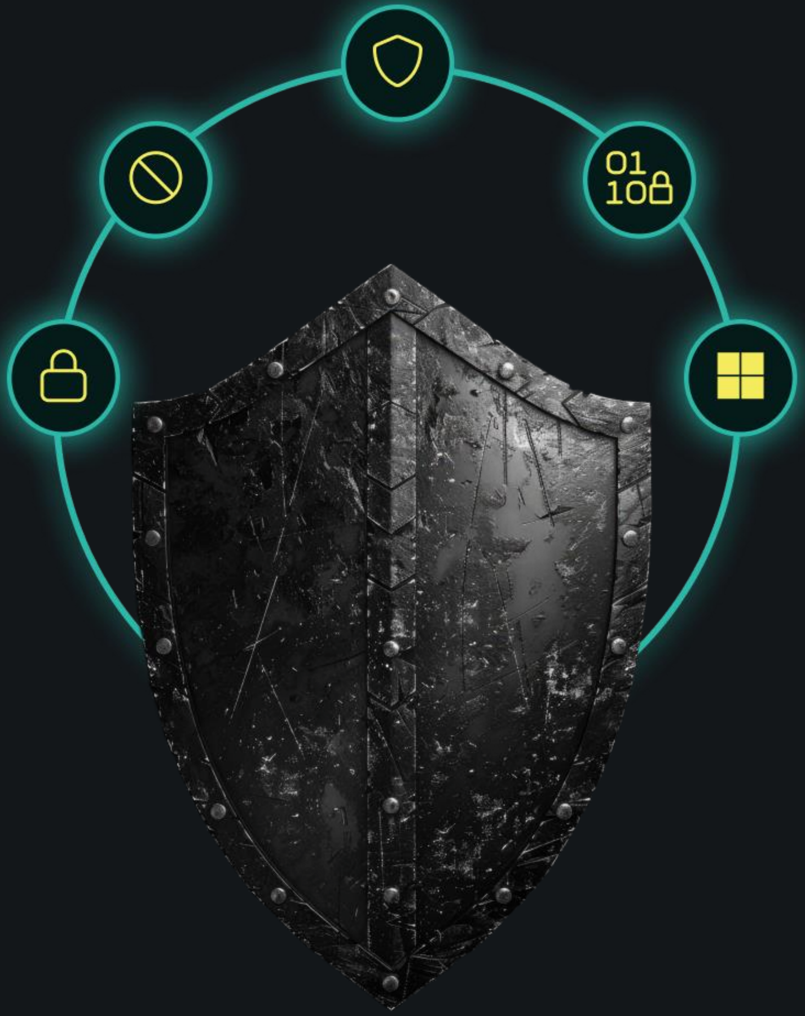
- ✓ Recovers the database server to a fully operational state
  - No need to rebuild the database from scratch after a ransomware attack
- ✓ Prevent database from being encrypted
  - Ensures only database processes can modify database files
  - Covers database instances, data, transaction logs, indexes, binary files and configuration
- ✓ Hides database files from non-database processes
  - Prevents remote and local attackers from stealing the data

EXFILTRATION PROTECTION

Device Hardening & Protection

Boot, Disk Wipe and Safe Mode

- ✓ Locks boot record / sector from changes
  - Stops malware from taking over the boot process
- ✓ Prevents writing to disk using raw / direct disk access
  - Stops wiperware from damaging data on disk
- ✓ Uniquely protects data in Safe Mode
- ✓ System Lockdown prevents re-encryption of data
- ✓ Signed & certified by Microsoft



Data-Driven Detection

Protects Files from Malicious Changes

✓ Compares before and after data has changed

- Checks if content has changed from a known to an unknown structure
- Our unique Mirror Shielding™ makes it easy to compare versions

✓ Provides early warning and alerts administrator and user

- Allows administrators to act before other machines are encrypted

✓ Doesn't rely on baselining, learning, or chasing signatures

- Doesn’t scan for malware processes or infections
- Works when other solutions fail to detect zero-day threats

Administration

EASY MANAGEMENT

SAAS WEB CONSOLE

Available anywhere, anytime

STREAMLINED UX

Simple deployment, quick configuration

ENTERPRISE FEATURES

MULTI-ORG

Manage organizations separately

REMOTE RECOVERY

Easily recover remote offices and workers

Cost Savings

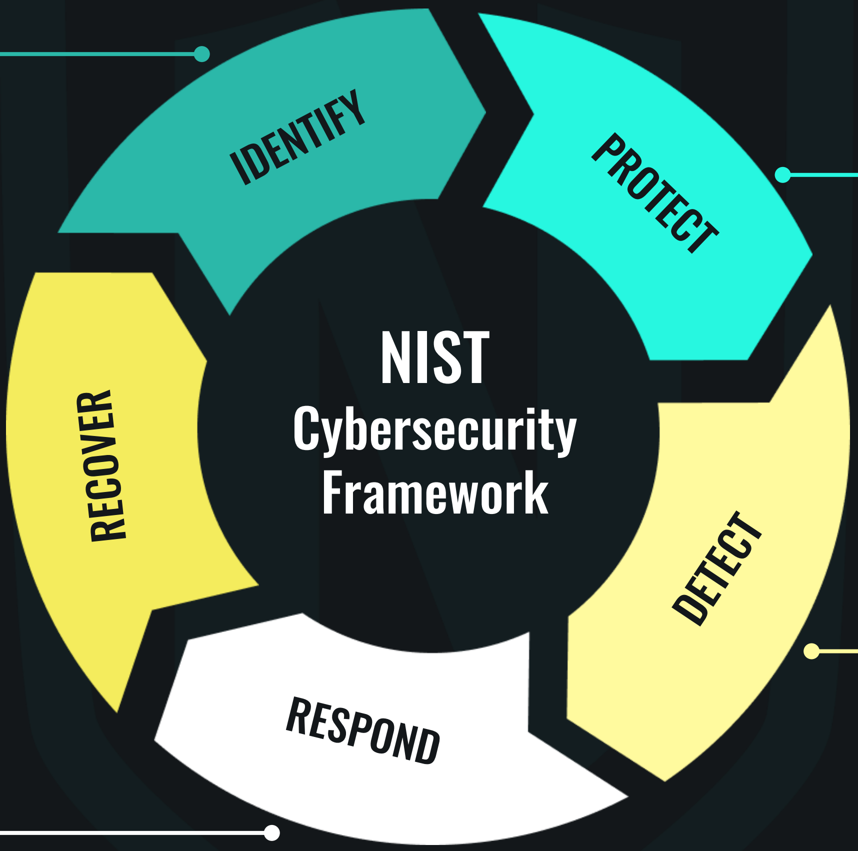
- ✓ Rapid ransomware recovery, hours vs. weeks
- ✓ Up to **6x** faster helpdesk / incident response times

  Bad patches, incorrect config, locked device, unwanted apps
- ✓ Over **50%** reduction in 3-2-1 storage

COST SAVINGS

Footprint

- ✓ **CPU** – negligible, less than 0.1%
- ✓ **Memory** – tiny, around 25 MBs
- ✓ **I/O** – virtually no additional disk activity, just writing to a different location
- ✓ **Disk Space** – 10% (on average)



IDENTIFY

Device information
Data health

RECOVER

Entire environment
Operating systems
Data (database & flat files)

RESPOND

Lockdown
Remote commands
Cost savings

PROTECT

Zero trust / Zero day
Known and unknown
Prevent data damage
Prevent exfiltration

DETECT

Early warning
Data driven

Summary

- ✓ Quickest ransomware recovery on the market
- ✓ Protects critical information from being stolen
- ✓ Works when other solutions fail
- ✓ Saves money and resources
- ✓ Patented and proven technology

NeuShield®
How much is your data worth?

CARISEC GLOBAL

Thank you!

WWW.CARISEC.GLOBAL