OROCK RANSOMWARE RESCUE AS A SERVICE

BATTLE CARD | INTERNAL USE ONLY

OROCK TECHNOLOGIES

Powered By HPE GreenLake

ELEVATOR PITCH

"Ransomware Rescue as a Service provides the necessary backups, data, and services so organizations can quickly and successfully recover from an attack with greater confidence and less downtime.

This integrated solution reduces the complexity of ransomware production by incorporating a secure hybrid connection, on-premises hardware, compliant off-prem cloud storage, and managed services delivered by highly-trained specialists."

END CUSTOMER BENEFITS AND VALUE PROPOSITION

- Customized solution that integrates into customer's existing IT on-prem infrastructure
- Reduces complexity of deploying and maintaining stand-alone systems and processes
- Installed and managed by experienced cloud, storage, and cybersecurity experts to complement or extend in-house expertise
- Developed with the latest HPE Gen10 hardware, Aruba networking technology, and software designed for cybersecurity threats
- Allows organizations to maintain critical backups (on-premises and in a secure cloud)
- Built for secure, encrypted and preconfigured hybrid data transfer over the Internet or network connection
- Advanced hardware w/ backup and recovery apps enable continuous, automated backups
- Protects your productivity, revenue and reputation with off-network backups of critical organizational data

KEY DIFFERENTIATORS

- Integrated solution: hardware, software, and services tailored to customer's environment
- Predicable monthly OPEX billing
- Deployed and managed by industry experts
- Government-grade security and controls
- Protected "air gapped" backups in the cloud
- Geo-resiliency built into price
- Multi-tenant and dedicated environments

USE CASES

- **Implementing the 3,2,1 Rule**—Industry best practice for safeguarding critical data
- **Automating Backups**—Define types, frequency and backup workflows
- **Protection for Remote Locations**—Secure on-prem and off-prem cloud backups
- **Supplement In-House Talent**—Enhance existing storage and cybersecurity expertise
- **Low Tolerance for Business Disruption**—Minimize risk of business interruption or damage to business reputation
- **Potential to Reduce Cyber Insurance Costs**

PAIN POINTS & SOLUTIONS

Ransomware attacks can take down an organization's network and systems for days or weeks resulting in significant business disruption	• ORock's comprehensive solution recovers the necessary files and data that have been compromised. • The solution provides a best practices approach that security and storage experts suggest: the 3-2-1 Rule. It enables customers to store 3 copies of their on 2 types of storage media, with 1 copy in the cloud.
Establishing a back-up plan that meets stringent customer requirements for data security and compliance	• RRaaS enables backup and storage of data that is encrypted at rest, with capabilities to encrypt data in-flight. • Data stored in the ORockCloud is always encrypted. RRaaS data is maintained separately and is isolated from network access. This data is invisible and inaccessible to ransomware viruses.
Lack of in-house security and storage expertise to design, implement and manage ransomware solutions	• ORock and HPE collaborate to deliver solutions that takes the customer's unique capabilities into consideration. RRaaS provides hardware, software and professional services which integrate into existing environments. • The solution enables customers to deploy and manage a comprehensive solution while limiting complexity and risk.

OROCK RANSOMWARE RESCUE AS A SERVICE

BATTLE CARD | INTERNAL USE ONLY

OROCK TECHNOLOGIES

Powered By HPE GreenLake

COMPETITORS

Public Cloud Service Providers

- Offer unmanaged backup and recovery services
- High cost of data egress if data recovery to the premises is required
- Vendor lock-in (too expensive to remove data)
- Complex billing plans

Ransomware Removal Services

- Solutions based on breaking ransomware encryption with decryption keys
- Tools unlock only previously decrypted ransomware infections
- Not 100% reliable as new and more advanced viruses are introduced

Disaster Recovery as a Service (DRaaS) Plans

- Lack of consolidated on-prem and off-prem integration capabilities
- Often don't leverage government-grade secure cloud data centers

CONTACT

Mario Guariello
VP Enterprise Sales, Storage Solutions
Email: mguarriello@OROCKTech.com
Direct: 610.762.6328

HPE PARTNER

Hewlett Packard Enterprise

HPE GreenLake

Hewlett Packard Enterprise — Solution Provider — BUSINESS PARTNER

QUALIFYING QUESTIONS

- How is your organization handling its ransomware protection strategy today?
- Is a comprehensive backup and recovery strategy a core component of your overall plan?
- What would you change about your current ransomware protection strategy?
- What is your confidence level in your ability to recover quickly from an attack?
- Does your organization have a defined and proven rescue plan in the event of a ransomware attack?
- Does your plan include a hybrid on-prem and off-prem cloud strategy?
- Do you have your critical backups "air gapped" so that ransomware can't find them and corrupt them?
- Has your company recently conducted a ransomware strategy assessment to determine:
  - What critical data must be backed up?
  - Where your data is backed up?
  - Adherence to the 3,2,1 rule?
  - How secure your data is and who has access to it?
  - If you are leveraging the latest backup and recovery technologies and processes?
- Are you looking to complement your existing backup and recovery infrastructure to gain greater performance and cost efficiencies?
- Does your organization understand:
  - The impact and potential damage and cost to your organization's reputation and lost revenue?
  - The operations and employee productivity impact that are likely to result from an attack?

OBJECTION HANDLING

I manage my own backups. How will RRaaS help me?

- Many organizations lack visibility into data protection gaps, backup schedules, and backup system performance. ORock RRaaS addresses these concerns.
- ORock can help you overcome existing obstacles to cloud backups, including consolidation of on-prem, edge and cloud backups, as well as defending against increasing cybersecurity vulnerabilities.

I have an MSSP supporting my organization already.

- The RRaaS solution offers additional capabilities which are often not included in traditional MSSP services.
- ORock and HPE will work side-by-side with MSSP partners to provide a deeper and more feature-rich set of IT and cybersecurity capabilities.

I have existing storage hardware and software in my infrastructure today. Do I need to replace it?

- In most cases, the RRaaS solution is architected to integrate, fill gaps, and provide additional functionality to your existing capabilities.
- Some organizations may need to upgrade existing infrastructure and leverage the latest generation hardware and software to enhance their ransomware recovery outcomes.

I've never heard of ORock.

- ORock is an HPE Business Partner and a Red Hat Certified Cloud and Service Provider.
- ORock was named the 2018 Red Hat Leading Edge Partner of the Year.
- ORock has primarily focused on doing business with the Federal government and Department of Defense. They are now offering the same government-grade solutions to commercial organizations. You can find them listed on the Federal government's FedRAMP Marketplace of approved cloud service providers.