# RAPID CYBERATTACK ASSESSMENT

Ransomware has become extremely lucrative for cybercriminals. The costs of Ransomware damage are predicted to hit $11.5B by 2019.[1] Paying a ransom to recover mission critical data is one aspect of cost, but there are other costs involved such as forensic investigation, downtime, lost productivity and reputational harm to name a few.

Rapid cyberattacks such as Ransomware are fast, automated, and disruptive. They spread through an enterprise in minutes, leveraging multiple traversal techniques (i.e., exploits, stolen privileged account credentials, impersonation), and it is almost impossible for an enterprise to respond effectively. The attacks are designed to deny access or destroy mission critical data and to be disruptive to the business and IT operations. They can cause significant downtime, lost productivity, and reputational harm.

Many enterprises, however, are behind the curve in protecting against, as well as remediating and recovering from rapid cyberattacks. This is mainly due to a poor understanding of how to assess their security posture against these types of attacks.

## RAPID CYBERATTACK ASSESSMENT

SoftwareONE's Rapid Cyberattack Assessment is designed to help enterprises understand their vulnerabilities to rapid and destructive cyberattacks and to provide recommendations on mitigating attacks. SoftwareONE consultants work with customers to assess how well protected the enterprise is from a cyberattack and evaluating mission critical assets on the risk of an attack. Key stakeholders will be interviewed to understand information security policies, procedure and practices.

**1. Scope** — Define project scope, understand business requirements & identify stakeholders

**2. Assess** — Run assessment tool, complete and review questionnaire with key stakeholders

**3. Analyze** — Analyze tool findings and responses to questionnaire, perform gap analysis and finalize roadmap

**4. Report** — Review and report on results of findings and help customers prioritize roadmap

At the completion of the assessment, SoftwareONE will provide a detailed roadmap, recommendations and best practices on how to successfully use Microsoft technologies to mitigate security threats that are associated with rapid cyberattacks.

1. Cybersecurity Ventures, November 2017

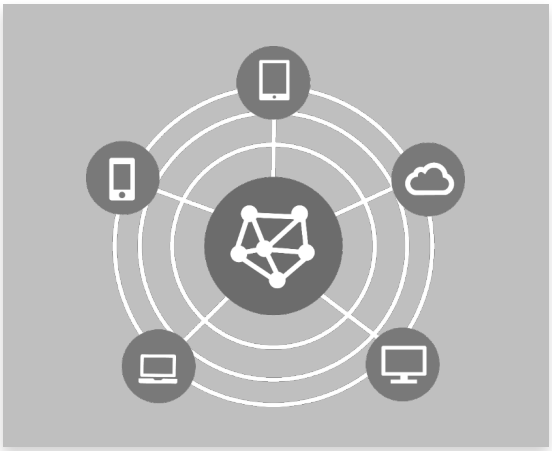


To learn more, visit us at:
**www.softwareone.com**

## CURRENT SITUATION

In a mobile-first, cloud-first world, the attack surface has expanded past the traditional IT perimeter and enterprises need to manage identities, protect devices, govern and manage Shadow IT, and make sure sensitive information is safeguarded.

SoftwareONE will help identify elements in the IT environment which are at high risk of a rapidly spreading and potentially destructive cyberattack. A short survey and technical assessment will be conducted by SoftwareONE security consultants to help enterprises understand their cyberattack vulnerabilities.



## TECHNICAL SECURITY READINESS

SoftwareONE will provide guidance, recommendations and best practices on how to successfully use Microsoft technologies to mitigate security threats associated with rapid cyberattacks. The prioritized recommendations are organized across 4 focus areas:

- Exploit Mitigation
- Business Continuity / Disaster Recovery (BC/DR)
- Lateral Traversal / Securing Privileged Access
- Attack Surface Reduction

## ROADMAP

A SoftwareONE actionable roadmap contains proposed actions to address discovered gaps, user impacts and implementation costs. The roadmap uses Microsoft technology capabilities and SoftwareONE managed services to close security and compliance gaps, based on each customer's objectives and requirements.

### INFORMATION PROTECTION

| | |
|---|---|
| **Office 365 DLP** | Protect sensitive data in Office 365 environments. |
| **Azure Information Protection** | Protect sensitive data in Azure environments. |

### IDENTITY AND ACCESS

| | |
|---|---|
| **Cloud Application Security** | Discover and extend enterprise-grade security to SaaS applications. |
| **Azure Active Directory (AAD)** | Manage identity from on-premises to cloud to protect application access from identity access. |
| **Microsoft Intune** | Manage access to corporate applications, data, resources from any device. |

### THREAT DETECTION & RESPONSE

| | |
|---|---|
| **Azure Advanced Threat Protection (ATP)** | Detect and protect against advanced targeted attacks and insider threats. |
| **Windows Defender ATP & Security Center** | Detect and protect Windows hosts against viruses, spyware and other malicious software. |
| **Office 365 Threat Intelligence + ATP** | Detect and protect against advanced threats in Office 365 environments. |



To learn more, visit us at:
**www.softwareone.com**

softwareONE