illumio

Q & A

The Zero Trust Cure for Ransomware Threats Q&A

Valuable perspectives from Forrester Analyst, Allie Mellen, after Illumio's Zero Trust webinar

Featuring FORRESTER®

1. **Does the current focus on ransomware mean that other vulnerabilities are being downgraded?**
2. **How do companies balance accepting risk vs. mitigating risk when it comes to ransomware?**
3. **Does the focus on using endpoint detection and response (EDR) to solve the ransomware challenge have the effect of blinding organizations to other solutions?**
4. **Does adopting a Zero Trust strategy help organizations mitigate against ransomware?**
5. **How can organizations measure their risk when it comes to ransomware?**

1 Does the current focus on ransomware mean that other vulnerabilities are being downgraded?

There is a huge public focus on ransomware right now, but that does not necessarily mean security teams are neglecting other threats in favor of shoring up ransomware protection. Ransomware defense requires many different aspects of an organization's security strategy, which is one of the reasons why it is so difficult to do well. Organizations should prioritize ransomware defense because it inevitably has a broader impact than just preventing ransomware. It helps strengthen their overall security posture to address this use case alongside other threats. Lastly, ransomware is a tangible, high-profile threat that CISOs can and should talk to the board about, if the board isn't already talking to them. Bringing clarity to the board about how to defend against ransomware and why it's so important to take these steps — with examples from recent attacks — can help them better understand why the CISO role is so critical to reducing business risk.

2 How do companies balance accepting risk vs. mitigating risk when it comes to ransomware?

One of the biggest challenges with ransomware defense is that there are infinite actions that practitioners can prioritize to reduce risk. There are so many, in fact, that it makes it difficult to know where to begin and where to focus your energies on an ongoing basis. The best way to approach ransomware defense is what I refer to as "survive by outrunning the guy next to you." There are ubiquitous steps every organization should take immediately to reduce its risk against a potential ransomware attack, including:

- Implementing multifactor authentication that is easy to use
- Ensuring backups are secure and tested
- Enforcing strong passwords
- Securing privileged accounts immediately
- Updating and testing your incident response plan

These five steps will get organizations on the right path but are just a starting point. They are the minimum steps an organization needs to take to make its defense better than other, easier targets. However, in the longer term, ransomware defense requires the strategic implementation of a Zero Trust strategy. Prioritize steps that require the least effort for the highest level of protection, that you can implement without buying additional tooling, and that are the most cost effective in the long term.

3 Does the focus on using endpoint detection and response (EDR) to solve the ransomware challenge have the effect of blinding organizations to other solutions?

Our research has shown that there is no consensus when it comes to ransomware defense. In particular, organizations struggle to decide whether backups, patching, or endpoint protection is the most important step an organization can take to defend itself against ransomware. Those are the top three steps organizations prioritize, yet they meet very different use cases in ransomware defense. Ultimately, ransomware defense requires a layered approach — defense in depth. It is not something organizations can implement overnight, which is why we recommend identifying the short-, medium-, and long-term steps you can take to improve your ransomware defense. Short-term steps should be the fastest actions for the highest impact; medium-term should be activities that take longer but still provide an outsize improvement; and long-term should be a focus on a Zero Trust security strategy. These will vary depending on the organization's existing security posture, toolset, and staffing.

4 Does adopting a Zero Trust strategy help organizations mitigate against ransomware?

A Zero Trust strategy absolutely helps organizations mitigate the effects of ransomware. Implementing Zero Trust in an organization can limit the spread of ransomware, preventing lateral movement. From a broader point of view, Zero Trust encompasses preventing access by default; utilizing prevention; and monitoring for, detecting, and responding to threats. That said, Zero Trust is a journey — it is an organization-wide effort that happens on an ongoing basis. It is a critical long-term approach to helping mitigate the effects of ransomware, but an organization can't implement it overnight. This should be part of an organization's long-term strategy to defend against ransomware and a plethora of other attacks.

5 How can organizations measure their risk when it comes to ransomware?

Measuring risk is easier said than done, as every CISO knows. In order to evaluate risk from ransomware, it's best to take stock of the state of existing ransomware defenses. Maintaining and keeping an up-to-date asset inventory gives security teams a sense of what devices and other assets they have and their status. Keeping a regular patching schedule gives security teams peace of mind that systems cannot be exploited by known vulnerabilities. Ensuring backups are protected and tested gives organizations a critical last line of defense if all else fails. These three basic steps will help security teams gauge risk when it comes to ransomware. Following these steps, it's critical to establish and implement a short-, medium-, and long-term strategy for ransomware defense.

To learn more, listen to the recorded webinar **"The Zero Trust Cure for Ransomware Threats"** with Trevor Dearing of Illumio and guest speaker, Allie Mellen, of Forrester Research.

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.