WHITEPAPER

untangle

# HOW CYBER THREAT INTELLIGENCE

## SAFEGUARDS AGAINST TODAY'S THREAT LANDSCAPE

As the overall cyber threat environment continues to increase in complexity, it's becoming more and more difficult for organizations across every industry to adequately protect themselves. Within this landscape, organizations are looking for more advanced and innovative strategies to help them proactively respond to the latest malware being leveraged by hackers.

Enter cyber threat intelligence, a proactive way to guard against emerging threats that's becoming a more critical part of IT security.

## INCREASINGLY SOPHISTICATED THREATS DEMONSTRATE NEED FOR PROTECTION

Experts and real-world use cases alike show that the tools traditionally employed – including legacy firewall and antivirus systems – simply cannot keep up with the expanding threat landscape:

- 5 billion records were exposed by breaches in 2018; 13.9% from the government sector, 13.4% from the medical sector, and 6.5% from the education sector.[1]
- Organizations should aim to detect a breach within 100 days, but on average it takes 191 days.[2]
- 92% of malware is delivered by email, according to Verizon's 2018 Breach Investigation Report.[3]
- Mobile ransomware infections increased by 33% in 2018.[4]
- Average cost of cybercrime for an organization has increased from $1.4 million to $13 million in the last year.[5]

These conditions are requiring new strategies for network security, particularly as cyber protection continues to rank among business leaders' top priorities.

This is where cyber threat intelligence comes in, helping to bridge the gap between emerging threats and organizational security.

## A CRITICAL SOLUTION: CYBER THREAT INTELLIGENCE

According to Gartner's Rob McMillan, cyber threat intelligence can be defined as knowledge about an emerging threat that can be leveraged to better direct an organization's response to that particular hazard. This knowledge can come from several evidentiary sources, including certain context clues, indicators, conclusions and actionable guidance.

This evidence-based approach can help an organization better identify suspicious behavior that may point to the presence of a threat, allowing the IT team to quickly respond and remediate the threat. This prevents the company from having to rely on outdated threat definitions that previously would allow certain dangers to slip through the cracks undetected.

"Cyber threat intelligence, when used correctly, can help defenders detect attacks during – and ideally before – these stages by providing indicators of actions taken during every stage of the attack," SANS Institute analyst Dave Shackleford wrote.

Threat intelligence solutions analyze data pertaining to attacks and vulnerabilities across networks to identify weak points and attack vectors as they emerge.

In the current threat landscape, this type of approach to end-to-end protection is absolutely invaluable. WIth cyber threat intelligence in place, organizations are better equipped to battle the newest threats and ensure the protection of their most important assets.

## GUARDING AGAINST THE KNOWN AND THE UNKNOWN

From the Wannacry cyber attack to the Equifax credit reporting breach, it is clear hackers are getting more sophisticated in their attack methods. Organizations need to be proactive and implement security tools to better protect their network and sensitive information.

Thankfully, there are solutions out there that can not only protect your network at the gateway but also provide additional protection against unknown and emerging malware threats and zero-day exploits. Untangle's cyber threat intelligence cloud-based service,


ScoutIQ™ proactively scans all networks—including encrypted traffic—for various threats and malware, provides continuous threat protection by aggregating data from NG Firewall deployments worldwide, and synthesizes data from industry-wide threat intelligence services. By inspecting data at the metadata level, ScoutIQ is able to better inform the protection offered by NG Firewall, ensuring that the network is guarded against even the newest, emerging threats.

***Untangle's NG Firewall solution combines unified threat management with policy management tools to enable organizations to monitor, manage and shape Internet traffic.***

To find out more about how Untangle can help support cyber threat intelligence within your organization, contact us today.

## SOURCES

1 https://pages.riskbasedsecurity.com/2018-ye-breach-quickview-report
2 https://www.ibm.com/security/data-breach/index.html
3 https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
4 https://www.symantec.com/security-center/threat-report
5 https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

**Untangle, Inc.**
25 Metro Drive, Ste. 210
San Jose, CA 95110
**www.untangle.com**

## ABOUT US

Untangle is the most trusted name in solutions specifically designed to help small-to-medium businesses and distributed enterprises optimize their networks while safeguarding their data and devices. Untangle's Network Security Framework provides cloud-managed security and connectivity options that work together seamlessly to ensure protection, monitoring, and control across the entire digital attack surface from headquarters to the network edge. Untangle's award-winning products are trusted by over 40,000 customers and protect millions of people and their devices. Untangle is committed to bringing open, innovative and interoperable solutions to its customers through its rapidly growing ecosystem of technology, managed services, and distribution partners worldwide. Untangle is headquartered in San Jose, California.

**For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at sales@untangle.com.**