



WHITE PAPER

# Endpoint Visibility Gap

# ENDPOINT VISIBILITY GAP

## Endpoints are risky

Users and hosts are by far the most vulnerable parts of your IT environment. A whopping 82% of network compromises are caused by the human element—phishing, stolen credentials, misconfigurations, etc. While training employees on how to recognize phishing scams, and providing some checks and balances on passwords, two-factor authorization, and the like can help, the reality is that people will always be subject to manipulation or accidental oversight.

To secure your organization, you need key insight into endpoint behavior. Closely monitoring endpoint behavior on the network allows you to detect and respond to cyber threats in real-time. Just look at some of these figures:

- According to Verizon, 40% of Ransomware incidents involve the use of Desktop sharing software and 35% involved the use of Email.
- According to Cybersecurity Insiders, 34% of organizations say they have insufficient visibility into what is happening on the endpoint.
- The 2020 State of Endpoint Security Risk by Ponemon Institute found that 68% of organizations experienced an endpoint attack in the past year.

With the average cost of a breach being \$4.35 million and the average cost of an insider threat being \$11.45 million, businesses cannot afford to delay increasing their endpoint visibility.

## SECURING YOUR ENDPOINTS

You can take a variety of steps to secure your endpoints. Firewalls, antivirus and anti-malware controls, employee training, patch management, and access controls can all help limit an endpoint's exposure to threats or the total impact of a threat on the business. An endpoint detection and response (EDR) solution can also help. But none of these controls are infallible.

For example, a Watchguard Technologies Report found that fileless malware, which is known to bypass endpoint security controls, rose 900% in 2020. And a SANS survey uncovered that over a third of businesses include IoT devices and BYOD endpoints in their company's risk profile but they do not centrally manage those endpoints. Unmanaged devices present a huge risk to organizations who do not have other defense and depth security strategies in place.

Endpoint security controls are not enough.



# HOW TO INCREASE YOUR ENDPOINT SECURITY

Plixer's platform gives you a Network Detection and Response (NDR) solution to ensure that threats are identified early and stopped before they cause damage—regardless of where vulnerabilities are in your IT environment.

Many endpoint solutions often require agents or are signature-based. This makes deploying and maintaining those solutions more difficult and likely more expensive as you scale your efforts.

So, while their value can be immense, it may not be feasible for you to deploy strong security solutions across all endpoints that access your network.

With [Endpoint Analytics](#), a built-in component of Plixer's platform, you get real-time visibility into endpoint activity across your network. This allows security teams to identify anomalous behavior, such as unauthorized access, lateral movement, command and control communication, or data staging and exfiltration.

This level of visibility allows security teams to take immediate action to block or quarantine suspicious activity and prevent further damage.

With Plixer you can:

- Automate endpoint discovery and profiling, without the use of agents.
- Gain real-time visibility into device identity, location, and behavioral information.
- Ensure high scalability and availability of endpoints.

- Authenticate devices, segment networks, and institute granular network access controls.
- Improve compliance with data privacy regulations.
- Correlate endpoint events with network and security incidents.

Additionally, you can integrate solutions like ServiceNow, Microsoft Defender, Tenable, Splunk, and more to increase your alarm context and priority to respond to threats more efficiently.

By tracking endpoint behavior across the network, you can detect threats that bypass other security controls.

Plixer allows you to see and understand endpoint behavior to keep your business secure.



## SUMMARY

Endpoint security is crucial for protecting organizations from cyber threats. But endpoint security tools are not infallible. Having a layer of network visibility that can also provide endpoint telemetry can help you detect threats across the enterprise and know when your endpoint tools have failed.

With Endpoint Analytics, a built-in component of Plixer's platform, you get real-time visibility into endpoint activity across your network. This allows security teams to identify anomalous behavior, such as unauthorized access, lateral movement, command and control communication, or data staging and exfiltration.


By tracking endpoint behavior across the network, you can detect threats that bypass other security controls. Plixer allows you to see and understand endpoint behavior to keep your business secure.

## ABOUT PLIXER

Plixer gives you visibility and context of every network transaction so you can better understand what's happening in your IT environment. Our 20+ years of network monitoring and management solutions help us provide innovative solutions that help you secure and optimize your digital enterprise. Supercharge your business defense with AI-powered visibility and insight that goes beyond traditional NDR.

 [sales@plixer.com](mailto:sales@plixer.com)

 [plixer.com](https://plixer.com)

 68 Main St Ste 4  
Kennebunk, ME 04043



©Plixer, LLC. All rights reserved. Plixer and Scrutinizer are trademarks of Plixer. All other brand names are trademarks or registered trademarks of their respective companies.

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function.