

Ransomware Readiness **ASSESSMENT**

We help companies protect, prepare for, defend against, and recover from successful ransomware cyber-attacks by providing the visibility they need to identify and mitigate their risks to become Ransomware Ready.

JUNE 2020

Prepared for
ACME CORPORATION

OnDefend Cyber Security
4215 Southpoint Blvd, Suite 260
Jacksonville, FL 32216

1-800-214-2107
contact@ondefend.com
www.ondefend.com



Table of CONTENTS

EXECUTIVE SUMMARY	3
Your Current Ransomware Readiness Status	3
How You Compare	5
Your Current Financial, Legal & Reputation Risk	5
FINDINGS & RECOMMENDATIONS	7
Employee Awareness & Defense	7
Vulnerability & Asset Management	10
Technical Controls	12
GET RANSOMWARE READY	16
SOLUTION OVERVIEW	19
ABOUT ONDEFEND	22
ADDITIONAL ONDEFEND SECURITY SERVICES	23

Confidential – ACME Corporation

Notice: Being 100% Ransomware Ready means that your organization is prepared to defend from, respond to, and recover from a ransomware attack. I.e., We cannot guarantee that your organization will not fall victim to an attack due to employee error, identified vulnerabilities not being remediated, response and recovery plans not being regularly testing as well as other risks not being mitigated per our Ransomware Readiness Recommendations & Solutions.

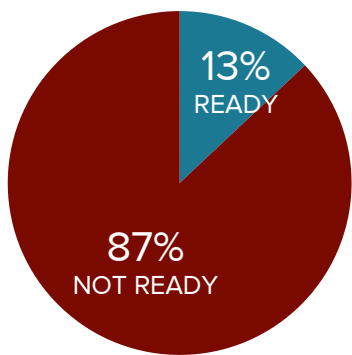






Executive SUMMARY

Thank you for engaging our Ransomware Readiness Assessment! This report will provide you with the guidance you need to **Prepare For, Defend Against**, and **Recover From** real-world ransomware attacks.

Your Current Ransomware Readiness Status

Readiness by Category



Ransomware Readiness Safeguard	Safeguard Tools & Controls	Current Status
 Employee Awareness & Defense	Attack Simulation Testing & Training	NOT READY
	Ransomware Identification	NOT READY
	Sender Identity Confirmation	NOT READY
 Vulnerability & Asset Management	Vulnerability Management	NOT READY
	IT Asset Management	NOT READY
 Technical Controls	Perimeter & Endpoints (Basic Protection)	✓ READY
	Backup & Recovery	NOT READY
 Response & Recovery Capability	Cyber Insurance	✓ READY
	Incident Response Plan	NOT READY
	Tabletop Exercises	NOT READY

Based on this assessment, your organization is **NOT** ready for a real-world ransomware attack.

A cyber adversary could use the risks in your organization that we have identified to breach your lines of defense, encrypt your data, and lock your organization out of day-to-day operations.

Your ransomware readiness status is based on the following **Four Ransomware Readiness Safeguards** that you must have in place to **Defend Against** and **Recover From** a real-world ransomware attack.

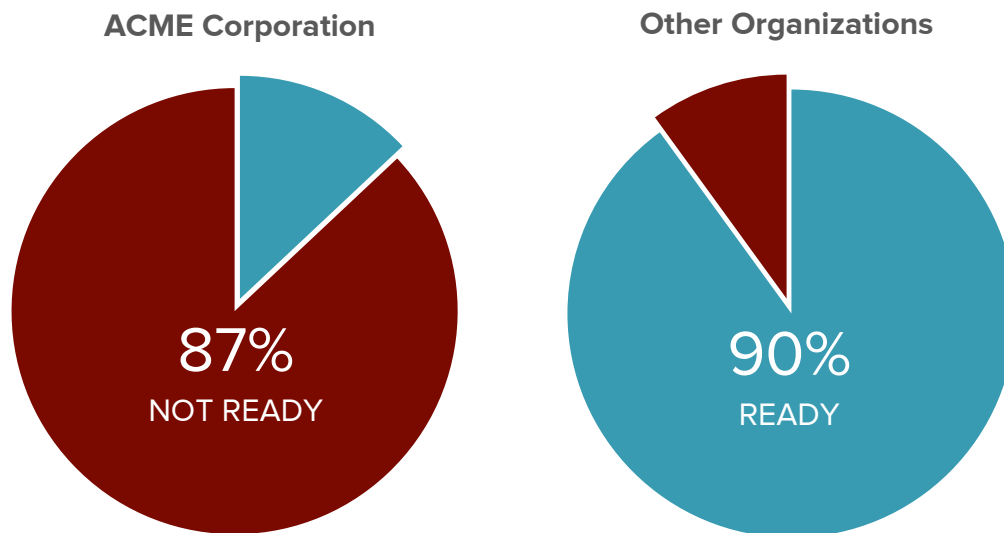
These categories represent each of your lines of defense against real-world ransomware attacks.



See the **Findings and Recommendations** section to learn more about these risks and reduction strategies to become Ransomware Ready.

How You Compare

The following Ransomware Readiness comparison shows the current status of your organization versus similar organizations across the United States.



Note: "Other Organizations" represent companies, municipalities, and other organizations in the U.S. that have also participated in this type of assessment or have provided information through various information-gathering interviews. Their Ransomware Readiness status is based on where each organization stands today, having become Ransomware Ready by following and implementing some or all of our recommendations.

Your Current Financial, Legal & Reputation Risk

If your organization falls victim to a ransomware attack, it would currently cost your organization a minimum of **\$850,000.**

Remember, being 100% Ransomware Ready is about Preparing For, Defending Against, and Recovering From real-world ransomware attacks.

Below is a breakdown of your current **financial, legal & reputation** risks:

Proven Financial Losses



Recovery Costs

Option A: Pay Ransom: National Average: **\$338,700** per attack.

The ransom amount is typically tied to the size and annual revenue of the victim organization.

Options B: Restore from Backups: If you have backed your data up, there are costs associated with the duration and efforts required to restore from backup. Many organizations have off-site backups, which further increase the time of recovery. Recovery can take hours to days, and in some cases, weeks. If backups are corrupted or incomplete, the restoration time and cost will significantly increase.



Downtime Losses

National Average: **\$250,000** per attack.

Whether you pay the ransom or restore from backups, your organization will face downtime whereby day-to-day operations will be considerably restricted, if not completely shut down. The **average business downtime is nine days** after a ransomware breach, which includes lost productivity, lost revenue, and other various factors.



Cyber Insurance

Even if you have cyber insurance, there may be limitations on your policy that may not cover some of the recovery and/or downtime costs noted above. Additionally, there will be costs associated with submitting your insurance claim, including your **deductible fee**, as well as **increased future premiums**.

Additional Risks



Legal Risk

After organizations are breached by ransomware, affected customers often resort to legal means for compensation, alleging privacy violations, negligence, and service disruption. Additionally, the data that was encrypted is sometimes exfiltrated and sold on the dark web, regardless if the victim paid the ransom, which also has long-term legal ramifications. **These legal ramifications could add to the ransomware attack costs noted above.**



Brand Damage

A **loss of confidence in your security** and its effect on your brand can be incalculable. The outcome of this damage typically results in some form of an **organizational/managerial overhaul** in an attempt to regain consumer trust.

All of these risks can be substantially reduced and continuously managed by becoming Ransomware Ready!



Learn more in the **Findings & Recommendations** section. Additionally, see the **Get Ransomware Ready** section at the end of this report to see how we can help get you Ransomware Ready and stay that way throughout the year.



Findings & RECOMMENDATIONS

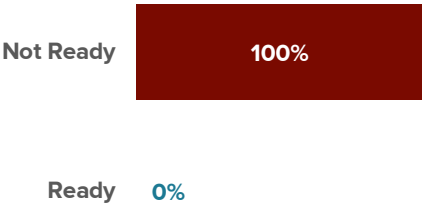
Your organization must have **Four Ransomware Readiness Safeguards** in place to **Defend Against** and **Recover From** a real-world ransomware attack. These safeguards were assessed, and the following pages include our findings and recommendations to become **Ransomware Ready**.



SECTION 1 Employee Awareness & Defense



Your Category Readiness



High-Level Findings

OnDefend executed two phishing email campaigns where employees provided credentials that could be used to access critical applications such as HR platforms.

OnDefend successfully executed a ransomware (simulation) inside the organization, proving that file shares, files, and folders can be encrypted and/or destroyed.

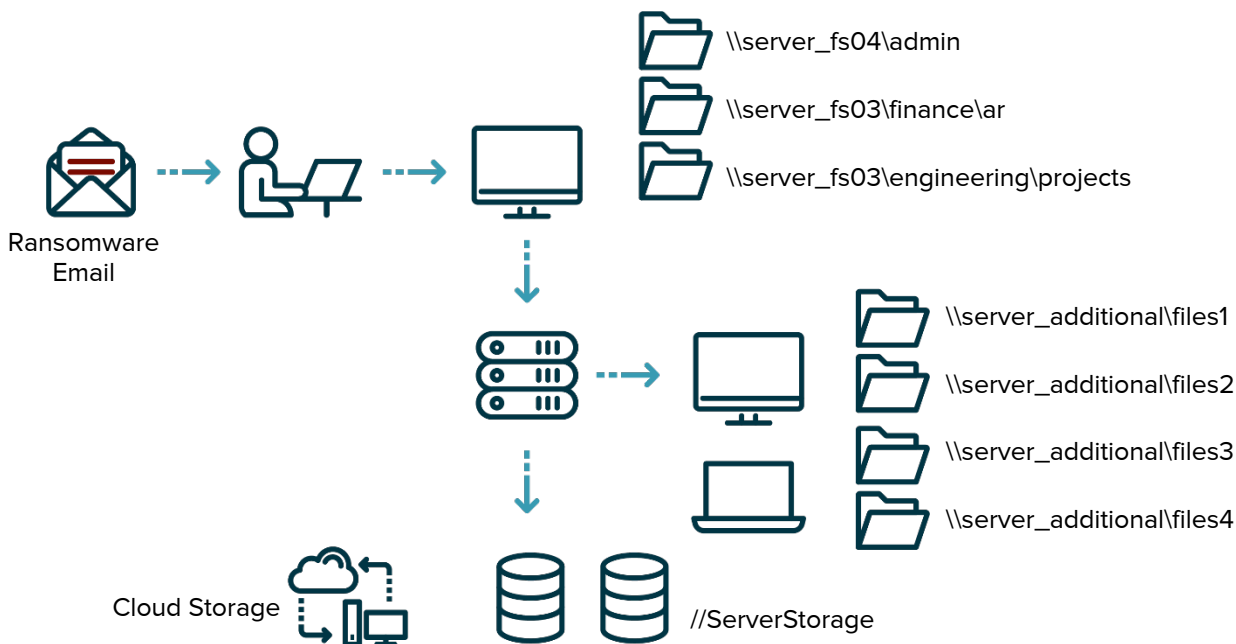
Why We Assess This Safeguard

Your employees are your **first line of defense** after malicious emails are delivered to their inboxes and are often referred to as your **“human firewall.”** Ransomware attacks target employees through advanced phishing emails that have downloadable executable files, links, and other malicious payloads. These phishing attacks are often disguised as regular business emails, otherwise known as a **Business Email Compromise** attack, which are extremely difficult for employees to identify. The goal is to arm your employees with the ability to **identify these suspicious emails** and **confirm they are safe** before interacting with them.

Our Findings

LOW RISK (Emails Unopened)	MEDIUM RISK (Emails Opened)	HIGH RISK (Clicked Link)	CRITICAL RISK (Submitted Login Info)	CRITICAL RISK (Executed Ransomware)
600	137	43	31	6

ONE employee fell victim to this ransomware attack simulation by opening, interacting with, or downloading the simulated dangerous payloads within these emails. If this were an actual ransomware attack, the following files and data would likely have been encrypted and held for ransom. Ransomware spreads quickly, and with a successful attack, many other systems fall victim. Ultimately it will work its way through the organization until it everything it can access is encrypted, including any connected cloud systems/storage.



Remember, it only takes **ONE** employee to fall victim to lock your organization out of business.

Additionally, we found that **31** of your employees provided credentials to one or more critical systems in your organization. This would have allowed a real attacker to gain access and those systems, which can allow **for stolen personal data, fraudulent transactions, and possibly a denial of service.**

Additionally, the 31 credentials harvested by the attack can lead to further system and network intelligence where additional servers, file shares, and other systems can be held ransom, manipulated, or destroyed.

How to Become Ransomware Ready

Your employees need to be aware of these types of attacks by learning how to identify them before falling victim. Additionally, when your employees suspect an email may be a cyber-attack, they need to confirm that the email is safe before interacting with it. We suggest the following measures to become Ransomware Ready:

Monthly Attack Simulation Testing & Training

Advanced phishing testing, similar to what was provided during this assessment, along with awareness training for those employees who fall victim to these tests, is an effective way to change employee behavior into a defensive posture when interacting with emails. This type of testing and training should be provided to your employees monthly.

Ransomware Identification

One of the best ways for employees to avoid these types of attacks is to provide technology within your email platform that identifies the attack and alerts them to it. Email filters offer this type of capability and are one of our recommendations in the Technical Controls section. However, unfortunately, they do not identify all ransomware emails. Sometimes the downloadable file does not have malware, but when the macro in the file is clicked, the ransomware is delivered. Phishing emails may also have links to access downloadable files with ransomware, which is impossible for the email filter to identify.

Email Sender Confirmation

If your employees suspect an email is a cyber-attack, or if you have technology that alerts them to suspicious emails, they should confirm the identity of the email sender to verify that the email is legitimate and safe. This practice should be accomplished through policy or technology. Note: Outside of ransomware attacks, many business email compromise attacks (which look almost identical to normal business emails) attempt to harvest credentials as well as other malicious activities. These emails also need to be confirmed in real-time.

We suggest you provide these tools to your employees so they can protect your organization as the first line of defense against ransomware and other types of cyber-attacks.



See the **Get Ransomware Ready** section to learn how we can help you lower this risk and become Ransomware Ready.



SECTION 2

Vulnerability & Asset Management



Your Category Readiness

Not Ready

100%

Ready 0%

High-Level Findings

Our Vulnerability Assessment found **20 CRITICAL** and **34 HIGH** risk vulnerabilities in the infrastructure. Additionally, a ransomware (simulation) was able to execute successfully without detection.

Why We Assess This Safeguard

If your employees do fall victim to a ransomware phishing attack, your second line of defense is the security of your network infrastructures, servers, and application. Your infrastructure is made up of technical controls, servers, applications, and devices that regularly require security updates such as software upgrades, security patches, configuration updates, and more. If these security updates are not identified and applied within days of their release, and continually, they will likely be exploited by ransomware or other forms of cyber-attack.

Our Findings

Vulnerability Testing Results

LOW RISK	MEDIUM RISK	HIGH RISK	CRITICAL RISK
14	115	34	20

We detected **183** findings during this vulnerability test. These vulnerabilities can be exploited to execute ransomware, steal information, control your devices, and spread other malicious malware throughout your network, eventually encrypting or exfiltrating your data and severely affecting the ability to perform continued operations.

See details at the VManage Results & Remediation Portal: <https://vmanage.ondefend.com/client/1592/reports>

How to Become Ransomware Ready

Your organization must regularly identify and apply security updates to your network, servers, and applications. We suggest the following measures are taken to become Ransomware Ready:

Vulnerability Management

Vulnerability management is the process of identifying vulnerabilities and remediating them on a recurring and continual basis. To do this, you must use a professional cybersecurity solution that will identify your vulnerabilities on a monthly basis and provide remediation recommendations. However, if these vulnerabilities are not managed and remediated in real-time, you will not decrease your risk.

IT Asset Inventory

IT asset inventory is the process by which you identify all assets on your network infrastructure, including network devices, servers, workstations, and other computing platforms. These assets can be utilized by cyber adversaries; if you don't know what's on your network, you cannot secure it.

We suggest you evaluate your network vulnerabilities and assets every month and remove these risks before they can be exploited by ransomware or other types of cyber-attack.



See the **Get Ransomware Ready** section to learn how we can help you lower this risk and become Ransomware Ready.

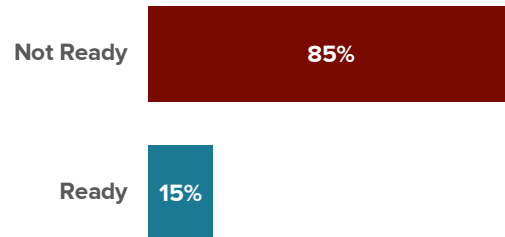


SECTION 3

Technical Controls



Your Category Readiness



High-Level Findings

The organization has deployed a Firewall and Basic Anti-Virus software on all devices. However, phishing emails still bypassed the standard controls, and SPAM filter(s), credentials were harvested, and ransomware was able to execute without detection. With no multi-factor authentication in place, OnDefend gained access to critical organizational systems.

Why We Assess This Safeguard

If a ransomware attack spreads throughout your network infrastructure, your third line of defense is the technical controls that should be in place to mitigate such a spread. Technical controls represent the makeup and layout of your IT infrastructure, including your network, systems, software, tools, and more.

Our Findings

OnDefend successfully gathered credentials and successfully executed a malicious attachment starting with the ransomware simulation. The current email defenses and SPAM filters were bypassed, and all attack emails were delivered to the end-user's email inbox.

With no multi-factor authentication in place, OnDefend gained access to critical organizational systems.

Additionally, your organization has a once-a-day backup routine, causing a potential data loss scenario where same-day information cannot be recovered. Workstations are not part of the backup routines, which will significantly increase the recovery time if all machines must be reinstalled without imaging technology.

How to Become Ransomware Ready

Add additional layers of security such as multi-factor authentication, email confirmation technologies, and more advanced email SPAM solutions.

Critical system and application backups should be executed multiple times a day or continuously to avoid data loss. Restoration of workstations that fall victim to ransomware is time-consuming. We recommend deploying a workstation backup and imaging solution to reduce the impact of a ransomware/malware outbreak.

We suggest you implement these findings so that this line of defense is fully successful before an attack, which will help mitigate the damage.



See the [Get Ransomware Ready](#) section to learn how we can help you lower this risk and become Ransomware Ready.



SECTION 4 Response & Recovery Capability



Your Category Readiness

Not Ready

75%

Ready

25%

High-Level Findings

The organization has a Cyber Insurance Policy. However, there is no comprehensive and detailed Response & Recovery program.

A basic Incident Response Plan exists, but it lacks critical details.

The organization does not perform recurring incident simulations to test the organization's capability to respond and recover.

Why We Assess This Safeguard

If a ransomware attack does penetrate the previously mentioned lines of defense, your last line of defense is your level of preparation to respond and recover from this event. Without a proper Response & Recovery Program, your organization will not be able to quickly and effectively mitigate the attack, decide whether or not to pay the ransom demand, restore services and processes, manage the legal outfall, and handle public relations. Additionally, you need the capability to back up your information and restore your data in real-time.

Our Findings

You have an incident response plan, but this plan lacks critical details required to respond and recover from a successful ransomware attack appropriately.

The current plan lacks detail in the following categories:

- Roles and responsibilities and contact information
- Executive and legal incident response team
- Security incident response team
- Reporting of security incidents, including PR
- Responding to security incidents by severity
- Related laws, regulations, or policies

How to Become Ransomware Ready

Your organization must have a comprehensive and current Response & Recovery Program that includes an Incident Response Plan that matches your organization's current employee stakeholders, technology stack, and overall environment, as well as regular testing of that plan to prove it will work.

We suggest you implement your Response & Recovery Program in case your other lines of defense fail so that you can recover efficiently and effectively.



See the [Get Ransomware Ready](#) section to learn how we can help you lower this risk and become Ransomware Ready.



Get Ransomware **READY**

Congratulations! Your organization has now gained visibility into your ransomware risks, and now you have guidance on the measures for your organization to become **100%** Ransomware Ready.

The recommendations in this report, which may appear daunting, can be successfully applied with the right attention, budget, and tools. The good news is that the tools and resources used to provide this assessment can be applied on a monthly basis to help your organization become Ransomware Ready today.

Your organization is currently **13% Ransomware Ready**. OnDefend can help you become Ransomware Ready by implementing the following solutions:



Employee Awareness &
Defense




Vulnerability & Asset
Management




Response &
Recovery Capability

Cyber Security Solutions by OnDefend

Ransomware Readiness Safeguard	Safeguard Tools & Controls	Current Status	OD Solutions	FINAL READINESS
 Employee Awareness & Defense	Attack Simulation Testing & Training	NOT READY	✓	✓ READY
	Ransomware Identification	NOT READY	✓	✓ READY
	Sender Identity Confirmation	NOT READY	✓	✓ READY
 Vulnerability & Asset Management	Vulnerability Management	NOT READY	✓	✓ READY
	IT Asset Management	NOT READY	✓	✓ READY
 Response & Recovery Capability	Cyber Insurance	✓ READY		✓ READY
	Incident Response Plan	NOT READY	✓	✓ READY
	Tabletop Exercises	NOT READY	✓	✓ READY
Cyber Security Solutions	READINESS	13%	+ 77%	= 90%

*For additional details on the solution view the Solutions Overview section.

Technical Control Solutions by Partners

Ransomware Readiness Safeguard	Safeguard Tools & Controls	Current Status	IT or Partners	FINAL READINESS
 Technical Controls	Perimeter & Endpoints	✓ READY	✓	✓ READY
	Advanced End-Point Protection	NOT READY	✓	✓ READY
	Backup & Recovery	NOT READY	✓	✓ READY
	Email SPAM Filter	NOT READY	✓	✓ READY
	Multi-Factor Authentication	NOT READY	✓	✓ READY
	Mobile Device Management	NOT READY	✓	✓ READY
	VDI Solution	NOT READY	✓	✓ READY
Technical Control Solutions	READINESS		10%	= 10%

Solutions Summary after Remediation

Cyber Security Solutions	OnDefend	90%
Technical Control Solutions	Partners	10%
	Total	100%

OnDefend Cyber Risk Protection Subscription: \$x,xxx/month

- ✓ Monthly Attack Simulation Testing and Training
- ✓ Confirm4Me Ransomware Identification & Sender Identity Confirmation
- ✓ Ongoing Network Vulnerability & IT Asset Inventory Management
- ✓ Incident Response Plan Development and Annual Tabletop Exercise
- ✓ Continuous Security Controls Validation
- ✓ Monthly Fractional Chief Information Security Officer

Your Return on Investment by solutions provided by OnDefend

- ✓ Annual Ransomware Readiness Investment = \$x,xxx.xx
- ✓ Annual Financial Risk = \$250,000
- ✓ Annual Potential Savings = \$xxx,xxx.xx

Return on Investment (ROI) = 825% every year!

*ROI is based on national averages

Solution

OVERVIEW

Employee Awareness & Defense

Monthly Attack Simulation Testing & Training

We will test your employees every month with email phishing simulations. If an employee falls victim to an attack simulation, they will be automatically directed to training, so they learn what to identify, avoid, and report. Our phishing simulations can also test other scenarios outside of ransomware, including credential harvesting, spear phishing, and different types of phishing attacks. All test results will be available via our VManage secure portal.

Confirm4Me - Ransomware Identification & Sender Identity Confirmation

Confirm4Me plugs into your email platform to identify and alert your employees to emails that appears to be ransomware attacks, including dangerous attachments, suspicious macros within those attachments, links that seem to lead to a ransomware attack, and more. Additionally, Confirm4Me provides your employees with a streamlined way to confirm the identity of the “sender” of internal emails within your organization.

Vulnerability & Asset Management

Monthly Vulnerability Testing with VManage

VManage is our professional, web-based platform that not only continuously tests your network for vulnerabilities and provides remediation recommendations but also gives you a way to manage and track these vulnerabilities being removed. Here, you can assign remediation tasks to your team, third-party providers, or our team if you need the assistance so that you can see your security posture in real-time. All test results will be available via our VManage secure portal.

Continuous Security Controls Validation

Continuous monitoring and validation of security solutions to constantly verify they are detecting attacks and alerting the defense team. This will alert the security team if any security control is not working as expected via misconfigurations, controls changes, and other external factors.

Response & Recovery Capability

Incident Response Plan Build and Management

We will assist you in developing a comprehensive Incident Response Plan or update a current plan that matches your organization's current employee stakeholders, technology stack, and overall environment. Additionally, we provide one annual tabletop exercise to simulate certain cyber-attacks and other disruptive events to prove your organization can respond and recover in real-time

Fractional Chief Information Security Officer

Fractional information security leadership that helps a company manage and mature their security program within their timeline and budget. For this instance, we will help the client implement all ransomware readiness recommendations, as well as build the overall security program.

Technical Controls

Annual Technical Controls Assessment

If you need assistance with implementing certain technical controls, we can provide this service, which will be billed separately from the subscription for hours worked.



THANK YOU!

Thank you for this testing opportunity, and please let us know if you have any questions.

We look forward to serving your future information security testing needs.

The mission at OnDefend is to provide its seasoned IT expertise and proven security methodologies to assist its corporate clients in reducing their exposed IT surface area while improving their overall security posture.

For more information about OnDefend, see below.



About ONDEFEND

We use and develop innovative, creative, and proven security solutions that improve our clients' overall security program, reduce their risks and liabilities, and defend against continually evolving and persistent cyber criminals and adversaries.

High Quality Service

Our security teams have seven years minimum applicable experience with a strong history of providing superior, premium, and reliable cyber security testing and consulting results and reporting.

Premium Results Reporting

All results and remediation reporting are provided in a professional, client-friendly, actionable, and easy-to-import formats. Reports include an Executive Summary to eliminate technical jargon and focus on decision making.

Remote & Fast Service

Our proprietary remote security assessment and testing processes provide efficient, affordable, and non-invasive security assessments and testing.

Advisory Expertise

Whether it's a security officer, compliance consultant, ethical-hacker, or cyber auditor, OnDefend has the service readily available at an affordable price.

Low-Touch Engagement

OnDefend prides itself on the ease and speed with which it can engage and deliver its testing and advisory services, which creates a headache-free, low-touch process for its clients' security management teams.



Additional OnDefend **SECURITY SERVICES**

Vulnerability Assessments

Identifies and quantifies assets within your IT environment that are vulnerable to cyber-attack.

Virtual Cyber Information Security Officer

Fractional cyber security consulting that helps your company affordably strengthen its security posture while moving up the information security maturity curve.

Network Penetration Testing

Simulation of an external and/or internal cyber-attack that attempts to prove and/or disprove whether a real-world attack would successfully exploit critical systems and gain access to your sensitive data.

Application Testing

Dynamic (app facing) or Static (code-based) tests that identify exploitable vulnerabilities within your web or mobile application that could provide unauthorized access to sensitive data or critical systems.

Email Attack Simulation (Phishing)

Simulates an email phishing scam attempting to engage your employees to attain sensitive information such as login credentials, network information, secure data, and account information.

PCI DSS Compliance Services

Consulting services to support your organization in achieving mandatory compliance with the PCI DSS, including required scanning, testing, and assessment guidance.