2022 Endpoint Protection

QUICKSTART GUIDE

syxsense™

Today's threat landscape is more unpredictable than ever in the wake of the COVID-19 pandemic and the ensuing "Work From Home" and hybrid work models, leaving organizations vulnerable to an increasing number of cyberattacks.

A single compromised password allowed access to the Colonial Pipeline Co.'s network, shutting down the largest fuel pipeline in the United States. Malware used in the SolarWinds hack resulted in the breach of several federal agencies' networks. Most recently, the Log4j security vulnerability has affected potentially millions of devices, leaving businesses scrambling to determine the extent of exposure and patch accordingly.

This broad spectrum of cybersecurity hazards is perhaps the clearest manifestation of the rising danger, and endpoint security lies at its core. Already a complicated issue by any standard, the enduring challenges of the pandemic have become more complex and urgent to address in 2022.

"Your organization's endpoints are doorways through which your users access company data."

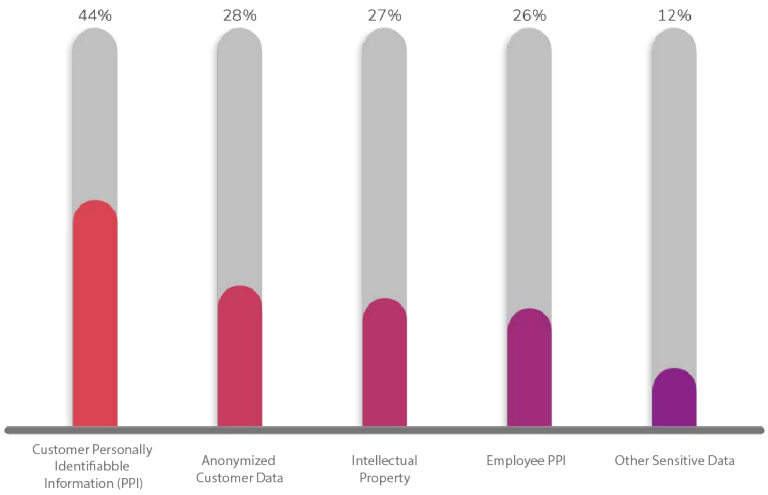
Many factors play into this forecast. The rise of newer and more dangerous threats, from crippling denial-of-service ransomware to large-scale records theft, is certainly among them, but so is the proliferation of mobile devices as IoT (Internet of Things) endpoints. Laptops hastily provided in the transition to remote work might lack security or may never have been seen by your IT professionals at all. BYOD policies that reduce equipment costs could expose you to greater risk by allowing devices that overlap with an employee's personal usage to have access to your network and resources.

UK-based analyst firm Expert Insights says "your organization's endpoints are doorways through which your users access company data. And the more diverse those endpoints are—be that in terms of location, device type or operating system—the more difficult they are to manage and secure."

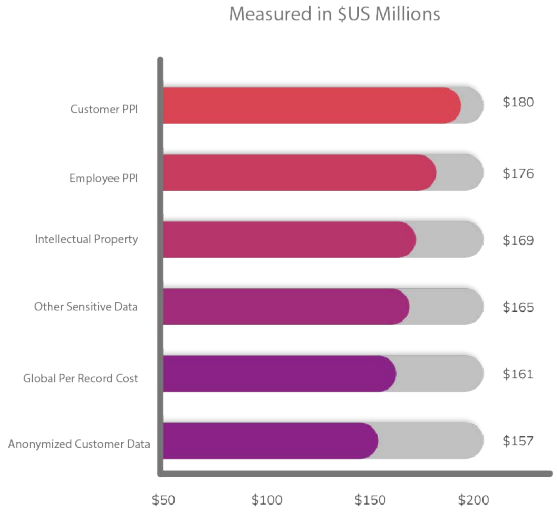
© Syxsense | All Rights Reserved |

Maybe it's your client database, including all the financial and personal information you've collected in the partnership process, that suddenly becomes inaccessible. Perhaps key files are abruptly encrypted in a way that you've never seen before. Or maybe systems grind to a halt and won't function. You see a message telling you, in so many words, to pay up or lose the data (or remain locked out of your mission-critical networks and devices). It's a simple and often successful exploit tactic.

Types of Records Compromised



Average Cost Per Record by Type of Data Compromised



Source: IBM's Cost of a Data Breach Report 2021

Five Critical Steps to Mitigate Risk

1. Know what devices are in your network, both on-premises and off-site
2. Quarantine new or returning devices
3. Scan for threats and vulnerabilities
4. Immediately apply critical patches and updates, and
5. Repeat steps 1-4 continuously

Modern endpoint security systems, such as **SYXSENSE**, handle every step of this process to keep your organization safe from endpoint attacks.

© Syxsense | All Rights Reserved |

THE BLENDED THREAT

Many modern threats are referred to as “blended threat” as they combine multiple threat vectors. The 2021 vulnerability referred to as PrintNightmare (CVE-2021-34527) required the application of a patch, plus a couple of required configuration changes to fully remediate the threat. In their Knowledge Base article KB5005010, Microsoft recommends the installation of a Patch, the scan of machines to determine the state of several Registry Keys, and the application of a Policy setting those Registry Keys to “0.”

Historically, it would require three separate tools to Patch, Check Status, and Apply Policy, plus substantial scripting effort to fully remediate this threat. The Syxsense security platform is unique in its ability to unify all these steps into a single process, and provide the entire remediation process as a simple, pre-built Syxsense Cortex™ Workflow.

THE COST OF EXPOSURE

While massive breaches can disrupt infrastructure on a global scale, targeted threats can affect the operations, revenue, and reputation of any business. To members of the C Suite who aren’t chief information or technology officers, the urgency of cybersecurity threats may not be realized.

In addition to the challenge of protecting an expanding, flexible device fleet, IT teams are also battling the fact that endpoint attacks are on the rise. As the number of attacks increases, so does the sophistication with which they’re carried out. Because of this, 68% of organizations recently experienced one or more endpoint attacks that successfully compromised their IT infrastructure and/or their data.

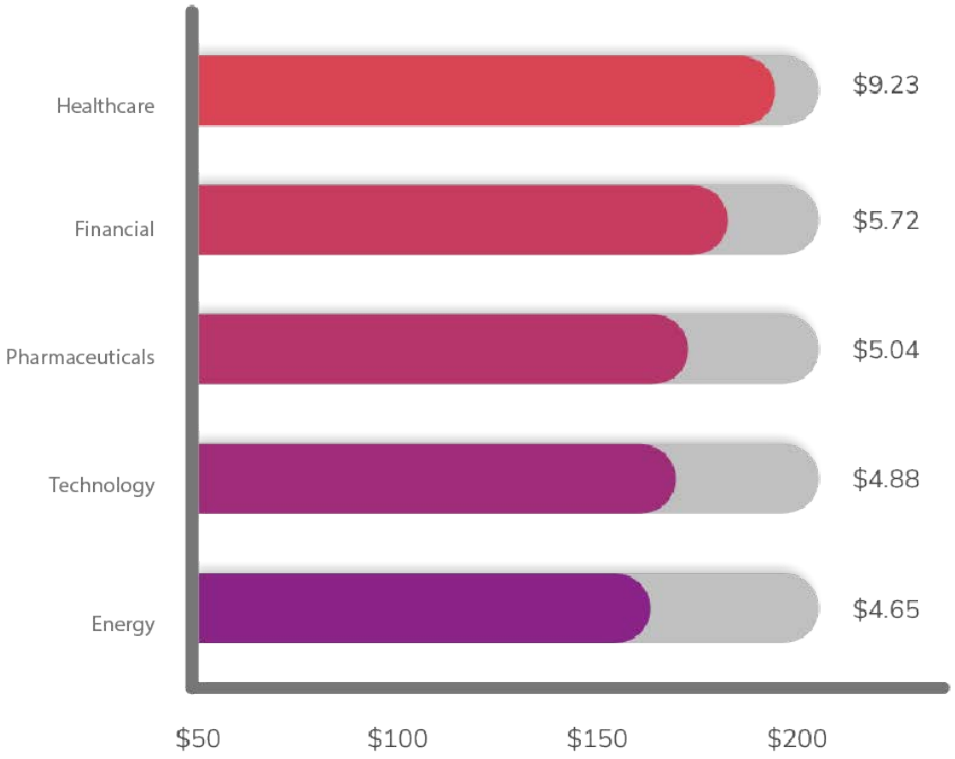
- Although average organizational cybersecurity spend is up — from $2,337 per employee in 2019 to $2,691 in 2020 according to Deloitte Insights (up from $1,337 per employee in 2018)— that may not be nearly enough for large enterprises, or those within commonly targeted industries like finance or healthcare. A 2019 survey by Deloitte and the Financial Services Information Sharing and Analysis Center reported that financial services firms spent anywhere from 6% to 14% of their IT budget on cybersecurity.

© Syxsense | All Rights Reserved |

• The average cost of a data breach rose 10% from last year, from $3.86 million to $4.24 million in 2021, according to IBM's Cost of a Data Breach Report. Specific figures vary by country, industry (healthcare breaches cost the most at$9.23 million per incident), and incident severity.

Average Total Cost of a Data Breach by Industry

Measured in $US Millions



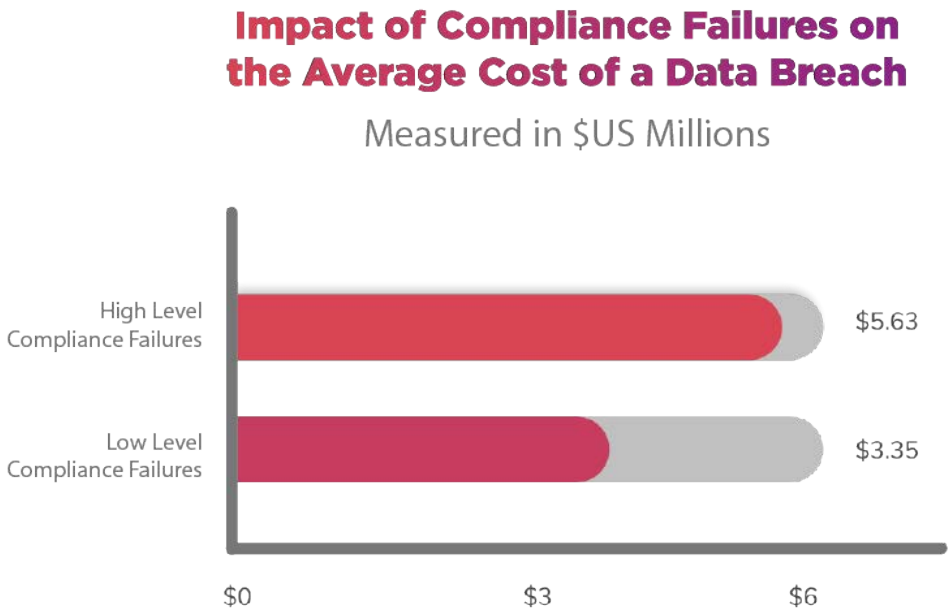
Source: IBM's Cost of a Data Breach Report 2021

• The average ransomware payment in 2021 was a record $570,000.

• According to the FBI, the cost of cybercrime in the US was $4.2 billion in 2020, compared to $3.5 billion in 2019, and expected to continue to rise.

• All told, the impact of cybercrime costs the world as much as $600 billion each year, without even considering the economic "drag" it causes.

There can be many additional hidden costs of an incident as well. A business that suffers a cybersecurity breach can face insurance premium increases, losses due to operational disruption or repairing operational capabilities, drop in credit rating, and lost customers.



Source: IBM's Cost of a Data Breach Report 2021

Specific industries, such as businesses in healthcare or finance, face increased risk due to their responsibility for the protection of sensitive private data. Organizations in these industries that insufficiently safeguard data open themselves up to fines and legal proceedings in the wake of an attack.

THE ENDPOINT NUMBERS GAME

88% of IT professionals understand the importance of endpoint management and security, but a significant number of those individuals may not know exactly how many endpoints their organizations' networks have.

Based on the current pace of tech development, the number of endpoints in any given system is bound to increase exponentially in 2022. Significant upticks in overall mobile device use, as well as expansion of IoT will drive this, increasing organizations' endpoint security risk by default.

© Syxsense | All Rights Reserved |

Endpoint management is even more challenging in remote and hybrid working environments where IT departments have less control. Employees might use their personal laptops or tablets for remote work, check company email on a personal cell phone, or work from a company device that shares an internet connection with family laptops or gaming consoles which could be accessing potentially malicious content online.

The average cost was $1.07 million higher in breaches where remote work was a factor in causing the breach.

The traditional network perimeter is no longer effective in this environment.

Cybersecurity experts refer to it as the 'crunchy/chewy' model, with network security protocols such as firewalls as the hard, crunchy exterior, blocking access to the soft and chewy inside. As users become increasingly mobile and they're no longer always within the perimeter (and network security protocols may not always apply to them), the industry is rapidly leaving this model behind.

The perimeter of protection needs to expand beyond the conventional boundaries of an organization's offices or a network's on-premise location – it needs to extend to the individual endpoints each time they return to a network.

More access points mean more vulnerabilities. The first step in strengthening the security perimeter of any organization is knowing how many endpoints are in your network and have access to your data. An endpoint security system discovers, scans, and logs devices in your inventory any time a device is introduced to your network.

See Endpoint Security in Action

© Syxsense | All Rights Reserved |

MAJOR ENDPOINT THREATS TO WATCH IN 2022

In the advancing technological landscape and the rise of the remote workforce, endpoints are among the most vulnerable. Everything from PCs and smartphones to IoT-enabled printers represents an attractive collection of weak spots to malicious online actors. Cybercriminals will use malware to attack said endpoints in any way they can, through the operating system and application layers as well as at the firmware and BIOS levels.

Threats of particular note include:

Ransomware
Ransomware operators are targeting increasingly larger enterprises and escalating ransom demands to record amounts as the groups become more highly sophisticated and coordinate attacks on anything from SMBs to software supply chains. The end goal of these attacks is no longer only infection; ransomware is oftentimes just one component of an attack, such as in the malware families WannaCry, NotPetya, Ryuk, Cerber, and Cryptolocker. These high-profile dedicated-denial-of-service attacks have successfully shut down municipal governments including Baltimore, Atlanta and Greenville, North Carolina during 2018 and 2019, and also devastated the healthcare sector.

Phishing
Social engineering threatens mobile endpoints just as much as desktops. Since the start of the COVID-19 pandemic, email phishing scams attempting to get confidential information have increased, leading the FBI's Internet Crime Complaint Center to label it a pandemic-fueled "internet crime spree." Emails claiming to be from human resources requesting proof of vaccination link employees to a fake sign-in page where criminals can harvest credentials, in just one example.

Other scams, like smishing (SMS phishing), and other similar attacks are also on the rise and can leave organizations open to fraudulent acts as the digital transformation continues.

Rootkits/backdoor-access attacks: Cyberattackers who care more about theft (monetary or informational) than havoc may use subtler methods like these to gradually take what they want.

© Syxsense | All Rights Reserved |

In the recently discovered SysJoker attack, the threat poses as a system update and allows the threat actor to control the system in targeted attacks, suggesting this is the first step in the attack and a ransomware attack may follow.

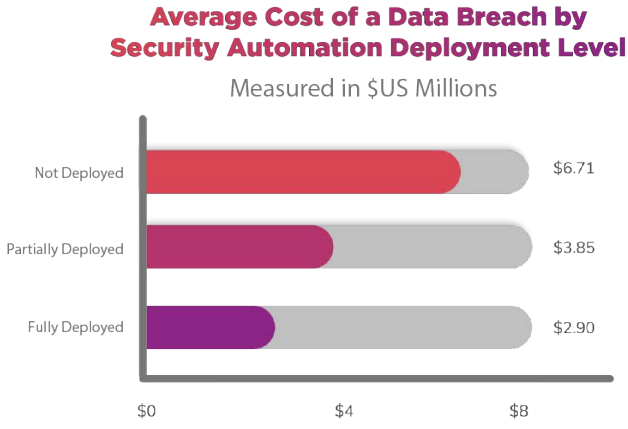
Employee negligence

Lax security-protocol adherence can leave endpoints more open to attack. For example, employee-owned mobile devices are the endpoints least likely to be properly secured.

Companies are requiring more advanced safeguards against attacks as remote workers are typically the first to face security threats, such as instituting a system of regular, forced password changes and stricter password requirements. Some businesses are using phishing 'drills', where employees are unknowingly sent 'suspicious' emails and links from their own IT department to increase awareness of scams and knowledge of reporting measures among employees.

CONSISTENCY IN ENDPOINT SECURITY

You can't protect your network's endpoints by operating on a case-by-case basis, going with the flow as different issues arise independent of one another. Doing so amounts to treating this as a "fly by the seat of your pants" issue, which is neither feasible nor responsible in the context of any aspect of cybersecurity (endpoint-related or otherwise).



Source: IBM's Cost of a Data Breach Report 2021

It is critical for organizations to adopt consistent approaches to endpoint security in 2022 and beyond, fully comprehending and addressing all risks associated with its endpoints. This involves vetting the security capabilities of new devices before they are introduced to the network and continuously monitoring device vulnerability

levels to ensure they never become dangerously outdated and unprotected.

One way for IT teams to achieve this without additional burden is with an endpoint security system that automates critical security tasks for each individual device in a network. Solutions like Syxsense Cortex™ use pre-built workflows to gather real-time data on your endpoints and execute multi-step actions that not only identify the security risk but resolve it.

ENFORCE ENDPOINT SECURITY HYGIENE

Around 50% of companies that have a breach will be breached again within 24 months. IT teams must relentlessly hold the organization to high endpoint security standards in order to manage and secure their endpoints more efficiently.

- **Retire and replace legacy hardware/software:** Such resources are more likely than not to have unmanageable vulnerabilities. Devices with software or operating systems that are past their end-of-life oftentimes don't receive critical patch updates, leaving them exposed to cyberattacks, such as in the 2017 WannaCry ransomware attacks.

- **Ensure all endpoints matter equally**: An attacker entering via a networked printer (a commonly under-protected endpoint) likely isn't interested in taking over that machine, but rather something far more destructive. Gaining access to any endpoint that sits on your network can open the door to other company data.

- **Keep up with trending threats:** Note which scams are most prevalent among your industry peers and in general (like ransomware/DDoS attacks and botnets), without losing sight of less obvious possibilities (logic bombs, man-in-the-middle attacks, formjacking).

- **Maintain up-to-date patch management:** Enable automatic updates for the most critical security patches, while handling less mission-critical patches manually (Also, ensure patch application disrupts day-to-day operations minimally or not at all.) Such as with the recent Log4j vulnerability, IT teams need to keep up-to-date with rapid patch releases to prevent the vulnerability from being exploited in their organization.

© Syxsense | All Rights Reserved |

TURN TO SYXSENSE FOR MORE SECURE ENDPOINTS

Syxsense is a cloud-based unified endpoint security and management platform that helps organizations manage and secure the PCs, desktop servers, and virtual, mobile and IoT devices connected to their networks. Syxsense encompasses vulnerability scanning, patch management and endpoint security—enabling organizations to align their core IT management processes with their cybersecurity strategies.

The most effective way to meet the challenges of today's threat landscape is to mitigate the risk of exposed endpoints, no matter where they're located, on a continual basis. Syxsense handles each step of the process, from the agent-based device inventory that gives you visibility on every network device to vulnerability scans and threat remediation through Syxsense's Cortex™ workflow engine.

Keep the cyberattacks of 2022 out of your system with the knowledge of exactly what's inside your infrastructure and what's changed in your environment in real-time with Syxsense.

Looking for an endpoint security solution?
Get a personalized demo of Syxsense.

SCHEDULE A DEMO

syxsense

www.syxsense.com

info@syxsense.com

(949) 270-1903