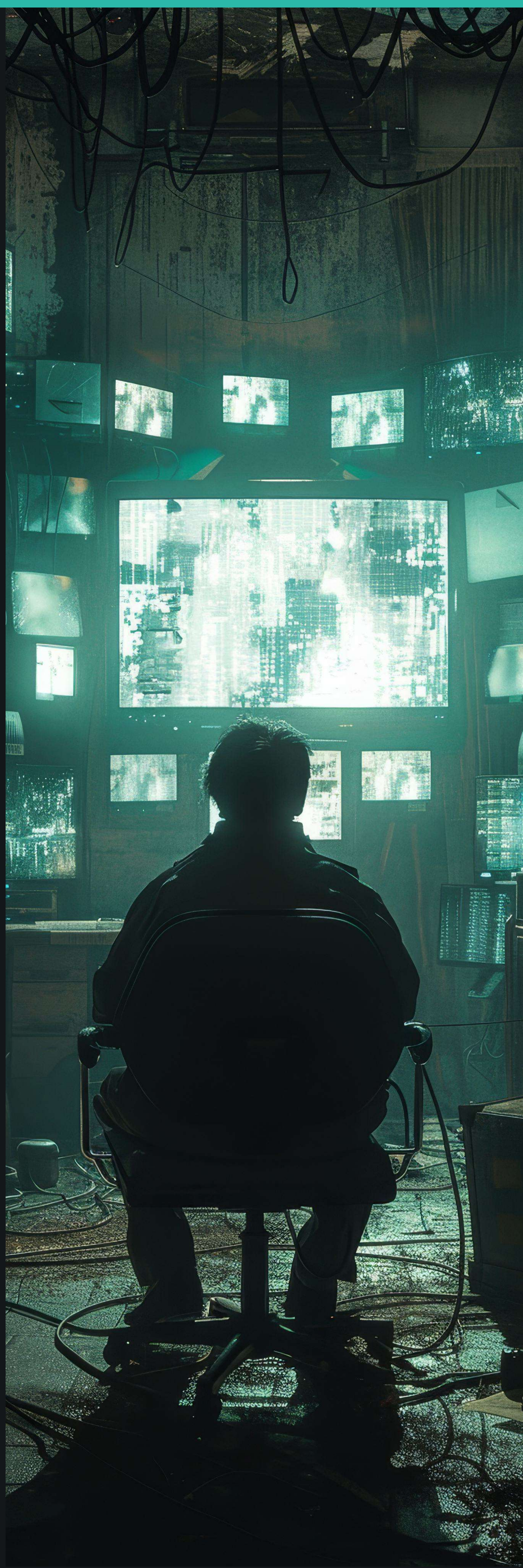
NeuShield®

How much is your data worth?

Obliterating MS SQL attacks

MAKE RANSOM DEMANDS IRRELEVANT AND DRIVE DOWN THE COSTS OF RECOVERY



Make Ransom Demands Irrelevant and Drive Down the Costs of Recovery

- Outperform data protection objectives for your systems.
- End reliance on traditional lengthy and expensive backups for recovery.
- NeuShield delivers rapid MS SQL data protection and restoration.
- Achievable in minutes, you will be able to re-establish business operations with minimal financial, reputation or operational disruption.

NEUSHIELD GUARANTEES

- No exfiltration of data or unauthorized data modification
- 99% faster business continuity after a ransomware attack
- Minimized recovery costs
- Never pay a ransom demand

TEST OUR RANSOMWARE PROTECTION PROMISES WITHOUT OBLIGATION.

For questions about this paper and to find out more about how NeuShield works:
Sales@neushield.com or call **+1 510-239-7962**

MS SQL Server Protection and Recovery - Not Fit for Purpose

MS SQL servers are database management systems (DBMS) that store some of an organization's most sensitive data for critical online services and applications. Database (DBA) and Security Administrators are tasked to ensure that this technology has no configuration flaws and is secure from unauthorized DBMS access, data manipulation and exfiltration.

Unfortunately, DBMS software faults (and human oversights) are recurring operational challenges that threaten even the best practices of the administrators. Then there's the fast-evolving landscape of cyber threats from existing, new and resurgent players (groups and gangs) which continually surface in waves of disruptive and financially impacting activities.

As well as targeting DBMS to steal TBs of database data, they will also modify system files to inhibit business processing and undermine recovery processes.

These types of attacks are sophisticated and devastating to organizations. Typical threat paths include:

1. Initial access is gained via numerous entry points (email, social engineering, lateral network movement) into the MS SQL server, using publicly exposed weak or stolen credentials.
2. Once inside, the attackers execute a command line or PowerShell script that pulls down additional scripts, scouts the environment and eventually sends the payload from a remote server to execute on the DBMS. Some of these files include updt.ps1, system.bat, and tzt.exe.
3. The payload then tries to delete Volume Shadow copies to prevent data recovery and uses Microsoft's wevtutil command line utility to clear application, security (including firewalls), and system event logs to prevent forensic analysis.
4. The next steps involve establishing long-term access persistence, exfiltrating files, and encrypting data files, changing valid extensions (.mdb, .mdf, .ndf, .ov, .oecl, etc.) with ransomware extensions (.malox, .FARGO3, .exploit, .avast, .bitenc, .xollam, as well as the victims' names) setting the stage for the ransomware demand distribution.

EXAMPLE:

Since 2021 the Mallox ransomware group (also known as TargetCompany, FARGO, and Tohnichi) has been actively targeting and attacking Microsoft SQL (MS-SQL) servers. The group's activities increased by a staggering 174% in 2023 compared to the previous year[1]. In September 2023, DB#JAMMER attacks on MS SQL DBMS infrastructures were exposed. Tactics employed by this threat actor exploited vulnerabilities in these servers, introducing formidable tools such as Cobalt Strike and the emerging ransomware variant, FreeWorld[2],

After An Attack

OPERATIONAL CHALLENGES, RECOVERY, AND LIMITATIONS

Following a cyber attack, the DBA and Security Administrators will revert to their well-documented MS SQL DBMS recovery process built for system failures, including sudden power failure, virus or malware infection, abrupt system shutdown or hardware failure issues. Unfortunately the documented recoveryz process for virus or malware infection does not factor in the complexity of intent (by the attacker) with a ransomware attack.

CONSIDERATION BEFORE RECOVERY

When a cyber-criminal successfully targets an organization with sophisticated malware, such as the type used in ransomware, the organization must react immediately. There will be multiple challenges that need to be prioritized prior to recovery of your affected critical MS SQL DBMS. Only once these challenges are addressed can you restore data and systems to a level that enables adequate business operations to resume.

CHALLENGE CONSIDERATIONS

The eight ‘challenge considerations’ shown below outline critical impacts to both business and operations.
See **Appendix A** for greater detail.

CHALLENGE 1

Exposure

How much data is encrypted, what data may have been exfiltrated?

CHALLENGE 2

Payment

Do/can we pay the ransom to decrypt the data?

CHALLENGE 3

Trust

Can I trust the attacker to:
1. Provide the decryption key(s) and
2. Never publish the data?

CHALLENGE 4

Damage

Have the attackers compromised system files as well as database data files?

CHALLENGE 5

Access

Do we still have access to the Shadow Volume copies and backups for data/ device recovery?

CHALLENGE 6

Recover

Are the backups and Shadow Volume copies stable and is there an appropriate recovery point for MS SQL DBMS?

CHALLENGE 7

Time

How long will it take to re-establish all MS SQL DBMS servers?

CHALLENGE 8

Cost

What additional unbudgeted and legal costs will be forced upon the business?

MS SQL DBMS DATA RESTORATION

Recovering lost data is not a serious deal as long as: 1) the basics(master database) are operational, 2) you have access to the backup file(s)/Volume Shadow copies, and 3) you follow the sequence to recover the data files.

System databases, such as: msdb, master, model, and distribution (if you use replication) are critical for the operation of a server instance. Every DBA and their IT Administrators will have ensured that these system databases are included in their backup policy to be restored and recovered.

The disrupted instance of SQL Server must be running to restore any database. Start-up of an instance of SQL Server requires that the master database is accessible - and at least partly usable. If any of these recovery files are unavailable your Incident Response (IR) actions, using standard operating procedures from Microsoft, become unusable. Recovery and Restoration (R&R) of your DBMS then demands that you:

- Rebuild master completely.
- Establish server instance, if available, to restore master from a full database backup.

Regular complex cyberattacks now confront DBAs, security, and IT Administrators with compromised (encrypted / deleted) backup or Volume Shadow copy files. You are now reliant on your ability to restore system files, data and OS backups to a prior clean state from an uncompromised off-site copy.

CURRENT TECHNOLOGICAL LIMITATIONS FOR R&R

Although attractive in their claims, add-on third-party data recovery tools require the same levels of system access and availability as the standard Microsoft procedures: master database active, data being restored should be unencrypted (or hold the decryption key), and a secondary server may be required to restore data.

When a business experiences an attack on MS SQL DBMS its operations are critically incapacitated. DBAs will not have the luxury of time to repair or source any new third-party tools if the SQL server is corrupted by ransomware. Instead, they will go back to the start and create a new SQL server, and then initiate restoring the old data to this new server.

NOTE

Many organizations claim that their existing depth of recovery (using Volume Shadow copies and backups) will respond adequately to neutralize the effect from a ransomware attack.

These recovery techniques do nothing to stop the attacker from exfiltrating the data prior to any data or system compromise.

NeuShield – The Minimum Criteria for MS SQL DBMS ActiveProtection

NeuShield guarantees no data exfiltration, no unauthorized data modification, and enables business continuity 99% faster both during and after a ransomware attack.

NeuShield's Datacenter Editionpositively addresses the critical challenges that impact your business and operations prior to recovery.

THE NEUSHIELD EFFECT - CHALLENGE CONSIDERATIONS

The NeuShield effect on the eight 'challenge considerations' shown below provides confidence in the protection and recovery of your MS SQL DBMS. See **Appendix B** for greater detail.

CHALLENGE 1

Exposure

No exfiltration is possible!

CHALLENGE 2

Payment

No ransom payment is necessary!

CHALLENGE 3

Trust

Businesses retain full control of data and systems!

CHALLENGE 4

Damage

Entire MS SQL DBMS is instantly restored!

CHALLENGE 5

Access

No network of backup dependencies!

CHALLENGE 6

Recover

Data retained is current or prior operational data, not a copy!

CHALLENGE 7

Time

Restoring the MS SQL DBMS can be <99% faster than traditional methods!

CHALLENGE 8

Cost

- No exfiltration
- No encryption
- No deletion
- No Network usage
- No missing RTO or MTD
  = No additional costs

NEUSHIELD HELPS YOU WITH YOUR BUSINESS RISK MANAGEMENT POLICY - PROTECTING REVENUES, CUSTOMERS, REPUTATIONS, INTELLECTUAL PROPERTY, AND MUCH MORE.

With NeuShield you never need to learn about new ransomware vectors that are intent on compromising your MS SQL DBMS systems and data. Never again be at the mercy of new and variants of existing malware that evade detection, subsequently allowing the attacker to disable your systems.

Six Ways NeuShield Architecture Will Fix Aour Current Data Security and Recovery Anomalies

1. **Prevent** data exfiltration from your MS SQL DBMS.
2. **Eradicate instances** of partial or damaged recovery of files. NeuShield assures that your first recovery successfully restores the recovery point objective (RPO) for the entire MS SQL DBMS and data.
3. **Meet your RPO** without any reliance on backups or compromised Volume Shadow copies.
4. **Achieve** your desired recovery time objective (RTO) even network connectivity has been taken down.
5. **Remove** network dependency to carry recovery data. Limit exposure of future malware attacks.
6. **Eliminate** the need for malware identification and removal when initiating data or system incident recovery plans.

NeuShield Obliterates MS SQL DBMS Attacks

The cost of a ransomware attack can run into millions of dollars. It's still taking companies an average of 273 days to adequately identify and contain a breach, costing anything up to $9.48 million[1]. Unplanned costs include business downtime, damaged reputations, compromised networks, regulatory fines, increased insurance, ransom payments, and extra staff costs while rectification is in progress.

Existing backup and recovery software can have hidden costs (on top of your license subscription) to perform your incident response: 5TB of current typical data restoration within a 5-hours RPO can run to more than $100,000 just for network bandwidth (for detailed information on this see our report: How NeuShield can supercharge existing backup strategies[2]).

There are NO hidden costs to recover your MS SQL DBMS with NeuShield Data Sentinel.

DON'T BE THE COMPETITOR THAT GETS LEFT BEHIND WHEN RANSOMWARE STRIKES YOUR SECTOR.

Instantly effective, NeuShield ensures that any malware attack targeting your data and systems will be irrelevant. Your only operational data disruption will be the minutes it takes to initiate NeuShield recovery.

- It ensures that data disruption from malware attacks are non-existent on your business.
- Installing NeuShield's Data Sentinel Datacenter Edition will achieve your minimum acceptable down (MTD) time and RTO, maintaining revenues and business continuance.
- NeuShield protects data and reputations, does not rely on backups, and drastically reduces the cost impacts of experiencing an incident.

Accelerating recovery and ransom risk removal, NeuShield protects and recovers your entire MS SQL DBMS system and data from undetectable threats, malware, and human errors. NeuShield is the active last line of defense in your security stack. It is the only technology on the market that can guarantee business continuance by directly eradicating the limitations of relying on traditional backup and restore methods.

[1] IBM Cost of a Data Breach Report 2023
[2] To be provided by NeuShield

Appendix A

CHALLENGE CONSIDERATIONS

CHALLENGE	BUSINESS OR OPERATIONS	CONCERN	THREAT	RISK
Exposure	Business	You know or are unaware if data has been exfiltrated.	Attacker exposes or threatens to expose sensitive data.	Sensitive data is or will be exposed, damaging both customer and business reputations
Payment	Business	Ransom demand to unlock files or systems.	The attacker will expose the exfiltrated data, financial loss to the business.	If you pay the ransom, do you have the funds and can you claim it back via cyber insurance?
Trust	Business	Reliant on the criminal to keep their side of negotiations.	You have no absolute control over the actions of the criminal.	Can you trust the attacker to 1) provide the decryption key and 2) never publish the data?
Damage	Operations	A malware attack may compromise the DBMS files and not just data.	The attacker has compromised the entire DBMS and may hide files for future compromise.	Do you waste time recovering data and then discover that the DBMS is compromised, extending the re-recovery time?
Access	Business & Operations	Network availability to move backup data and confirm data copies have not been deleted.	Restoration of the DBMS and data is critically dependent on access to data copies (3), and if the network N in a state to transmit backup data Malware may compromise your recovery data.	Disabling networks to protect your infrastructure can restrict access to recovery data until confirmation of malware cleansing is assured. This further delays business continuity.
Recovery	Operations	Being confident that backups and Volume Shadow copies are stable (recoverable) to your desired recovery point.	Backups are known to be Incomplete or have data write errors; and a desired recovery point for Volume Shadow copies has passed.	The desired recovery point may not be achievable. This means that the DBMS and data will need recovering to a prior point. It also means losing access to the more recent data (anything after the available recovery point).
Time	Business & Operations	The elapsed time to re- establish operational continuity of all compromised servers.	Backup vendors claim to instantly recover data. However, this assumes classic recovery situations. It doesn't address the multi-disruptive scenarios which are introduced during cyber attacks.	Failure to meet the RTO for the DBMS and data begins to seriously and unacceptably impede the flow of normal business operations. Time is money. Both are lost.
Cost	Business & Operations	Recovery actions can demand exceptional unbudgeted costs that are vital in order to meet desired RPO and RTO.	The attack will expose failings in data privacy, Incident Recovery capabilities, adequate sustained network bandwidth and exceed your maximum tolerable downtime (MTD).	Obstructions in recovery can add thousands of one-off expenditure to minimize MTD delays. Exposing sensitive customer data risks, regulatory fines, reputation damage and class action lawsuits.

Appendix B

THE NEUSHIELD EFFECT - CHALLENGE CONSIDERATIONS

CHALLENGE	BUSINESS OR OPERATIONS	CONCERN	NEUSHIELD EFFECT	NEUSHIELD DATACENTER EDITION DELIVERABLES
Exposure	Business	You know or are unaware if data has been exfiltrated.	No exfiltration is possible.	No exfiltration is possible. NeuShield protects the data from being exfiltrated by hiding files from any application or program. This ensures that remote and local attackers are unable to steal or copy your sensitive data.
Payment	Business	Ransom demand to unlock files / systems.	No ransom payment is necessary.	NeuShield's impenetrable Mirror Shielding.", Database Guardian, and anti-exfiltration architecture mitigates any prohibited file modification and subsequent ransom demand for data decryption.
Trust	Business	Reliant on the criminal to keep their side of negotiations.	Businesses retain full control of data and systems.	NeuShield negates future criminal back-tracking ensuring that data recovery controls always remain with the business.
Damage	Operations	A malware attack may compromise the DBMS files and not just data.	Entire MS SQL DBMS is Instantly restored.	NeuShield's One-Click Restore always recovers the entire MS SQL DBMS after an attack. This ensures that critical system databases, files and data are the same as before the Incident or a chosen RPO.
Access	Business & Operations	Network availability to move backup data and confirm data copies have not been deleted.	No network or backup dependencies.	NeuShield has no reliance on networks to transfer data. All recovery commands can be executed on the compromised devices. If centralized recovery is stipulated, a network connection would be required to send a single command to the devices. Full system and data recovery happens without further IT Admin involvement.
Recovery	Operations	Being confident that backups and Volume Shadow copies are stable {recoverable/ to your desired recovery point.	Data retained is current or prior operational data, not a copy.	NeuShield does not perform backup copies. All data is operational data that never leaves the device. One-Click Restore, Data Engrains and copies of the entire MS SQL DBMS system databases, files and data ensures an RPO for the prior 7 days can be established.
Time	Business & Operations	The elapsed time to re-establish operational continuity of all compromised servers.	Restoring the MS SQL DBMS can be <99% faster than traditional recovery methods.	NeuShield is unique as it deletes the compromised data prior to re-establishing the RPO data. Deleting data is faster than rebuilding data - minutes compared to hours/days, Immaterial of TBs of data being protected. NeuShield recovers in-place with no reliance on sustained bandwidth to move data. Operations can recover multiple instances of MS SQL DBMS simultaneously meeting your MTD and an accelerated RTO <99% faster than traditional methods.
Cost	Business & Operations	Recovery actions can demand exceptional unbudgeted costs that are vital in order to meet desired RPO and RTO.	No exfiltration, no encryption, no deletion, no network usage, no missing RTO or MTO equals no additional costs.	Installing NeuShleld on your MS SQL DBMS, servers and workstations helps to avoid costs from operational downtime, damaged or stolen data, regulatory fines, and reputations/ damage.

NeuShield®
How much is your data worth?

Contact us today to actively protect your data and deliver instant recovery. Re-establish operations faster without additional costs.

NeuShield Data Sentinel does more than just detecting and blocking ransomware. We're the only anti-ransomware solution that can recover encrypted data from any known, unknown or zero-day threat. No matter how much data is encrypted NeuShield can get it back instantly from any laptop, desktop or server. NeuShield is an endpoint agent that works locally to recover data without using a backup or internet connection.

sales@neushield.com

NeuShield, Inc
200 Brown Road, Suite 306
Fremont, CA 94539
Main: +1 510-239-7962
Toll Free: +1 888-999-0965 (U.S.)

WWW.NEUSHIELD.COM