Cybercriminals have refined their attack strategies and are now targeting data protection environments. To stay ahead of the last attacker, consider incorporating these nine data protection trends we’re seeing across modern data protection environments.

**The lifecycle of a cyberattack**

Before you can effectively prevent a breach, it’s important to understand the lifecycle of a cyberattack.

1. **Preparation:** The cybercriminals gather information about your organization, identifying potential entry points and vulnerabilities.
2. **Execution:** Using the gathered information, the cybercriminals launch an attack, exploiting vulnerabilities in your systems to gain access.
3. **Maintenance:** Once access is gained, the cybercriminals establish a foothold and begin to exfiltrate sensitive data.
4. **Exfiltration:** The attacker moves the stolen data out of your environment, often to an offshore location.
5. **Command & control:** The cybercriminals use the stolen data to control and direct further attacks, often launching additional attacks to spread the compromise.
6. **Lateral compromise:** The attacker uses the compromised device to gain further access to the environment and spread the compromise.
7. **Exfiltration:** The attacker exfiltrates additional data from the environment.
8. **Command & control:** The attacker uses the stolen data to control and direct further attacks, often launching additional attacks to spread the compromise.
9. **Persistence:** The attacker establishes a foothold and begins to exfiltrate sensitive data.

**9 trends in modern data protection**

1. **Immutable storage:** Historically known as the “nuclear option,” immutability has become an essential component of modern data protection strategies. The attackers now have full access to sensitive data, intellectual property, or other mission-critical information about the environment.
2. **Air gap:** All-flash storage is growing in popularity due to its ability to maintain data security by isolating it from the rest of the network. The result? It’s completely impervious to ransomware attacks.
3. **Transformational architecture:** In today’s hybrid and multi-cloud environments, teams are ensuring they only work with top cloud providers.
4. **Asset visibility:** With access established, the cybercriminals attempt to compromise additional users and machines.
5. **Air gap:** As storage moves out of the traditional data center to the edge and into the hybrid cloud, teams are ensuring they only work with top cloud providers.
6. **Data discovery & classification:** Data discovery and classification, performed regularly, is the key to highly effective cloud data protection. You can’t protect what you don’t know exists. Data discovery and classification, performed regularly, is the key to highly effective cloud data protection. You can’t protect what you don’t know exists.
7. **Disaster recovery:** An essential component to any modern data protection strategy, disaster recovery provides a failsafe in the event of a catastrophic failure. All-flash storage is growing in popularity due to its ability to maintain data security by isolating it from the rest of the network. The result? It’s completely impervious to ransomware attacks.
8. **All-flash storage:** The attackers use the compromised device to gain further access to the environment and spread the compromise.
9. **Command & control:** The attackers use the stolen data to control and direct further attacks, often launching additional attacks to spread the compromise.

**Sources:**
- Long Live Tape — And Other Data Protection Trends for a New Threatscape — the”0n a unique environment.