Secureworks®

WHITE PAPER

Endpoint Security: Protecting Your Business Wherever It Goes

Exploring the Evolution of Endpoint Security and Emerging Solutions

If you were to ask business leaders to define endpoint security, most immediately think of anti-virus software, but they would be only partly correct. Rarely does a day go by where we don't hear about a new cyberattack resulting in data encryption and theft. And while the risk of an attack to corporate reputation, shareholder value, and compliance has never been greater, at the same time, advancements in protection means it's never been easier to secure endpoints in a holistic way.

How can security teams secure endpoints and ensure they're addressing each facet of this challenging issue? This paper will explore how endpoint security has evolved from primitive antivirus software to sophisticated next-generation antivirus (NGAV) with Endpoint Detection and Response (EDR), for data protection regardless of where it resides—from the edge to the core to the cloud. We'll also look at the leading endpoint solutions available today.

The threat landscape has grown increasingly sophisticated, and with the exponential adoption of connected devices, comes an ever-expanding attack surface.

The Evolving Challenges of Endpoint Security

Endpoints provide an entry point of access to corporate networks, where threat actors can steal data, leverage existing software vulnerabilities, and hold information hostage.

Historically, cybersecurity concentrated on guarding the network perimeter. The network perimeter is the first line of defense against various forms of cyberattacks, fortifying and protecting all the data within the four walls of your company. However, in recent years, new technologies were created to help us work more efficiently—think cloud computing, mobile and IoT devices, and remote access to networks. As we traveled, the data traveled with us, and so too did the risk of data compromise. The network perimeter extended as these endpoints became the weakest links.

The COVID-19 pandemic introduced more risk as companies transitioned rapidly to a work from home model. This shift saw companies provision remote access and allow employees' personal devices to access the network. In some circumstances, employees had to use their own laptops as work computers while their desktop machines sat unused in company offices. Threat actors saw these changes as an opportunity and organizations saw an uptick in phishing scams and malware attacks using the pandemic as a social engineering tactic. In this confused milieu, many organizations didn't have the time or resources to figure out how to build a robust endpoint security posture, right at a time when they needed it the most.

The trend of remote working shows no signs of waning. According to some estimates, upwards of 30% of the workforce will likely work from home multiple days per week by the end of 2021.[1] On top of this, digital transformation projects are expected to grow

[1] Global Workplace Analytics, Work-At-Home After Covid-19—Our Forecast

to $1.3 trillion in 2020[2], and the number of IoT-connected devices is projected to reach 43 billion by 2023.[3] At no time in enterprise computing has the attack surface been greater, making it a critical business need to have a robust endpoint security posture. In fact, according to research by the Ponemon Institute, more than one third of IT security professionals indicated that their organization experienced at least one endpoint attack in 2019, with the cost of an endpoint breach averaging $9 million.[4]

$1.3 trillion

digital transformation projects are expected to grow in 2020.

43 billion

IoT-connected devices is projected to reach by 2023.

Common Endpoint Entryways to Corporate Data

There is an enormous variety of endpoints types, with these among the most commonly exploited:

- Desktops
- Printers
- Smartphones
- Laptops
- Tablets
- Servers

The challenge in securing data at the endpoint is having an endpoint security plan which effectively reduces risk. Identify what can be done effectively at the endpoint itself, including ransomware protection, enabling firewalls, and disabling known attack vectors. Since endpoint solution effectiveness varies greatly, it's important to know which solutions you should evaluate. What you can't prevent natively an endpoint solution should provide. There are some fundamental functionalities you'll want when looking for a solution that meets your needs. Here are some tips to get started.

3 Things You Want Your Endpoint Security Solution to Do

1. An endpoint security solution should detect malware and other threat actor tradecraft, as well as detect behaviors which could indicate the presence of a threat actor in your environment.
2. It should also reduce the time to detect and respond to attacks and quickly remediate, lowering the effort and cost in fixing them.
3. And finally, it should provide greater context into the motives and identities of the attackers so that new threats can be more easily addressed — and even prevented — in the future.

[2] IDC, New IDC Spending Guide Shows Continued Growth for Digital Transformation in 2020, Despite the Challenges Presented by the COVID-19 Pandemic

[3] McKinsey & Company, Growing opportunities in the Internet of Things

[4] Ponemon Institute, Ponemon Institute Reveals 68% of Organizations Were Victims of Successful Endpoint Attacks in 2019

Tools of the Trade

The continually evolving threat landscape, coupled with hundreds of thousands of unfilled cybersecurity jobs in the U.S. alone[5], leaves security teams stretched. For many teams, there isn't enough time to investigate all relevant events. Too often, the result of this is missed threats. Managing and securing endpoints effectively against today's threats requires combining anti-malware capabilities with a high level of visibility and behavioral-based detection. By arming itself with these weapons, an organization has a chance to not only detect threat actors and their evasive tactics, but to also slash the amount of time it takes to respond to attacks and minimize the damage they cause.

As threat actors continue their unrelenting pursuit of corporate data, a holistic approach is critical to ensure data is protected at the endpoint. What follows are some best practices which, along with the right endpoint security solutions, will go a long way in protecting your critical assets and data.

Zero Trust and Other Endpoint Security Best Practices

These best practices can be implemented now. Along with the right endpoint security solutions, you'll fortify your network and reduce the vulnerability of your data.

1. **Adopt a Zero Trust Philosophy**
    - Zero Trust means treating every user and device as potentially suspicious
    - Limit permissions extensively at first and slowly expand as your confidence level increases
        - Employees should not have administrator access
    - Minimize access to resources as much as possible
    - Implement privileged access workstations
2. **Harden Endpoints & Reduce Capabilities**
    - Disable Microsoft Office macros
    - Disable unused network ports
    - Whitelist applications for team access
    - Institute controlled folder access
    - Disable legacy protocols
3. **Conduct Functional Exercises**
    - Test backup recovery monthly
    - Conduct Purple Team[6] exercises quarterly, if not more
    - Practice technical foundations such as forensic imaging, log analysis (O365, AWS, Azure, endpoint, etc.), in your own environment

[5] Cyber Seek, Cybersecurity Supply/Demand Heat Map
[6] SANS, Purple Team Cyber Security Resources

While the best practices outlined above require security practitioner involvement, Secureworks® offers a wide range of endpoint security technologies through a unified Endpoint Platform that includes a wide range of tools, including antivirus, Next-Generation Antivirus (NGAV) with EDR, antispyware, host IDS/IPS, and other endpoint security technologies. What follows are two more solutions offered by Secureworks that are critical to ensuring the safety of your endpoints:

4. Proactive Threat Hunting

Employ Endpoint Detection and Response solutions which continually hunt for undetected threats. Think of the mission of EDR as detection and response – to find threat actors who are lurking on your endpoints and get the detailed information you need to identify and evict them. Even when evasive threat actors leave behind only behavioral clues, Secureworks EDR technology can identify them by analyzing telemetry using our threat intelligence.

5. Employ Comprehensive Security Analytics Solutions, Including Endpoint Security

- Red Cloak™ Threat Detection & Response (TDR) transforms the way your security analysts detect, investigate, and respond to threats. TDR is security analytics software that uses AI techniques to apply our threat intelligence to network, endpoint, and cloud telemetry and escalate only events that matter. The user interface presents analysts with all the context they need to act fast and allows for collaboration on event investigation. Analysts have the option to automate containment actions recommended by TDR. An internal chat box allows your team to connect with our experts instantly, 24/7/365.
- Managed Detection & Response (MDR) offers the same benefits of Red Cloak™ TDR for companies who prefer our experts to operate the software on their behalf, as a managed security solution. MDR includes regular proactive threat hunting and is backed by over 20 years of threat intelligence, incident response, and security operations expertise at Secureworks. Additionally, your analysts still get access to use the software and can contact our experts using the Ask an Expert chat box to ask questions 24/7/365.

By deploying the tactics and best practices outlined above, your organization will be prepared to detect evasive threat actors and significantly reduce the time it takes to respond to attacks. Monitoring customers environments around the world gives us global visibility into the threat landscape, which helps all our customers detect and respond to threats faster.

Our solutions are designed for the challenging conditions modern organizations face and are backed by a world-class team of security experts.

Each day, Secureworks processes more than 310 billion events, and we use that cumulative knowledge to continually optimize our detection capabilities.

Secureworks®

Secureworks® (NASDAQ: SCWX) a global cybersecurity leader, enables our customers and partners to outpace and outmaneuver adversaries with more precision, so they can rapidly adapt and respond to market forces to meet their business needs.

With a unique combination of cloud-native, SaaS security platform and intelligence-driven security solutions, informed by 20+ years of threat intelligence and research, no other security platform is grounded and informed with this much real-world experience.
www.secureworks.com

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp