CASE STUDY

Prodatix Ransomware Resilience

Ransomware Recovery Success Story

Prodatix Ransomware Resilience: Ransomware Recovery Success Story

When ransomware struck, it threatened to bring one of the nation's leading engineering firms to its knees.

The challenge

The engineering company faced a devastating $2.5 million ransom demand, along with multi-million dollar remediation costs, reputational damage and severe business disruption.

The response

Prodatix enabled our client to return to business as usual within 48 hours, turning a potential crisis into a testament to ***preparedness and partnership.***

The solution

In this Case Study, we will share the full story of the ransomware attack that posed an existential threat to our client, including insider details of how they responded with the help of Prodatix.

Setting the Scene

About The Target

Our client, the target of the attack, is a leading engineering firm specializing in high-stakes federal government projects and large-scale infrastructure development, including hospitals, bridges, and other monumental undertakings.

The company employs over 250 people distributed across two office locations and maintains a hybrid work environment to support both in-office and remote employees. With a reputation for tackling complex engineering challenges, the company depends heavily on its advanced IT infrastructure for day-to-day operations, project management, and communication.

IT Infrastructure

The IT ecosystem is entirely on-premises, underscoring the firm's self-reliant approach to data management and security. Their setup consists of 40 virtual machines (VMs) running on four host servers within a VMware environment. The two offices are interconnected via a VPN, with all data stored centrally at the primary location.

While this setup provided operational efficiency, it also exposed vulnerabilities due to the lack of multi-factor authentication (MFA) and reliance on simple password configurations. The absence of cloud-based operational services meant the company's data was confined to its physical infrastructure, amplifying the risks associated with localized attacks.

Data Protection Setup

Before the ransomware attack, the company employed a dual-pronged approach to data protection:

On-site Backups: Two Veeam servers handled the backups, each covering half of the virtual machines. However, these backups were not stored in immutable storage, making them susceptible to tampering during a cyberattack.

Off-site Backups: Hourly replication of critical data was performed to Prodatix's immutable storage at an off-site data center. This aligned with the 3-2-1 backup strategy, ensuring a degree of resilience against data loss.

Prodatix, as the data protection partner, had conducted a comprehensive risk analysis, identifying the need for on-premises immutable storage as a critical enhancement to their existing setup. While this was recognized as a priority, budget constraints delayed the implementation, with plans deferred to 2025. Matt Bullock from Prodatix aptly summarized the risk: "Ransomware waits for no one."

This environment, while robust in theory, was not enough to protect against modern threats like advanced ransomware. The absence of on-premises immutable storage and insufficient safeguards for remote access created significant exposure, setting the stage for the devastating ransomware attack.

The Attack

Ransomware struck on a Friday evening—a prime target window when IT teams are minimally staffed, and vulnerabilities are more likely to go unnoticed. The attackers launched a sophisticated brute force assault on the company's VPN, exploiting weak passwords and the absence of multi-factor authentication (MFA) to gain entry. This method, though less common compared to phishing attacks, remains highly effective when organizations fail to enforce basic cybersecurity measures.

By 8:20 p.m., the attackers had breached the central server through the compromised VPN. **They injected ransomware which spread rapidly across the environment, encrypting all 40 virtual machines in under an hour.** Employees working late at the secondary office began experiencing connectivity issues around 10 p.m. Initially, they assumed it was a routine network glitch, but when local diagnostics showed no issues, they alerted the IT Director to investigate further.

Their IT Director arrived at the primary office just after 11 p.m., prepared for a possible power outage or hardware failure. However, upon attempting to access the systems, the full scale of the attack became evident. The ransomware had encrypted every file, appending random extensions like ".xbj73encrypt" to signal its malicious intention.

Adding to the chaos, the ransomware activated a "nuclear option" during Prodatix's initial assessment: it deleted the hypervisor and wiped all servers clean within 30 minutes, leaving the IT infrastructure in ruins.

And to make things worse, a ransom demand of $2.5 million in Bitcoin was received and a message to that effect appeared on every desktop. The company was completely paralyzed, and to get back on its feet, they need to make a whopping payment of $2.5 million to the malicious attacker to restore operations.

The Response

Prodatix Notified

The IT Director immediately contacted Prodatix for emergency assistance at 10:15 p.m., triggering a coordinated response from their experienced team. Within minutes, Prodatix assessed the situation and confirmed the catastrophic impact.

While the on-site backups were inaccessible due to the hypervisor wipe, the company's off-site immutable backups at Prodatix's data center remained secure—a critical safeguard against total data loss.

An Unexpected Twist - Insurance Provider Steps In

Prodatix swiftly began preparing for data restoration, but their efforts were delayed by the company's cyber liability insurance provider. The insurer required a forensic investigation before restoration could proceed, citing the need to identify vulnerabilities and ensure compliance with policy terms.

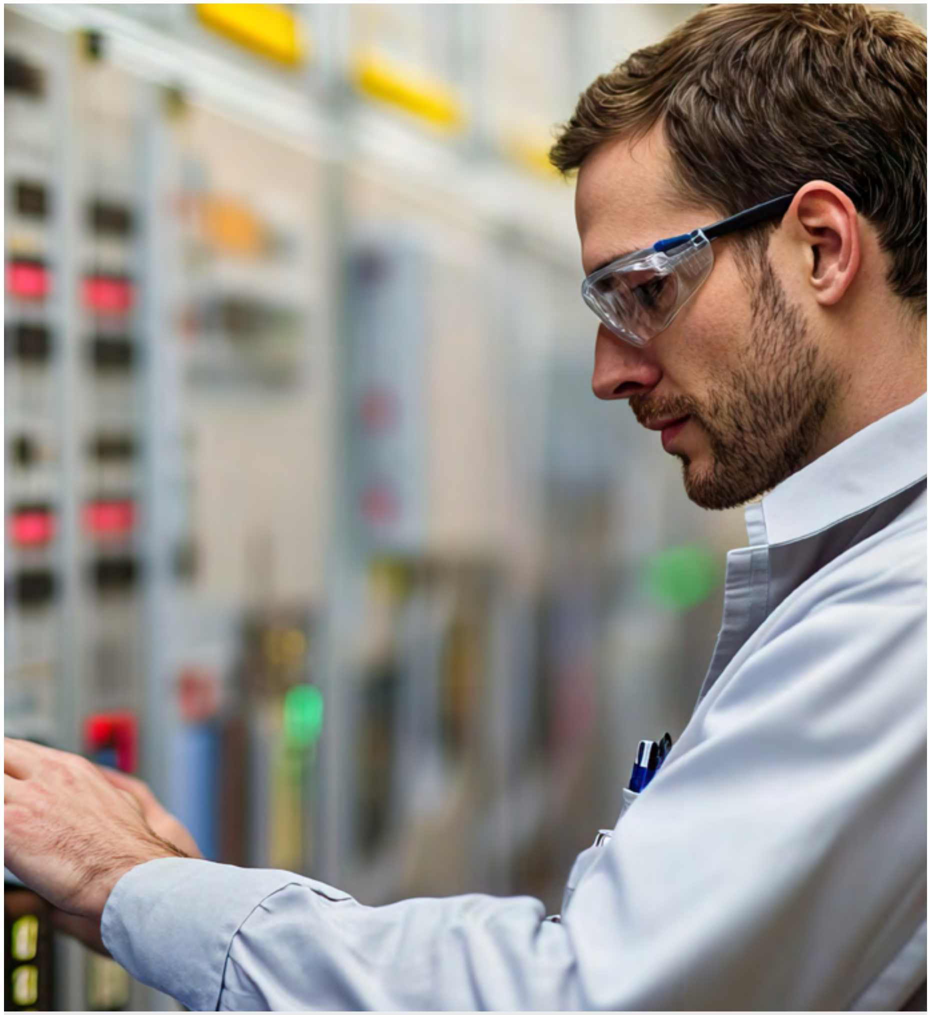
Practically this meant that the insurance company required ALL impacted hardware to be sequestered for inspection by the cyber-forensics team. As every server in the business had been impacted by the attack they were out of action until the investigation completed.

This unexpected hurdle added to the uncertainty, as the investigation could potentially take weeks or even months to complete.

Resilience in Action

Recognizing the urgent need to restore business operations, Prodatix leveraged their disaster recovery environment:

- All 40 virtual machines were fully restored at Prodatix's data center within four hours.
- Pre-configured failover VPN connections ensured immediate access for employees, both remote and on-site.



By Sunday evening, Prodatix's disaster recovery strategy had restored full functionality to the company's systems, allowing them to operate entirely from Prodatix's environment. This proactive planning enabled operational downtime to be avoided and shielded their federal and private-sector clients from any impact of the attack, preserving the company's reputation.

The Aftermath

Business Continuity Restored

By Monday morning, it was back to business as usual, thanks to Prodatix's seamless disaster recovery solution. Employees logged in as they normally would, while Prodatix closely monitored the restored systems to ensure stability and security. Throughout the 34-day forensic analysis period, operations were maintained from Prodatix's data center without any major disruptions.

Once the insurance company approved restoration, Prodatix transitioned operations back to the regular on-site production environment. This phased reintegration, combined with round-the-clock monitoring, ensured minimal risk during the transition. By avoiding prolonged downtime, our client not only preserved its reputation but also avoided the financial losses, excessive remediation costs and reputational damage that often accompany ransomware incidents.

Cost Savings Achieved

Prodatix's timely intervention and advanced capabilities saved the business from paying the $2.5 million ransom demanded by the attackers as well as millions more in remediation costs.

Instead, the financial burden was **limited to $50,000**, covering forensic investigations and additional recovery efforts—a fraction of the potential cost.

Moreover, the company's ability to demonstrate resilience through Prodatix's immutable storage and disaster recovery capabilities solidified their standing with their insurance provider, protecting future coverage terms.

Lessons Learned: Building Your Ransomware

The ransomware attack was a wake-up call, highlighting critical lessons for organizations looking to protect themselves from similar threats. These insights are not just technical checkboxes—they're actionable strategies that can make or break a company's resilience. Here's what we can all learn from this

1

Don't Let Budget Processes Delay Data Protection

One of the clearest takeaways from the company's ordeal is this: ransomware doesn't wait for your budget committee to approve upgrades. They knew their data protection setup had gaps, and they had planned to implement on-premises immutable storage by 2025, but the attackers struck long before that could happen.

The lesson here? If you know there's a critical upgrade needed to safeguard your systems, treat it as an immediate priority, not something to address "next year." Waiting too long for approvals or budget cycles leaves your organization exposed.

2

Plan for Insurance-Driven Access Restrictions

A surprising roadblock during the recovery period was the company's cyber liability insurance provider. You might assume that insurance is there to help you recover quickly, but in reality, it can slow things down. The insurance company required a forensic investigation before allowing any restoration efforts to proceed. This delayed recovery and added stress to an already chaotic situation.

What can businesses do to prepare? Well, first, you need to anticipate that insurance companies may restrict access to your systems during their investigations. Your disaster recovery plan should include contingencies, such as alternative environments (like Prodatix's disaster recovery setup) to keep operations running while you navigate these delays.

3

Understand Your Insurance Policy Conditions

Speaking of insurance, there's an important and often overlooked lesson here: know your policy inside and out. During the forensic investigation, the company's insurer scrutinized every detail of their security practices, searching for any lapse that could nullify the claim.

It's a stark reminder that insurance companies aren't just there to write checks. They're also looking for reasons not to. If your passwords are weak, MFA isn't in place, or backups aren't secure, you might find yourself footing the bill instead of your insurer. The takeaway? Read the fine print, address any vulnerabilities proactively, and document everything to strengthen your position if a claim arises.

4

Enforce Multi-Factor Authentication (MFA)

This point cannot be overstated: MFA is non-negotiable. The attack succeeded because remote access relied on weak passwords, and MFA wasn't implemented. Brute force attacks thrive on these gaps, and they're completely preventable.

Adding MFA to your systems is one of the simplest, most effective ways to block unauthorized access. It's no longer a "nice-to-have"; it's an absolute must. If MFA had been in place, the attackers likely wouldn't have gotten through the VPN.

5

Include PR and Proactive Notifications in Your Response Plan

One of the company's strong points during the crisis was their legal team's quick action in notifying clients, employees, and vendors about the breach. While Prodatix's role was technical, the proactive communication ensured transparency and maintained trust.

The lesson for other businesses? Your response plan shouldn't just cover technical recovery—it must include public relations and a proactive notification strategy. Who do you need to notify? What should you say? How do you balance compliance with maintaining your reputation? These are questions you should answer before an attack happens, not in the heat of the moment.

Choosing the right data protection and security partner is a critical decision for any business aiming to safeguard its assets and ensure operational resilience. With cyber threats evolving rapidly, your partner must offer more than just tools—they should provide a comprehensive strategy tailored to your organization's unique needs. Here's what to prioritize when selecting your data security partner:

Expertise

Your data sec urity partner should bring deep technical expertise and proven experience to the table. Look for:

Certified Professionals: Ensure the provider has qualified staff, such as Veeam architects or similar experts, with relevant certifications and years of hands-on experience.

Industry Knowledge: The team should have decades of expertise across multiple industries, allowing them to anticipate challenges and recommend best practices tailored to your sector.

Custom Solutions: A strong partner doesn't rely on cookie-cutter strategies. They should be able to assess your specific requirements and design solutions that align with your business goals and threat landscape.

Veeam Products Used to Help This Company To Succeed Despite Ransomware

- Veeam Data Platform Premium
- Veeam ONE analytics and monitoring
- Veeam Sure Backup

Consultation and Advisory Approach

The right partner won't merely implement a system and disappear. Instead, they will:

Advise Proactively: Help you navigate complex regulatory requirements, evolving cyber threats, and changing business needs with tailored advice.

Collaborate Closely: Act as an extension of your team to ensure alignment with your operational priorities.

Provide Ongoing Reviews: Conduct regular audits and updates to ensure your security measures evolve alongside emerging threats.

Customizable Solutions for Threat Environments

Your business faces unique risks, and your data protection partner should design solutions accordingly. Seek providers who:

Adapt to Your Needs: Whether you're managing hybrid cloud environments, scaling rapidly, or complying with stringent regulations, they should offer tailored solutions.

Incorporate Advanced Technologies: AI-driven threat detection, automated recovery solutions, and real-time monitoring should be integral to their offerings.

Emphasize Flexibility: Ensure their systems can adapt to shifts in your IT infrastructure or growth demands without major overhauls.

Around-the-Clock Support

Data breaches and system failures don't adhere to business hours. Ensure your partner provides:

24/7/365 Support: Rapid, reliable assistance whenever you need it—especially during critical incidents.

Proactive Monitoring: Continuous monitoring to identify and address vulnerabilities before they become issues.

Dedicated Account Teams: Direct access to experts who understand your system and can resolve issues swiftly.

prodatix
DATA PROTECTION

Choose Prodatix
Your Trusted Data Protection and Security Partner

The ransomware attack highlighted in this case study underscores the importance of working with a provider who goes beyond traditional backup services. Prodatix not only ensured rapid recovery but also safeguarded our client from a multimillion-dollar ransom demand, preserving their reputation and client trust.

Don’t wait until it’s too late to protect your business. Contact Prodatix today to discuss how we can design a data protection and disaster recovery solution tailored to your needs.

Start protecting your business now

Matt Bullock | 623-253-9500 | matt.bullock@prodatix.com

www.prodatix.com