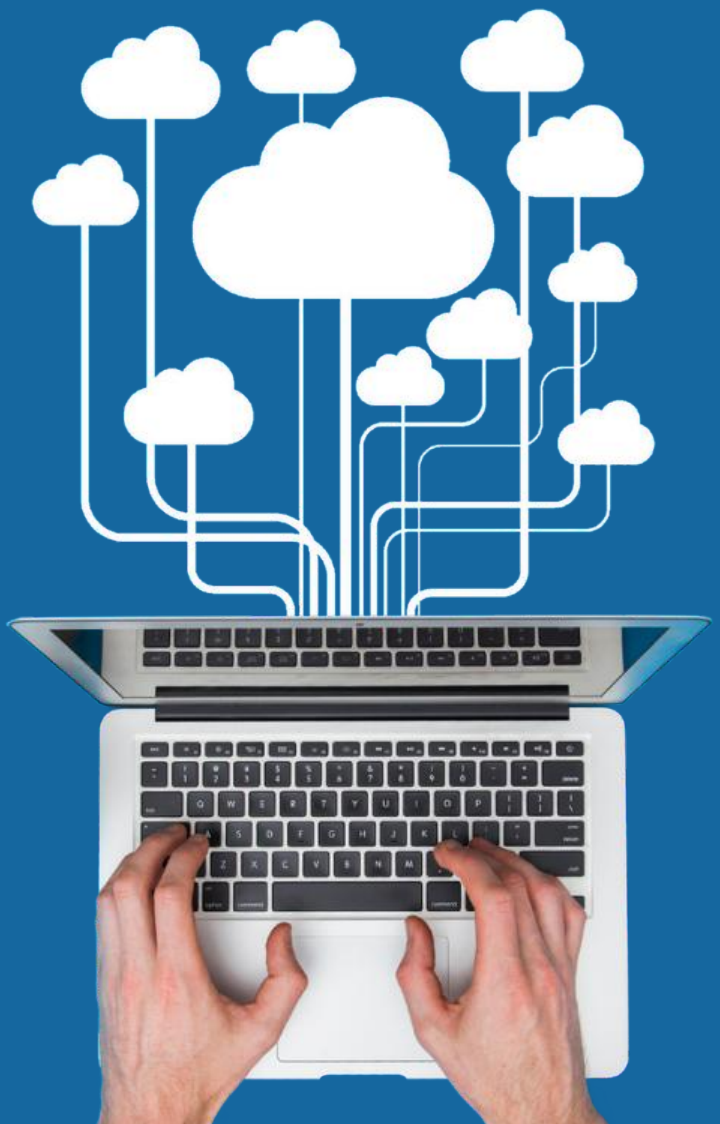
Top 7 Trends in Endpoint Security for 2023

Safeguarding Your Business in an Evolving Threat Landscape



stratodesk

Introduction

Endpoint security has become increasingly critical in today's rapidly evolving threat landscape. With the proliferation of remote work, cloud adoption, and the rise of sophisticated cyber attacks, businesses face numerous challenges in protecting their endpoints.

This report outlines the top 7 trends in endpoint security for 2023, providing IT and security leaders with valuable insights to enhance their endpoint security strategies.

1

Zero-Trust Architecture

The concept of Zero Trust Architecture (ZTA) continues to gain traction as an effective strategy to mitigate endpoint security risks. ZTA assumes that no user or device should be inherently trusted, regardless of their location or network.

By implementing strict access controls, continuous monitoring, and authentication protocols, organizations can prevent unauthorized access and limit lateral movement within the network.

A study by Forrester Research found that organizations with Zero-trust strategies experienced

50%

fewer security incidents

2

Importance of a Thin Managed OS

With the increasing adoption of cloud, Desktop-as-a-Service (DaaS), and Virtual Desktop Infrastructure (VDI) solutions, thin managed operating systems are more valuable than ever before.

By using a streamlined and hardened operating system, organizations can securely connect to cloud-based resources from both office and remote environments. This reduces the attack surface and minimizes the risk of endpoint compromise.

According to a report by Gartner, by 2023

70%

of enterprises will adopt thin managed operating systems for their endpoint devices

stratodesk

3

Cloud Native Endpoint Security

The adoption of cloud services and the shift to remote work has made cloud-native endpoint security a vital trend for 2023. Cloud-native solutions offer scalability, flexibility, and improved threat visibility.

They provide real-time protection, advanced threat hunting, and centralized management capabilities.

A study by IDC reveals that organizations using cloud-native security technologies experience a

43%

reduction in security incidents and a

33%

faster response time

stratodesk

4

Extended Detection and Response (XDR)

According to a report by ESG, organizations with XDR solutions detected security incidents

30%

faster and achieved a

40%

reduction in time spent on investigation and remediation

XDR platforms are gaining popularity as organizations seek to consolidate and streamline their security operations.

By integrating and correlating data from various security controls, XDR enables comprehensive detection, investigation, and response across endpoints, networks, and cloud environments.

stratodesk

5 Human-centric Security

Recognizing that humans are often the weakest link in the security chain, organizations are increasingly adopting a human-centric approach to endpoint security.

This trend involves training employees on best practices, implementing security awareness programs, and fostering a culture of security.

A study conducted by Ponemon Institute found that organizations with strong security cultures experienced

50%

fewer security incidents caused by human error

6 Endpoint Detection and Response (EDR)

EDR solutions are evolving beyond their traditional detection and response capabilities. New features, such as proactive threat hunting, automated response, and threat intelligence integration, enable organizations to take a more proactive stance against threats.

stratodesk

7

Integration of Security Orchestration & Automation

Endpoint security orchestration and automation play a vital role in streamlining security operations and reducing manual efforts.

By integrating security tools, orchestrating workflows, and automating routine tasks, organizations can improve incident response times and operational efficiency.

A study by EMA found that organizations adopting security orchestration and automation solutions achieved a

90%

reduction in response times

About Stratodesk

Founded in 2010, Stratodesk drives the adoption of secure managed endpoints for accessing the modern workspace through its innovative OS. Stratodesk NoTouch software gives IT customers endpoint security and full manageability while allowing the flexibility to choose endpoint hardware, workspace solution, cloud or on-premises deployment, and the cost consumption model that fits their business.

Today, with one million licenses deployed globally across multiple industries, Stratodesk prides itself on its authenticity and dedication to delivering the most innovative software solution to its customers. For more information, visit www.stratodesk.com.

Sources

Forrester Research, Study on Zero Trust strategies.
Gartner, "Market Guide for Endpoint Detection and Response Solutions."
Gartner, "3 B2B Marketing Trends you Must Know in 2023."
Gartner, "Magic Quadrant for Endpoint Protection Platforms."
IDC, Study on the benefits of cloud-native security technologies.
ESG, Report on the advantages of Extended Detection and Response (XDR) solutions.
Ponemon Institute, Research on the impact of strong security cultures on reducing security incidents caused by human error.
Gartner, "Hype Cycle for Endpoint Security."
Verizon, Data breach study highlighting the involvement of mobile devices in security incidents.
SANS Institute, Study on the benefits of continuous endpoint visibility.
EMA, Research on the effectiveness of security orchestration and automation solutions.

stratodesk

Try the most powerful thin client OS today

The #2 endpoint security trend is available for you to try today! See why thousands of customers choose Stratodesk NoTouch OS as their organization's Operating System of choice.

Start Free Trial