DELL Technologies

Expertise and resources for quick recovery from a cyber attack

Gain confidence that you're well prepared for a disruptive cyber incident

Dell Incident Recovery Retainer Service

The risks and costs of cyber attacks continue to increase. Losing the ability to conduct business operations can harm financial performance, customer relationships, regulatory compliance and company reputation.

When an attack occurs, the speed of response is paramount for a successful recovery. But the effort to restore normal operations can be highly challenging. In addition to containing the incident, IT environments and massive quantities of data must be restored to get critical applications back online with minimal delay.

75%
of organizations will face one or more attacks by 2025[1]

97%
Dell success rate in recovering operations for customers who have experienced a cyber event[2]

16 days
Average downtime after a ransomware attack[3]

Many IT teams do not have sufficient capacity or the combination of skills needed to recover from a cyber attack. With the Dell Incident Recovery Retainer Service, you have a team of industry-certified experts in cybersecurity and infrastructure working by your side to restore your environment. The service includes 120 or 240 hours of recovery assistance, which means there is no wait for order authorization – our team gets going on your recovery right away.

Recovery Readiness Evaluation. At the beginning of the service, we think it's important to understand your organization's current recovery and restoration strategy. Our experienced team reviews your existing recovery plans, network and infrastructure, backup processes and more. The team prepares an evaluation and planning summary report which provides you with a roadmap for strengthening your incident readiness and recovery posture.

Key Benefits

- In the event of an incident:
  - You get rapid response from highly skilled, experienced Dell cybersecurity professionals
  - Our team quickly assesses your situation and determines the best course of action to minimize business interruption
  - The threat is eradicated and the vulnerability that was exploited is closed[4]
- Retainer model provides 120 or 240 hours of annual recovery assistance
- Dell Technologies cybersecurity team brings diverse experience, skills and tools to each unique customer situation
- Initial evaluation of existing recovery capabilities and coverage, including summary report to guide priorities for improvement
- Recovery process is more efficient since Dell team becomes familiar with your environment by conducting the initial evaluation

Key Features

120 or 240 hours per year for incident recovery activities

- Delivered remotely (onsite available in some regions, subject to additional fees)
- Project manager oversees activities
- Assessment of incident and situation
- Assignment and deployment of resources
- Forensic analysis – digital, malware, data
- Threat eradication
- Data sanitization, recovery, preservation
- Re-establish environment and applications

Evaluation of incident recovery capabilities

- Conducted at beginning of engagement
- Discovery of client network, infrastructure and facilities to prepare for response in the event of a cybersecurity incident
- Review incident recovery plan, data backup and restoration capabilities
- Dell prepares a summary report including recommendations for strengthening readiness and recovery posture

Service levels:

- A service initiation meeting is scheduled with the customer within 2 hours of customer's initial request (mean time to react)
- Remote response commences within 6 hours after the service initiation meeting (mean time to respond)
- If onsite response has been agreed upon, it will commence within 24 hours after the service initiation meeting (mean time to respond)

Consumed hours and remaining balance will be reviewed with the customer each quarter

- In the event that hours for recovery and restoration are not fully consumed, remaining hours may be applied to expert assistance in incident recovery planning, cybersecurity improvements and related areas

Be prepared

There's no way to know exactly when your organization will experience a severe cyber incident. Make sure you're prepared with Dell Incident Recovery Retainer Service. You'll have peace of mind knowing highly skilled and experienced cybersecurity professionals will be on the case without delay, working to eliminate the threat and re-establish your critical operations.

Contact your sales representative today

[1]Detect, Protect, Recover: How modern backup applications can protect you from ransomware, Nik Simpson, Gartner, Jan 6 2021, Gartner Document ID G00733304 https://www.gartner.com/en/documents/3995229

[2]Based on Dell analysis of service requests from June 2019 to July 2021 in North America

[3]Why Ransomware Costs Businesses Much More than Money, Forbes, April 30, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=469c541a71c6

[4]If more than the included 120 or 240 annual hours of recovery work is required, additional hours are available for purchase.