The Future of Network and Endpoint Security

From current business vulnerabilities to emerging security trends, Spiceworks examines the current state and future of network and endpoint security in businesses across North America and Europe.

There's a common saying in the world of cybersecurity: It's not a matter of "if," but "when" a security incident will rear its ugly head. Businesses constantly have to deal with phishing, malware, insider threats, and newly discovered vulnerabilities. To reduce risk and adequately protect against cyber threats, organizations need to employ a multi-layered security strategy that protects corporate networks, devices, and data. But this is no simple task for IT departments.

To understand how organizations approach security, we surveyed nearly 500 IT decision makers across North America and Europe to uncover insights on how businesses are protecting their environments, what network and endpoint security solutions they're using, and which emerging cybersecurity technologies they're adopting.

**Key Findings**

1. Two-thirds of businesses believe their current security solutions adequately protect their corporate network.

2. However, outdated operating systems on endpoint devices and the limited use of encryption pose major vulnerabilities.

3. A cybersecurity skills gap is also prevalent, especially in SMBs where more than half of organizations do not have a security expert on staff.

4. To face ever-evolving security threats, many businesses are turning to next-gen security solutions like AI-powered threat intelligence and security “as a service.”
Emerging Cybersecurity Trends

The number of cybersecurity incidents businesses face continues to grow. In 2018, the U.S. Federal Bureau of Investigations (FBI) received more than 350,000 complaints of internet crimes, up 23% in five years. However, losses from these crimes increased more than threefold in the same time period, rising from $800 million in 2014 to $2.7 billion in 2018.

New Spiceworks research shows two-thirds of businesses believe their security solutions adequately protect their corporate network from security threats, but this still leaves a lot of room for improvement. Thankfully, emerging security technologies can help businesses in the fight against cyber threats.

The rise of AI-powered security tools

With the sheer volume of emails, messages, and other data travelling across corporate networks, it’s challenging for IT professionals equipped with traditional defenses to keep an eye out for ever-increasing dangers — but many believe artificial intelligence (AI) can help.

According to Spiceworks survey data, 59% of IT decision makers agree that AI and machine learning technologies can help organizations better detect and respond to security threats. We expect this positive outlook to translate into a sustained increase in adoption of AI-powered security solutions, which can help organizations analyze and respond to large volumes of threat data in real time.

For example, Spiceworks survey data indicates 18% of businesses currently use AI-powered threat intelligence platforms, and another 30% of businesses are considering using them by 2021. Additionally, adoption of network security appliances equipped with AI capabilities, which help protect against unknown threats such as zero-day attacks, currently stands at 12%, and another 32% of businesses are considering adopting them by 2021.

Adoption of “zero trust” becoming commonplace

In recent years, organizations have increasingly moved towards a “zero trust” security model, whereby companies adopt a “never trust, always verify” stance towards access and authentication. In fact, our research shows the zero trust model has widespread approval: 69% of IT decision makers agree it’s a very effective way to protect against security breaches. And currently, 42% of businesses have adopted zero trust in some form:

- 13% use an “absolute zero trust” model where no access is granted without proper authorization/verification
- 29% are “approaching zero trust,” where the vast majority of systems and critical data require authorized/verified access

However, a “moderate trust model” is more common among respondents (47%) where at least some efforts are made to restrict access to sensitive data and systems. Thankfully, trust is assumed by default in only 7% of businesses, where companies rely on employees’ best intentions to access only what they need.
Growing adoption of “as a service” security solutions

In many cases, “as a service” offerings allow businesses to outsource IT responsibilities to a trusted service provider. In line with this trend, we found that adoption of security solutions offered “as a service” is expected grow in the near future.

The most common security solutions offered “as a service” include endpoint security as a service and threat protection as a service. Within the next two years, use of intrusion detection and prevention as a service is expected to see the most growth: 12% of organizations use it today and another 23% are considering it by 2021.

Current Security Vulnerabilities

Now that we better understand where cybersecurity solutions and practices are headed in the future, let’s focus on the current state of corporate cybersecurity. While the advancement of security technology and increasing adoption of new solutions is promising, there are still blind spots and vulnerabilities for businesses around the world.

Outdated operating systems persist

Often, older devices or software remain present on networks far past their end of support dates, whether due to legacy applications that won’t run on newer operating systems, embedded software that was never updated by the manufacturer, or lack of funding and resources needed to update end-user or back-end systems. In fact, according to Spiceworks technology deployment data, 32% of businesses still have Windows XP installed on at least one device on their network, despite the OS’s end of service date in 2014. While this figure is down slightly from 42% in 2017, the number of companies with outdated and therefore vulnerable machines is alarming.
With Windows 7 reaching end of service date on January 14, 2020, there will soon be even more out-of-support systems to worry about. According to Spiceworks technology deployment data, 79% of organizations still run at least one instance of Windows 7, and many of these businesses will procrastinate in their migration efforts. In fact, Spiceworks survey data shows 67% of businesses running Windows 7 plan to migrate all their machines off of Windows 7 prior to the end of service date, but 25% plan to migrate after the deadline.

Limited use of data encryption

It’s a commonly held belief that encryption can help protect data wherever it resides. In fact, three out of four IT decision makers surveyed believe it’s critical to encrypt data wherever it may be (at rest, in motion, or in use at the application level) to protect sensitive data.

However, according to Spiceworks research, 17% of businesses still do not employ any type of encryption. Among businesses that do use encryption, over half (56%) are encrypting data at rest, but only 40% encrypt data in motion, and only 31% encrypt data at the application level — a concern, given numerous recently-discovered CPU vulnerabilities including Spectre and Meltdown. Unfortunately, only 14% of businesses employ all three types of encryption.

Lack of preparedness for common cybersecurity threats

When we asked IT decision makers to tell us how prepared their business is to defend against common security threats, 27% told us their business is unprepared to respond to internal data leaks, making it the top threat organizations are vulnerable to.

Other threats businesses felt unprepared to face include zero-day exploits (18%), attacks on IoT devices (17%), supply-chain attacks (15%), DDoS attacks (15%), and cryptojacking (15%). Additionally, less than 20% of businesses said they were “completely prepared” for any of the common types of security threats they were surveyed about, which also included phishing, ransomware, and supply chain attacks.
Limited access to security experts

One reason businesses feel unprepared to face common security threats might be due to limited access to security expertise. According to our research, only 47% of businesses have one or more cybersecurity experts on staff (e.g., IT security expert, CSO, information security officer). When comparing the data by company sizes, small businesses are the least likely to have expertise in house: 38% of small businesses have a security expert on staff, compared to 48% of mid-size companies and 72% of enterprises.

To compensate for a lack of on-staff security knowledge, many businesses turn to outside sources for help. For example, 51% of all businesses surveyed work with third-party security consultants, and 22% work with one or more managed security service providers. However, 17% of organizations have no access to cybersecurity expertise.

Security Purchase Consideration Factors

When it comes to what attributes matter most to IT decision makers evaluating security products and vendors, many respondents told us it’s critical for solutions to offer great value for money (46%), minimal performance impact (44%), and protection against zero-day threats (44%).

<table>
<thead>
<tr>
<th>Importance of Consideration Factors When Evaluating Security Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Great value for money</td>
</tr>
<tr>
<td>Minimal performance impact</td>
</tr>
<tr>
<td>Protection against zero-day threats</td>
</tr>
<tr>
<td>Supports a variety of devices</td>
</tr>
<tr>
<td>Interoperability with other security tools</td>
</tr>
<tr>
<td>Holistic approach to threat protection</td>
</tr>
<tr>
<td>Offers innovative features</td>
</tr>
</tbody>
</table>

Most businesses purchase solutions from a variety of security vendors to meet their needs today. However, more than half of IT decision makers (51%) would consider using a single security vendor if they offered a comprehensive, multi-layered product portfolio that, for example, protects both endpoint devices and corporate networks.

Security vendors should also keep in mind that many businesses are moving to cloud-based security solutions. In fact, 40% of businesses use cloud-based security solutions, and another 24% are considering adopting them by 2021. Looking forward, 37% of IT decision makers believe the majority of their organization’s security solutions will be cloud-based in the foreseeable future.
Endpoint Security Solutions

As employees increasingly work at home, in cafes, in coworking spaces, and while travelling, it’s now more important to protect individual devices when they leave the relatively-safe confines of the corporate network. To get a snapshot of how businesses are protecting endpoint devices, we examined which endpoint security providers are on the rise and how satisfied businesses are with their solutions.

According to our data, the following endpoint security technologies and capabilities are expected to see the most growth in the next two years:

Among endpoint security providers, the data shows Malwarebytes and Sophos are the most commonly used across all company sizes, but it’s worth noting the vast majority (93%) of Malwarebytes customers use their product in conjunction with another endpoint solution.

The data indicates Symantec, Webroot, Trend Micro, Bitdefender, and ESET are also among the top endpoint security providers. Other notable players not charted below include McAfee and Palo Alto Networks with 8% adoption each, and Kaspersky and Avast with 6% adoption each.

---

**Top Endpoint Security Providers: Current Usage + Consideration**

*Current business adoption plus the percent of businesses considering each provider within the next 2 years*
When examining the data by company size, enterprises (1,000+ employees) are most likely to use Sophos (34%). Enterprises are also much more likely to use McAfee (23%), compared to mid-size (7%) and small businesses (4%).

We also examined how satisfied users are with their current endpoint security providers. The survey results show the following brands have the highest user satisfaction across the top three most important purchase consideration factors:

1. Great value for money: Webroot
2. Minimal performance impact: Webroot and ESET
3. Zero-day threat protection: Sophos

**User Satisfaction of Top Endpoint Security Providers**

*Percent of IT decision makers who believe their provider meets or exceeds expectations for each attribute*

![Graph showing user satisfaction of various endpoint security providers.]

**Network Security Solutions**

Security solutions offering protection at the network layer can help stop security threats attempting to penetrate corporate networks. Traditionally, network firewalls have been used to block ports at the network perimeter, but in recent years, newer types of network security devices have gained additional functionality including packet inspection, content filtering, spam filtering, and more.

While practically all businesses use some form of network security appliance, basic network firewalls are currently most prevalent. However, in the future, the most growth is expected among more modern next-generation firewalls and unified threat management devices, which typically offer a higher degree of protection.
Vendors offer many security features and capabilities across a variety of network appliance offerings. According to the data, the following network appliance technologies and capabilities are poised to see the most growth within the next two years:
When examining providers of network security appliances, Spiceworks survey data indicates Cisco, SonicWall, and Meraki by Cisco are most commonly used by businesses today. Sophos, Fortinet, and Barracuda are also among the top providers. Other notable players not charted below include Palo Alto Networks, WatchGuard, and pfSense with current adoption at 9%, 8%, and 6% respectively.

Breaking down usage by company size, larger businesses surveyed are more likely to use Cisco (not including the Meraki brand). In fact, 57% of enterprises use Cisco-branded network security appliances, compared to 39% of mid-size businesses and 25% of small businesses. The same goes for Palo Alto Networks: 17% of enterprises surveyed use Palo Alto devices, compared to 12% of mid-size companies and 3% of small businesses. On the opposite end of the spectrum, smaller companies surveyed are most likely to use SonicWall, with 31% usage among small businesses, compared to 20% of mid-size businesses, and 6% of enterprises.

When asked how satisfied they are with their current security appliance provider, users indicated Sophos (which also scored high marks for their endpoint security solution) earned the highest user satisfaction score for two of the three most important consideration factors:

1. Great value for money: Sophos
2. Minimal performance impact: Fortinet
3. Zero-day threat protection: Sophos
Growth Opportunities for Security Vendors

As security technology evolves, so do the techniques used by malicious actors to launch cyber-attacks. In today’s heightened threat landscape, organizations must contend with zero-day threats, sophisticated social engineering and phishing campaigns, spoofed websites, cryptojacking, fileless malware, and much more.

In the face of these challenges, there are several areas where businesses indicated they want more support from security vendors and consultants. In fact, businesses need the most support when it comes to penetration testing, risk and vulnerabilities assessments, security training for end users, and security training for internal IT staff.

Areas Where Businesses Need More Support from Security Vendors & Consultants

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penetration testing</td>
<td>52%</td>
</tr>
<tr>
<td>Risk and vulnerability assessments</td>
<td>51%</td>
</tr>
<tr>
<td>Security training for end users</td>
<td>46%</td>
</tr>
<tr>
<td>Security training for internal IT staff</td>
<td>38%</td>
</tr>
<tr>
<td>Compliance assessment</td>
<td>31%</td>
</tr>
<tr>
<td>Developing a comprehensive security program</td>
<td>29%</td>
</tr>
<tr>
<td>Incident response</td>
<td>29%</td>
</tr>
<tr>
<td>Improving threat intelligence capabilities</td>
<td>29%</td>
</tr>
<tr>
<td>Digital forensics</td>
<td>27%</td>
</tr>
<tr>
<td>Implementing company-wide security policies</td>
<td>27%</td>
</tr>
<tr>
<td>Network architecture design or redesign</td>
<td>20%</td>
</tr>
</tbody>
</table>
In summary, it’s clear security is a large undertaking for businesses of all sizes, and that very few, if any, organizations feel completely safe. And while businesses are steadily improving their defensive capabilities, malicious actors are constantly finding new ways to wreak havoc.

But amidst the ever-growing threat landscape, there’s a massive opportunity for security vendors to help businesses better protect their devices, data, and networks, especially as many businesses begin to evaluate more advanced security technologies. Looking forward, security vendors that can offer solutions and services with the right mix of value for money, protection against emerging threats, and innovative capabilities stand to gain the most ground.

**Methodology**

The Spiceworks survey was conducted in June 2019 and included 489 IT decision makers in Spiceworks. Respondents represent organizations in North America (77%) and Europe (23%) across a variety of company sizes, including 37% from small businesses (1 to 99 employees), 53% from mid-size businesses (100 to 999 employees), and 10% from enterprises (1,000+ employees). Respondents represent a variety of industries, including education, healthcare, nonprofits, government, finance, retail, construction, manufacturing, and IT services. The survey data was supplemented by operating system data that was collected in April 2019, based on anonymized, aggregated technology deployment data from Spiceworks products.

**About Spiceworks**

Spiceworks is the marketplace that connects the IT industry to help technology buyers and sellers get their jobs done, every day. The company helps people in the world’s businesses find, adopt, and manage the latest technologies while also helping IT brands build, market, and support better products and services. Founded in 2006 and headquartered in Austin, Texas, Spiceworks empowers people to use technology to make their organizations, their communities, and the world better. For more information, visit [www.spiceworks.com](http://www.spiceworks.com).