The Ransomware Survival Guide

Use Our Guide To Identify Prescriptive Recommendations For A Successful Ransomware Strategy

November 10, 2021

By Steve Turner, Allie Mellen with Stephanie Balaouras, Melissa Bongarzone, Alexis Bouffard, Peggy Dostie

Summary

Organizations have more tools, technologies, and processes at their disposal than they know what to do with to combat ransomware. This report helps security pros organize their ransomware strategy and execute by introducing a new survival guide with prescriptive, tactical recommendations on how to detect, prevent, respond to, and overall limit exposure to ransomware and other destructive attacks.

Additional resources are available in the online version of this report.

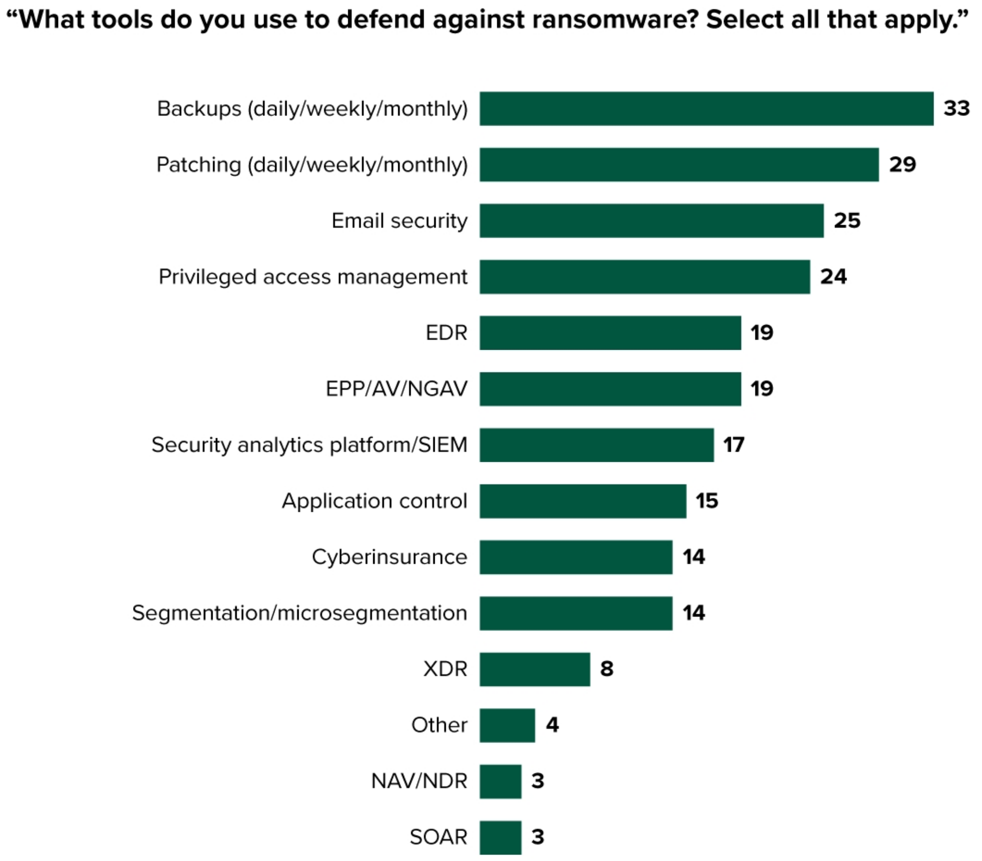
Ransomware Doesn’t Discriminate

There is a constant new stream of ransomware attacks, with thousands of victims in 2020 and even more in the first half of 2021. Ransomware actors don’t discriminate based on industry, organization size, customer base, or any other factors, as shown by the breadth of attacks targeting healthcare, manufacturing, financial services, and other organizations. As a result:

- **Security teams are anxious.** Security pros continue to struggle to prioritize the appropriate initiatives to combat ransomware, exemplified by an ad hoc survey we ran in May 2021. Over 90% of practitioner respondents are worried about ransomware despite having an established plan to mitigate it (see Figure 1).
- **There is no single source of truth for ransomware defense.** Frameworks and taskforces exist today to combat the ransomware threat, but they fail to provide a strategic way to organize ransomware defense and the prescriptive recommendations necessary to give actionable direction. In the same ad hoc survey we conducted of security practitioners, we asked what tools respondents use to defend against ransomware. Eighty percent of organizations selected “backups,” and, interestingly, 61% selected “email security.” There is no clear consensus as to what tool is the single most important when it comes to ransomware defense.

Figure 1

Ransomware Defense Doesn't Have A Consensus



Base: 41 security professionals

Source: Forrester's 2021 Ransomware Defense Survey

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

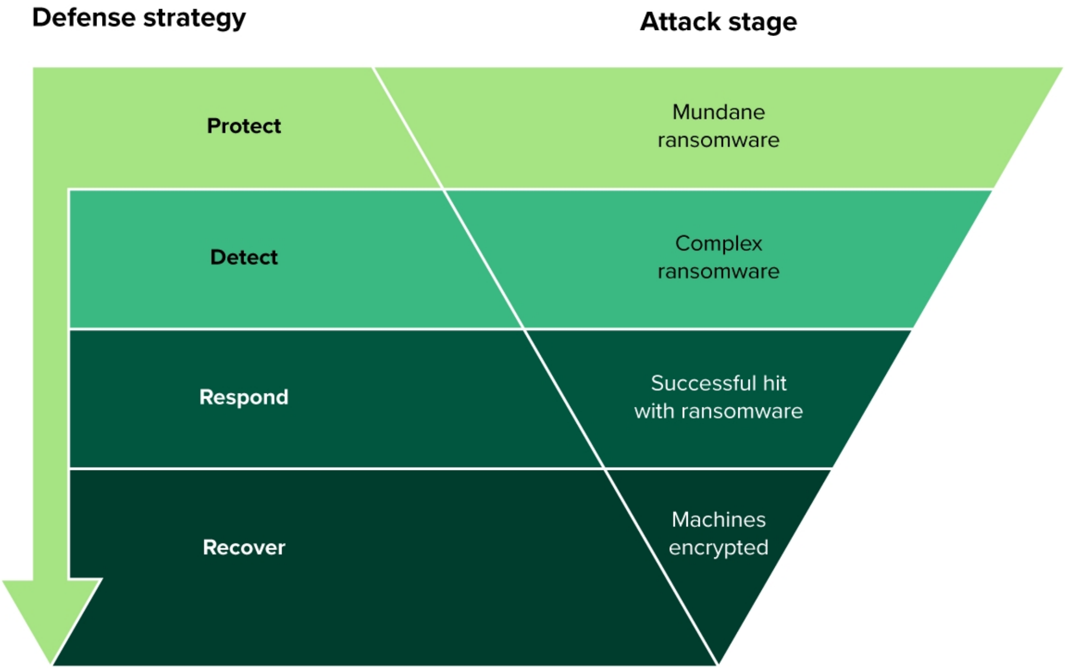
Use The Ransomware Survival Guide To Make Yourself The Difficult Target

Organizations have a fighting chance against ransomware if they get the right support to strategically prepare. There are steps you can take that aren't operationally challenging and that limit your attack surface by leaps and bounds, which we outline in tactical depth in the ransomware guide included with this research. The guide provides prescriptive recommendations organizations need to tailor their investments around their environment, so they can implement critical, achievable steps to defend against and survive a destructive attack like ransomware. The guide provides:

- **Practical steps to defend against destructive threats.** We've combed through a multitude of ransomware and other destructive attacks to find consistent attack patterns (see Figure 2). This research identifies key control categories and the associated steps that every organization must take to stop ransomware.
- **Prioritization combined with customizability.** Implementing security is hard. Prioritizing the implementation of different security controls is even harder. We designed this guide with different inputs specific to your organization, like ease of implementation, cost, impact to reducing threat, and others, so you can prioritize based on your environment and your resource constraints.
- **Direct guidance on which controls matter and how to implement them.** Top 10 lists of how to solve different security situations mean nothing without context and detailed guidance. The guide includes suggested configurations, resources, and assessment of potential operational impacts to help security pros implement these controls faster and more effectively.

Figure 2

Forrester's Framework For Aligning Ransomware Defenses To Attacks



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

The Maturity Stages Of Ransomware Defense

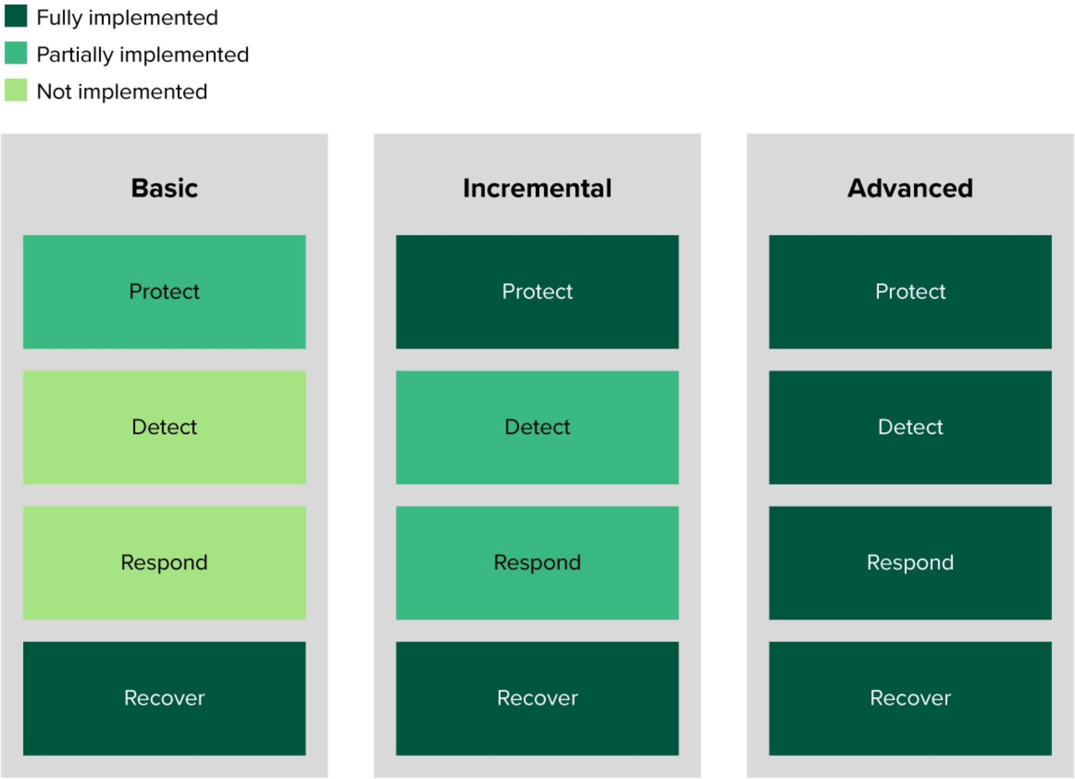
There are three stages of ransomware defense, classified by the maturity of the security program: basic, incremental, and advanced (see Figure 3). Each stage builds on the other to create a more robust ransomware defense. These stages are not a checkbox for total protection against ransomware, but require continual tuning, auditing, or other human intervention. They are steps organizations can take, depending on their resources and maturity, to prevent common and advanced attacks, limit any damage, respond completely, and recover quickly. For each stage, we list the top recommendations found on the interactive tool:

- **Basic stage.** The is the baseline of critical controls for a ransomware protection strategy; it encompasses recovery capabilities and basic protection.
- **Incremental stage.** This stage builds a more robust protection capability and initiates the detection and response journey.

- **Advanced stage.** The last stage outlines further protection and incident response processes to continue to strengthen the program.

Figure 3

Forrester's Ransomware Defense Maturity Stages



■ Fully implemented

▨ Partially implemented

□ Not implemented

Basic	Incremental	Advanced
▨ Protect	■ Protect	■ Protect
□ Detect	▨ Detect	■ Detect
□ Respond	▨ Respond	■ Respond
■ Recover	■ Recover	■ Recover

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Basic Stage: Recover And Baseline Protection

When it comes to the first stage of ransomware defense, the essentials are backups, configuration changes, and prevention. This stage is easiest to implement and requires the least number of resources: limited-to-no full-time security personnel, and periodic updates. It focuses on stopping the most common ransomware attacks and ensuring a successful recovery from backup for any attacks that get through. Our top recommendations are the bread and butter of ransomware defense (see Figure 4).

Figure 4

Top Recommendations To Basic Ransomware Defense

Category	Defense stage	Recommendation	Implementation priority
Endpoint	Basic	Secure RDP and other remote access configurations	Critical
Macro configurations	Basic	Restrict macros from executing when downloaded from the internet	Critical
Process	Basic	Establish an incident response plan	Critical
Identity	Basic	Implement multifactor authentication that's easy to use and ubiquitous	Critical
Process	Basic	Implement an offsite backup solution	Critical

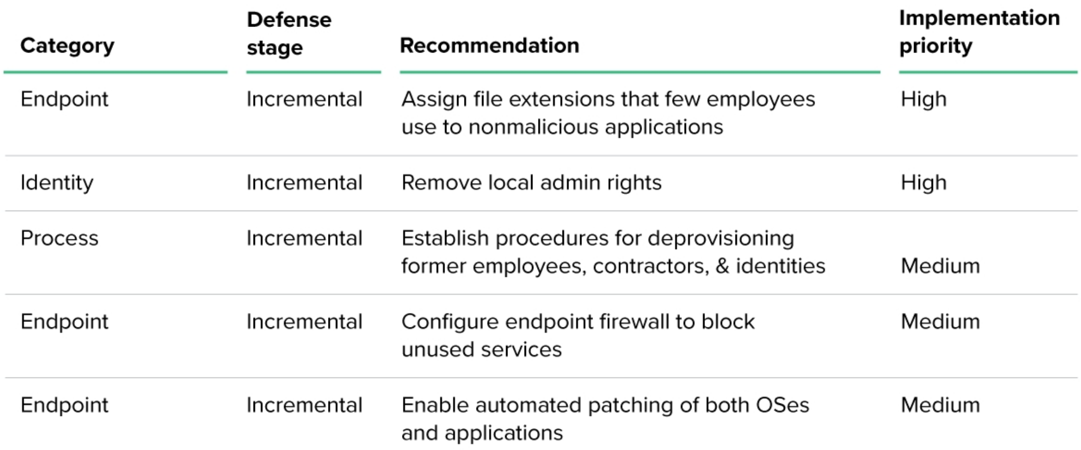
Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Incremental Stage: Protect And Detect

The incremental stage of ransomware defense focuses on improving protection capabilities with more robust configuration changes and control implementations, as well as beginning to address detection and response (see Figure 5). This stage requires more resources, including full-time security personnel, deeper budget, and strategic process improvements. It builds on the basic stage to stop common ransomware attacks, ensure a successful and secure recovery, and limit spread of ransomware; it introduces detection and response capabilities that allow analysts to investigate and respond to more advanced ransomware strains.

Figure 5

Top Recommendations To Incremental Ransomware Defense



Category	Defense stage	Recommendation	Implementation priority
Endpoint	Incremental	Assign file extensions that few employees use to nonmalicious applications	High
Identity	Incremental	Remove local admin rights	High
Process	Incremental	Establish procedures for deprovisioning former employees, contractors, & identities	Medium
Endpoint	Incremental	Configure endpoint firewall to block unused services	Medium
Endpoint	Incremental	Enable automated patching of both OSes and applications	Medium

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Advanced Stage: Enhanced Protection And Incident Response

The advanced stage of ransomware defense focuses on implementing more-sophisticated protection and incident response processes that will take continuous improvement. You should implement the recommendations in this stage in conjunction with a wider security strategy (see Figure 6). It requires the largest number of resources, including full-time security personnel and significant budget. It's the cream of the crop in ransomware defense and builds on the basic and incremental stages to address common ransomware attacks, ensure a successful and secure recovery, limit spread of ransomware, and empower incident responders against advanced ransomware strains.

Figure 6

Top Recommendations To Advanced Ransomware Defense

Category	Defense stage	Recommendation	Implementation priority
Endpoint	Advanced	Application control (allowlisting/denylisting)	Critical
Endpoint	Advanced	Disable legacy protocols (SMB v1/v2, TLS 1.0, 1.1,NTLMv1)	Medium
Network	Advanced	Restrict outgoing traffic from endpoints	Medium
Network	Advanced	Block outgoing traffic from critical devices	Medium
Endpoint	Advanced	Restrict employees from running Terminal, Command Prompt, PowerShell	Medium

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Ransomware Needn’t Be Your Organization’s Swan Song

Use the ransomware survival guide to identify where your current maturity sits around defending against, detecting, and recovering from ransomware and other destructive attacks. Use that information to elevate and evolve your capabilities and processes to address the gaps you’ve identified. In addition, we recommend that you:

- **Take immediate action on controls that are critical to stop the bleeding.** Controls that have a critical impact to reducing the threat should be the number one priority for your organization. These controls are your organization’s critical defensive shield against destructive attacks, and you must undertake them immediately, regardless of long-term strategy.
- **Use the guide to map out a short-, medium-, and long-term strategy.** Within the attached tool, columns “Cost,” “Ease of implementation,” and “Impact to reducing threat” are adjustable so you can fine-tune the guide to fit your enterprise approach. Map which actions are the most important based on your organizational needs, while considering the default values as our guidance and what makes sense for the average organization.
- **Make incremental improvements.** Build your capabilities incrementally and map them out in your security roadmap based on their implementation cost and other resource constraints. It will be easiest to start with configuration changes and

recommendations you can accomplish natively before looking to buy a new tool. Consider resource constraints beyond cost, including full-time employees and other factors.

- **Integrate your ransomware strategy.** Ransomware defense does not just stop ransomware. Integrate your ransomware strategy into the rest of your security strategy; the recommendations listed here will give you a fighting chance against a multitude of different destructive attacks.

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com