Gartner | Gigaom

Network Visibility and Ransomware

Ransomware attacks have become a major cybersecurity concern for many organizations across technology, retail, healthcare, manufacturing, and other critical infrastructure sectors. This infographic presents the results of a survey of 1,000 IT and security leaders in North America, Europe, and Asia-Pacific, to understand how organizations are addressing ransomware risks and strengthening their cybersecurity defenses, including network visibility and threat detection and response capabilities.

Data collected: February 28 - May 5, 2022 | Respondents: IT and security leaders

An overwhelmed or complacent minority could be putting organizations at higher risk of ransomware

86% of respondents say their ransomware activity has increased significantly or somewhat over the past 12 months.

Additionally, nearly all respondents (97%) say they have either implemented endpoint detection and response (EDR) or plan to implement it in the future.

However, in the APAC region far fewer respondents have actually implemented endpoint detection and response.

Of those who have already implemented EDR or XDR, 80% say it is the most important or a top three priority for ransomware.

EDR is especially important for those working in Information Security. 90% of Information Security leaders say it is the most important or a top three priority for ransomware, versus only 70% of those in other roles who responded to the survey.

However, despite achieving an endpoint detection, only 3% of respondents globally say they're very comfortable with the risk of unmanaged devices on their networks.

Organizations lack confidence they are fully prepared for the next ransomware attack

Almost all respondents (96%) have experienced at least one ransomware attack in the last 12 months.

Among respondents (EDR), ransomware attacks seem even more likely. 75% say they expect to experience a attack in the next year.

Despite the pervasive danger of ransomware attacks, only 40% of respondents globally say they know where most of their critical network infrastructure is.

In addition to indicating a higher risk of attack, respondents in EMEA are also less confident in their organizations' ability to prevent ransomware. Only 34% of EMEA respondents say they know how to prevent an attack, versus 48% of those in North America.

Only 40% of those who are confident in their organization's ability to prevent ransomware are also confident that their organization is fully prepared for a ransomware attack.

Network visibility and threat detection are foundational to a holistic ransomware defense

Network visibility and threat detection are foundational to a holistic ransomware defense. Organizations need visibility into their network to identify and respond to ransomware attacks, and threat detection and response provides the capabilities needed to detect and respond to ransomware attacks. Network visibility also provides the data to detect threats in encrypted traffic, which is critical for ransomware detection.

70% of respondents from all geographies either agree or strongly agree that having a holistic network visibility and threat detection and response capabilities is critical to our organization's ability to prevent ransomware attacks. Only 3% of respondents globally disagree or strongly disagree with this statement, while only 5% of respondents in EMEA say they agree.

Similarly, 66% of those surveyed in North America agree or strongly agree that an effective network visibility and threat detection and response capability is critical to our organization's ability to prevent ransomware attacks, versus only 44% in EMEA.

Organizations consider proactive threat hunting with NDR and Network Visibility as a best practice for ransomware defense

Proactive threat hunting is a key component of a holistic defense against ransomware, and a friendly practice. Threat hunting by using a combination of AI-driven NDR and network visibility.

However, respondents in APAC are much more likely to outsource their threat hunting to managed services and artificial intelligence (AI) by outsourcing to the most mature of threat hunting.

Despite utilizing multiple resources to threat hunt, 50% of respondents are only slightly, or moderately confident in their ability to identify threats.

Finally, 52% say they maintain and track management (EMEA, 57%), and 46% say they track and prioritize remediation (APAC, 54%) of ransomware.

Finally, 52% say they maintain and track management (EMEA, 57%), and 46% say they track and prioritize remediation (APAC, 54%) of ransomware.

Proactively, 50% agree or strongly agree that they are exercising tips and tips professionals and Purchase of the Ransomware attack, versus only 3% disagree or strongly disagree.

Organizations estimate ransomware would significantly disrupt their business

Ransomware attacks have become a major cybersecurity concern for many organizations, and it is a threat if impacted by a successful ransomware attack.

Additionally, 90% agree or strongly agree that they are exercising tips and Tips professionals and Purchase of the Ransomware attack, versus only 3% disagree or strongly disagree.

Gartner

This infographic contains research results and analysis from Gartner and Gigaom research. Gartner and Gigaom research publications consist of the opinions of their research organizations and should not be construed as statements of fact.

Gartner and Gigaom disclaim all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner and Gigaom are trademarks of Gartner and Gigaom.