

# McAfee Incident Response Readiness Assessment Service

## Build your defenses for a cyberattack

What happens when a cyberattack occurs? Have you planned and prepared for one? McAfee® Incident Response (IR) Readiness Assessment Service can help you prepare. This service is an effective, structured approach that helps you prepare for and successfully manage a cyberattack.

### IR Readiness Can Help Mitigate the Impact of a Breach

Planning is one of the most important aspects of cybersecurity awareness and successfully overcoming breaches. It is not important to consider “if” a cyberattack will occur but “when” it will happen. You need to be prepared.

According to a Ponemon Institute report, preparedness and agility are by far the most important factors to achieving a high level of cyber resilience.<sup>1</sup>

In addition, companies need experienced cybersecurity professionals to aide in success. In a recent study by Frost & Sullivan, it was revealed that 66% of organizations lack the number of experienced cybersecurity professionals needed for today’s threat climate.<sup>2</sup>

Furthermore, companies that contained a breach in less than 30 days saved more than \$1 million versus those who took more than 30 days to resolve.<sup>3</sup>

Bottom line: The best way to counter the unpredictable and ever-present nature of cyberthreats is to be prepared.

### Wide-Ranging IR Assessment

The approach for the McAfee IR Readiness Assessment Service, a part of McAfee® Advanced Cyber Threat Services (McAfee ACTS) practice, involves a gap analysis evaluation of your processes, technologies, and internal capabilities. The McAfee IR Readiness Assessment Service is conducted by our experienced security consultants, who are product-agnostic.

This 40-hour service begins with pre-engagement planning through a kickoff call before the consultant comes on site to discuss basic engagement logistics.

During the onsite meetings, McAfee consultants work with you to identify and interview your security staff and then determine and define roles and responsibilities during an attack. We will also work with your team to help you identify threats and perform proper triage and mitigation, including remediation steps.

### Key Business Outcomes

- **Prepare for cyberattacks:** During the IR readiness assessment, McAfee security experts proactively work with your staff to review your current IR plan.
- **Reduce business disruptions:** With what you have learned during the assessment, you now have an up-to-date IR plan that helps you prepare for and recover from a cyberattack.
- **Improve ROI:** Throughout this process, our product-agnostic experts help you gain knowledge to leverage technology you already own.

### Connect With Us



## DATA SHEET

Next, we will evaluate how to maximize your current tool set during an attack. Then our team will work with you to identify other departments/disciplines in your organization that complement and influence your program, such as your security operations center (SOC), threat intelligence, threat hunting, and more. We will also collect and review documentation to baseline your practices against industry best practices.

Following the week-long assessment, the McAfee team will help ensure that the documentation is current to industry best practices. They will provide a functional program and heightened response capability report, along with an outline of their observations, recommendations, and a roadmap that is tailored to meet your specific needs.

### Prepare for Cyberattacks, Reduce Business Disruptions, and Improve ROI of Your Solutions

By partnering with McAfee, you will receive valuable insights that provide guidance on how to effectively handle a cyberattack.

Whether it is malware, ransomware, or a distributed denial-of-service (DDoS) attack, we identify areas of your business that are most at risk and offer advice on how you can help mitigate the damage after a breach.

To make your IR strategy and emergency response purpose-built, we help you leverage the technology you already own. The McAfee IR Readiness Assessment

Service will test your current state of readiness and preparedness for an incident, review the gaps, and provide recommendations on how to become more proactive rather than reactive. This improves the ROI of your solutions—and, by improving them, you can reduce the cost of a cyberattack.

### The Four-Step IR Readiness Assessment Service Methodology

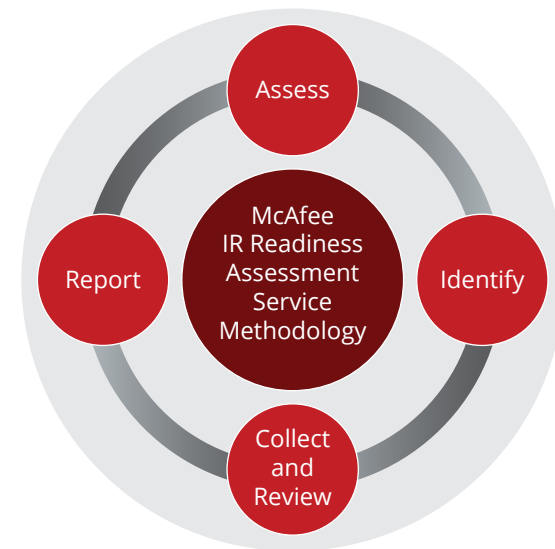
During this engagement, our domain experts use a defined methodology that consists of a consistent, repeatable process. We identify and interview key players and determine and define their roles and responsibilities before and during an attack.

**Step 1. Assess:** Evaluate how to maximize your current tool set during an attack.

**Step 2. Identify:** Specify other departments/disciplines in your organization that complement/influence your program (SOC, threat intelligence, threat hunting, and more).

**Step 3. Collect and Review:** Provide documentation that baselines your processes against industry best practices and guidelines.

**Step 4. Report:** Present the findings to you.



## DATA SHEET

### About this Service

The IR Response Readiness Assessment Service is part of the McAfee® Advanced Cyber Threat Services (McAfee ACTS) practice in the McAfee® Consulting Services portfolio. It is delivered by experts in the McAfee® Customer Success Group (McAfee CSG).

### The McAfee ACTS Difference

McAfee domain experts work collaboratively to assess, report, remediate, and continually improve security across all industry sectors globally. Security certified in almost 20 areas, including CISSP, CEH, CISM, GCIH, GREM and GIAC, we serve as your trusted partner to help resolve your challenges quickly, efficiently, and cost-effectively.

Our robust mix of strategic consulting and technical assessment services offers a unique approach to enhance people, process, and technology across any organization. By engaging with us, you can expect:

- **Confidentiality:** We have a proven track record with our clients and colleagues for retaining the privacy of incidents, as outlined in the statement of work.
- **Experience:** We have collective decades of experience in conquering the most complex breaches, managing risks, preventing attacks, and building successful security programs using industry best practices and guidelines.
- **Education:** We provide advice on how to make it all work—ensuring the right processes and procedures are in place and the most effective tools are used.
- **Proven methodology:** We use a proven Security Engagement Process (SEP) for project management to deliver successful consulting engagements.

### Key Deliverables

- Presentation and discussion of program and expected outcome
- Interviews with key players and stakeholders
- Review of current IR plan
- Understanding of product integration into the IR plan
- Report, including findings and recommendations, IR playbook, and a roadmap

## DATA SHEET

### About McAfee Customer Success Group

McAfee CSG uniquely brings together support, consulting, education, and customer success as “one team” to help you achieve successful business outcomes in all security lifecycle stages.

Our mission is simple: McAfee is committed to help you successfully deploy, adopt, consume, and realize the value of your McAfee solutions and achieve a stronger security posture.

From onsite incident response assistance, deployment services, and proactive success management to training, self-help resources, and communities, we deliver the people, processes, and tools through our comprehensive McAfee Cybersecurity Services portfolio.

### Learn More

Whether you need a first responder to help you quickly identify and remediate a breach, or a trusted partner to deliver independent, strategic security guidance, you can rely on McAfee ACTS. To learn more, visit [McAfee Consulting Services](#), or contact your sales account manager or partner.



1. [Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT](#) (Ponemon)
2. [2017 Global Information Security Workforce Study—ISC2](#) (Frost & Sullivan)
3. [Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT](#) (Ponemon)

McAfee does not control or audit third-party benchmark data or the websites referenced in this document. You should visit the referenced website and confirm whether referenced data is accurate.



2821 Mission College Blvd.  
Santa Clara, CA 95054  
888.847.8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2019 McAfee, LLC. 4365\_1119  
NOVEMBER 2019