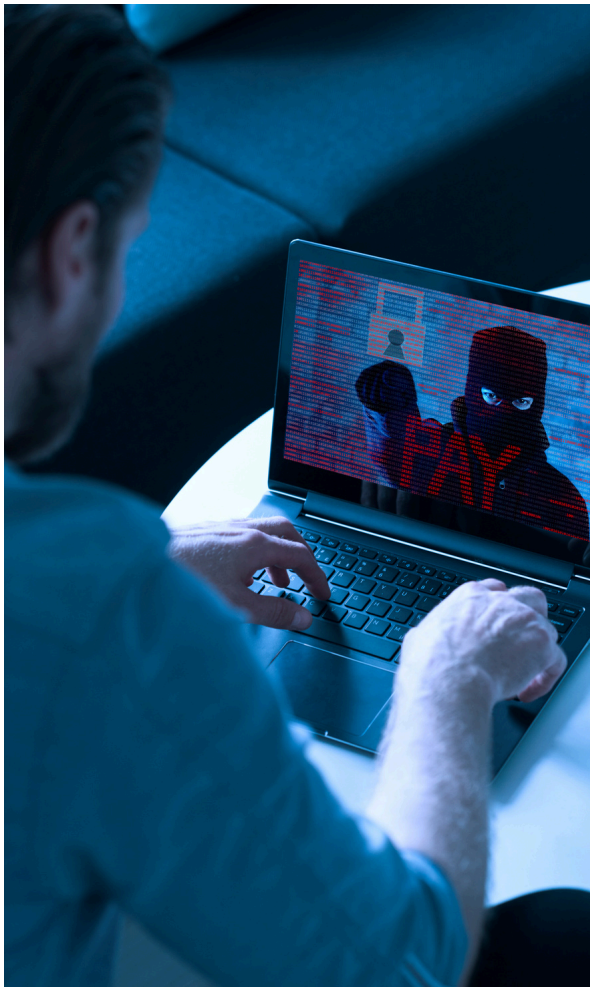
VANNADIUM

Ransomware Safety Net

Continuity of Operations at the Speed of Crisis

Overview: Ransomware attacks are no longer rare, they're expected. They're escalating in cost, frequency, and impact. Vannadium provides an operational safety net that ensures you never stop working.

The Problem: Ransomware Is a Growing Threat to Healthcare and Beyond



- In the U.S. healthcare sector alone, ransomware has become the leading cause of data breaches, compromising 285 million patient records over the past 15 years—and accounting for 69% of records exposed in 2024 Michigan State University.
- One recent attack on DaVita affected 2.7 million patients, and cost over $13.5 million in remediation and operational expenses The HIPAA Journal+11Reuters+11Tom's Guide+11.
- In 2024, the U.S. healthcare sector saw 14 breaches each impacting over 1 million records, totaling nearly 238 million affected individuals, roughly 70% of the U.S. population The HIPAA Journal+3Rubrik+3DeepStrike+3.

These trends highlight escalating risks to patient safety, financial stability, and organizational continuity, pointing to the urgent need for more resilient data continuity approaches.

VANNADIUM

Ransomware Safety Net

Our Solution: Real-Time Data Continuity That Acts Like an Emergency Backup Generator

Vannadium is more than a cybersecurity vendor, it's an operational resilience partner. Our sovereign data infrastructure twins incoming data in real time and distributes it across a highly redundant, distributed mesh network. In the event of a ransomware attack, clean copies of your data are instantly accessible outside the compromised environment, ensuring uninterrupted operations without ever paying ransom.

Key Value Propositions

- Continuity of Operations: Systems stay online, even mid-attack.
- Instant Data Restoration: Clean data is recoverable in seconds, not days.
- Immutable Audit Trail: Every data change is logged in real time for easy rollback.
- Seamless Integration: Works with existing IT systems; no rip-and-replace required.
- Zero-Ransom Assurance: Focuses on resilience, not prevention.

Ransomware Resilience Through Distributed Backups

- Live Data Twinning: Incoming data is captured and tokenized at the edge.
- Distributed Redundancy: Tokenized data is routed in parallel across hundreds of thousands of nodes.
- Immutable Storage: Data versions are stored with cryptographic integrity.
- On-Demand Recovery: If production data is compromised, clean versions are ready immediately.

Don't Pay. Don't Pause. Stay Online.

Contact us to explore how Vannadium can provide your organization with a ransomware safety net built for zero downtime and maximum resilience.

Get in touch

solutions@vannadium.com

https://vannadium.com