

# 勒索软件的恐怖攻击 vs 韧性应对



Veritas NetBackup 作为保护全球 EB 级海量数据的解决方案，可大规模恢复企业关键业务数据。NetBackup 凭借其不断推陈出新的现代化功能在业界处于领先地位，助力企业弥合勒索软件应对韧性战略中的差距。



## 保护

### 分层主动防护

支持 AWS S3 上的防篡改存储，确保合规，同时维护数据完整性。



## 检测

### 全面主动检测

AI/ML 异常检测是整体战略中的一环，有助于确保数据始终可恢复。



## 恢复

### 自动恢复编排

适用于 VMware 的 CDP 低影响备份和即时回滚功能提供一体化的数据保护，实现零停机目标。



勒索软件造成的年损失额将超过 2650 亿美元<sup>1</sup>

到 2031 年，每隔 2 秒就有一家企业遭到勒索软件攻击<sup>1</sup>

## 空前绝后的数字化转型



这次疫情使全球数百万人遭遇了不幸，也触发了全球经济体的快速数字化转型。”

PWC CEE TMT 行业负责人 Dejan Ljustina



为了生存下去，我们不得不进行快速数字化转型。原本计划三年完成的转型战略被生生压缩到 3 个月。虽然艰辛，但我们做到了。”

财富 2000 强企业，Veritas 客户



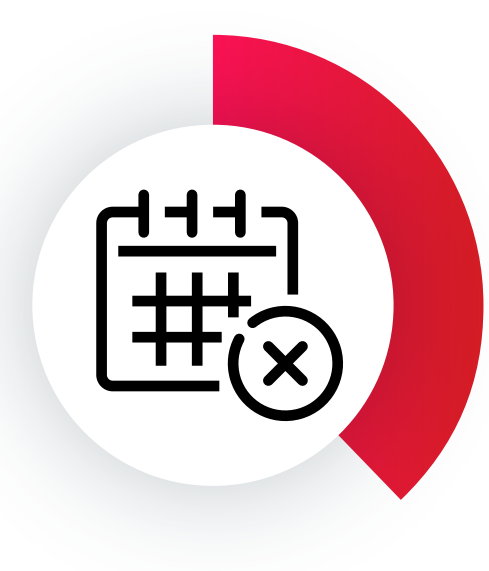
64%

的 IT 高管表示，安全措施无法应对当下复杂的 IT 环境。<sup>2</sup>



66%

的高管表示未采用 3-2-1 备份流程。<sup>2</sup>



38%

的 IT 高管表示，他们在遭到攻击后通常要停机 5 天以上。<sup>2</sup>

## 勒索软件攻击是头号挑战

勒索软件与应对韧性之间的差距越来越大。

96%+

的业务负责人将勒索软件列为重大威胁。<sup>2</sup>

是的，团队没有步调一致

公司高管与公司 IT 团队没有就勒索软件应对准备达成共识，而且差距巨大。

25%+

的企业称不止一次经历过勒索软件攻击。<sup>2</sup>

无论在哪里，无一幸免。

研究表明，勒索软件攻击遍及所有的基础架构，包括云平台。

1. <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/>  
2. [https://www.veritas.com/content/dam/Veritas/docs/ebook/V11117\\_GA\\_EB\\_2020-ransomware-resiliency-report\\_EN.pdf](https://www.veritas.com/content/dam/Veritas/docs/ebook/V11117_GA_EB_2020-ransomware-resiliency-report_EN.pdf)

以十足韧性对抗勒索软件 >