The Blueprint To Prevent, Detect & Beat Ransomware

Let's get started.

Navigate Your Content

See which chapters you are interested in.

Contents

59% of IT decision makers indicated their Firewall/VPN technologies need to be upgraded over the next two years.*

*IDG research commissioned by WEI, Jan 2021

The World Is At War With Ransomware

Fight with a grounded framework.

The world is at war with ransomware.

It is a threat that every business with a digital presence must contend with. As with any war, you must have a strategy to win. Still, it can be hard to understand how so many enterprises fall victim to ransomware attacks with all the money spent on cybersecurity over the past decade.

Truth is, you can have an entire arsenal of best-of-breed cybersecurity tools at your disposal and still fall victim to ransomware. Yes, having the right defensive tools is critical, but beating ransomware first requires a well-conceived multi-layer strategy based upon an established framework that is implemented by the proper mindset.

A Grounded Framework

There are several reputable and established frameworks out there that you can freely utilize. **At WEI, we like to suggest the NIST Cybersecurity Framework that touches on all the things you need to secure your organization.** The NIST framework is written in common language to bridge the technical gap between internal IT and business leadership.

NIST can be used to help educate stake holders from across the organization to understand, manage, and reduce cybersecurity risk.

What is your top IT objective?

- ○ Improve Data Security
- ○ Improve Operational, Process Efficiency
- ○ Improve Customer Experience

POST ANSWER

NIST Core Functions:

Identify: Assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities.

Protect: Outlines appropriate safeguards to ensure delivery of critical infrastructure services.

Detect: Defines the appropriate activities to identify the occurrence of a cybersecurity event.

Respond: Includes appropriate activities to take action regarding a detected cybersecurity incident.

Recover: Identifies activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a security incident.

Which Framework Tier Is Your Organization Operating From?

See where most enterprises stand.

Which Framework Tier Is Your Organization Operating From?

The objective is to reach Tier 3 or Tier 4.

The NIST Framework Tiers provide context into how an organization approaches cybersecurity when managing its risk exposure. Each tier describes the priority and effort allotted its cybersecurity risk management practices and how it deals with current threat environments and regulatory requirements.

The tiers represent a progression of mindset ranging from an informal reactive response to approaches that are agile, and risk informed.

See which tier your organization qualifies for!

Tiers 1 - 4

1 **Tier 1:** There is little semblance of a formalized approach to organizational cybersecurity management. Risk is managed in an ad hoc case by case basis. This mindset typically exemplifies a reactionary approach to risk, which stems from the limited awareness of cybersecurity risk at the organizational level.

2 **Tier 2:** Awareness of cybersecurity risk begins to be realized at the organizational level as well as the establishment of risk objectives to govern security initiatives. Management takes more of an active role in prioritized risk management efforts but initiatives lack an established organizational-wide policy. Cybersecurity information is shared on an informal basis.

3 **Tier 3:** A formal approach begins to take hold. Risk management practices are now expressed as established policies that follow an organizational approach. This tier is characterized by repeatable processes as policies are defined and regularly reviewed. Cybersecurity practices are regularly updated to address the inevitable changing threat and technology landscapes.

4 **Tier 4:** This is top of the summit from a risk management perspective. The organization rapidly adapts to new and evolving sophisticated threats, but leadership also fuses a relationship between cybersecurity risk and organizational objectives. A total proactive approach to cybersecurity permeates throughout the organization with user education being a priority.

Combat Risk: Use Multiple Security Layers

Identify, determine, and prioritize.

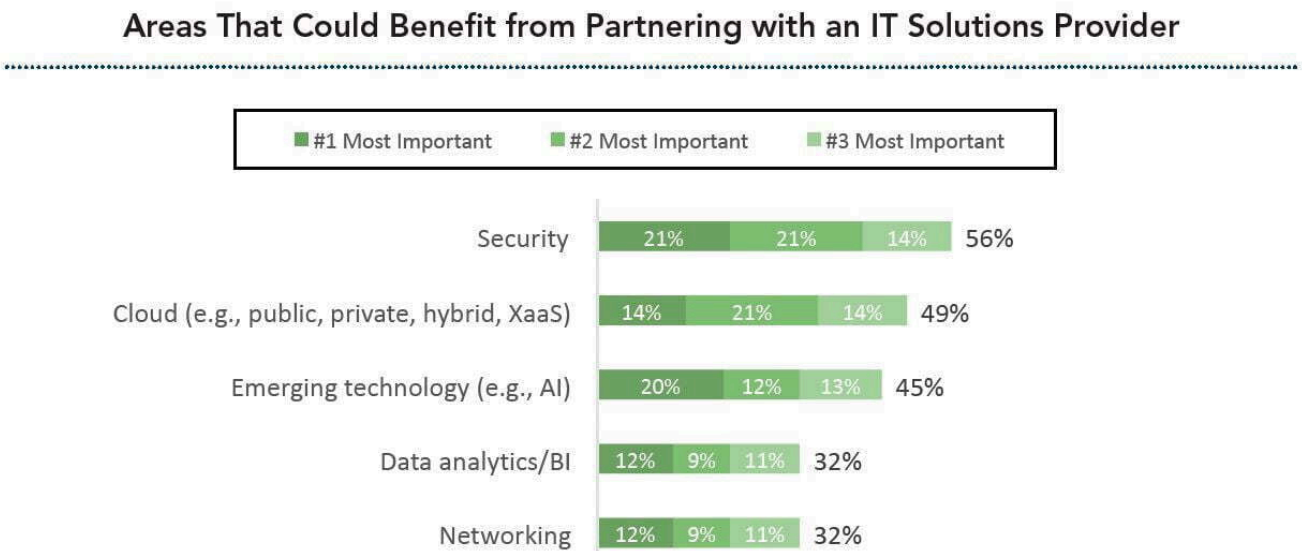
Organizations are exposed to cyberattacks.

That is the risk we take in a digitally connected world. Cybersecurity is all about the management and mitigation of risk. That starts with identifying where risks lie, determining which risks are worth accepting, and prioritizing the risks to mitigate.

Every enterprise is exposed to attack avenues.

The biggest avenue is your internet connection, but singularly focusing your efforts to defend this gate would be a mistake. There are many avenues into your network, and that number has vastly increased with the growth of remote work. Remote work architectures represent a large attack artery that companies must contend with.

For instance, remote access solutions now offer remote users to copy and paste between their consumer grade laptop and their on-premise corporate desktop. These small but permissive attack avenues are but one example of how challenging it is to secure an IT estate.



IDG Research commissioned by WEI, January 2021.

Identifying Security Layers

1. One layer would be an email security solution that would eradicate phishing attacks that target user inboxes. Of course, no email security solution is failsafe, which is why another supplementary layer is an educated user that can identify a suspicious embedded link or attachment and know not to click on it.

2. Another layer would be an enforced configuration policy that denies access to removable drives, preventing users from transferring infected files using USB sticks.

3. Organizations should also consider bringing their firewall inside the organization. Rather than treating the firewall exclusively as a perimeter tool, additional firewalls can be strategically placed to segment, analyze and scrub traffic crisscrossing VLANs or traveling between sites, thus creating more security layers.

WEI Blog: The top mistakes of internal security teams:

- Remoting into the server that hosts backup solution
- Joining backup system to Microsoft Active Directory
- Installing backup software on virtual server
- Relying on passwords to protect log-on processes

Read Full Article

Layers That Work Cohesively Together

The effectiveness of multiple security layers to mitigate ransomware threats is further augmented if these layers work together.

For instance, a user decides to download a file from the internet that contains malicious code. Because the code is part of a zero-day attack that is part of a zero-day threat, the firewall mistakenly lets it through. That's why you have an EDR client serving as another layer that detects something isn't right about the file and contains it. While the immediate threat has been avoided, the containment doesn't deter other users from downloading the file. This means the battle might be fought a thousand times, increasing the chances of a successful infiltration.

But what if...

...the EDR sent the file to a sandbox where it was detonated and identified as malicious? The sandbox could then forward the code signature to the firewall where it then blocks it from that point on, preventing anyone within the organization from downloading the code ever again. Under this scenario, the EDR clients work as sensors, digital sentries that alert central command, ensuring that the battle only be fought once.

That is the power of layered security working in unison under a united front!

Maximize The Resources You Already Have

Don't ignore your treasure trove!

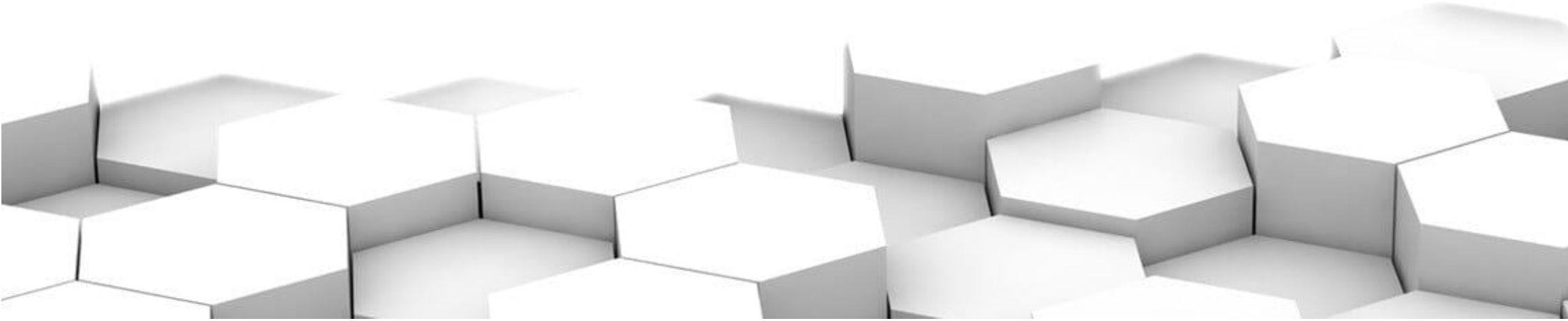
Maximize The Resources You Have

Many organizations fail to realize the integrated firewall tools they already have at their disposal while others ignore the treasure trove of information contained within the internal logs of these devices.

1 To maximize your investment in your next generation firewall, you need to enable all the features and functionality that it already has. These untapped features provide additional security layers. Besides the ability to block potentially malicious traffic from infiltrating or leaving the network, firewalls today provide visibility into your traffic patterns.

2 Integrated heuristic tools can actively monitor and analyze incoming traffic for abnormal packet activity, allowing you to act on them.

3 The firewall dispersed throughout your IT estate also contain extensive logging information that can be aggregated and correlated into a historical record, allowing you to discern how an attack occurred in order to contain it. This visibility can be enhanced with an external analyzer or SIEM that can generate actionable reports in real time, giving you the necessary time to react.



Turn Questions Into Solutions

And before you go...

Ransomware is a war, but a winnable war...

...if you have the correct cybersecurity strategies in place.

Transitioning from a Tier 1 organization to a Tier 3 or 4 doesn't happen overnight. There's also a learning curve when it comes to implementing a multilayer security strategy, strategic firewall placement, and logging interpretation.

WEI can flatten the learning curve and accelerate the implementation of your risk management action plans. Our experienced SMEs can help you access where you are right now, and determine where you need to be, **providing the guidance** to create an effective cybersecurity strategy.

Let WEI help you create the blueprint required to win the war against ransomware.

Why WEI? We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. We understand customer goals to integrate **meaningful strategy** with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.

Our clients benefit from a strong focus on customer satisfaction and attention to detail. From solution design through implementation, WEI's sales and technical team remains focused on providing unwavering support throughout a project. **Call 1-800-296-7837 to get started.**

Visit Our Blog

Contact Us

Thank You For Reading

The Blueprint To Prevent, Detect & Beat Ransomware

Call WEI at 1-800-296-7837