How Companies Protect Themselves from Cyberattacks: Enterprises vs. SMEs

The need to address cyberattacks increases all the time. According to the World Economic Forum, "the FBI reports that more than 4,000 ransomware attacks occur daily, while other research sources state that 230,000 new malware samples are produced every day."

It can easily get overwhelming, so to help you navigate these uncertain times, let's take a look at how companies of different sizes protect themselves from the new malware that's created on a daily basis.

Cybersecurity Policy

Cyber threats impact businesses of all sizes, yet many SMEs aren't aware of the fact that they're in just as big a danger as large companies.

That said, even those who are aware of the risk find it challenging to develop policies and game plans around it, given that almost half of SMEs "have no understanding of how to protect their companies against cyberattacks," according to Betanews.

Large companies are further ahead in the process, at least in the US. 94% of survey participants from large companies in the US told Clutch that they have a cybersecurity policy, yet Clutch added that two thirds of global organizations "lack a formal cybersecurity policy."

Among those 94% survey participants, "cybersecurity policies most commonly include required security software (84%), how to back up data (81%), how to detect scams (79%), and how to report security incidents," shared Clutch, adding that companies tend to "implement cybersecurity policies that focus on communication and training more than enforcement."

Here's where communication comes in handy:

Employee Education

In an interview with Fortune, Asheem Chandna, an investor with Greylock Partners and a Palo Alto Networks director, explained that "most hacking attacks come about in two ways, and neither of which involves a high level of technical sophistication: An employee clicks on a… link or attachment – perhaps in an email that appears to be from her boss – or someone steals an employee's log-in credentials and gets access to company network."

Fortune pointed out that no level of seniority in the organization is safe from getting hacked. "In the summer of 2015, several of New York's most prestigious and trusted corporate law firms… found themselves under cyberattack. A trio of hackers in China had snuck into the firms' computer networks by tricking partners into revealing their email passwords," Fortune reported. The hackers discovered information on upcoming mergers and used it to their advantage when trading stocks.

Therefore, it's no surprise that 85% of large companies invest in employee training, according to the Clutch survey.

SMEs, as we've covered, often don't even know where to start, making employee education more challenging, unless they're one of the few that have enough experts on the team, and enough bandwidth to handle necessary training.

Cybersecurity Team Development

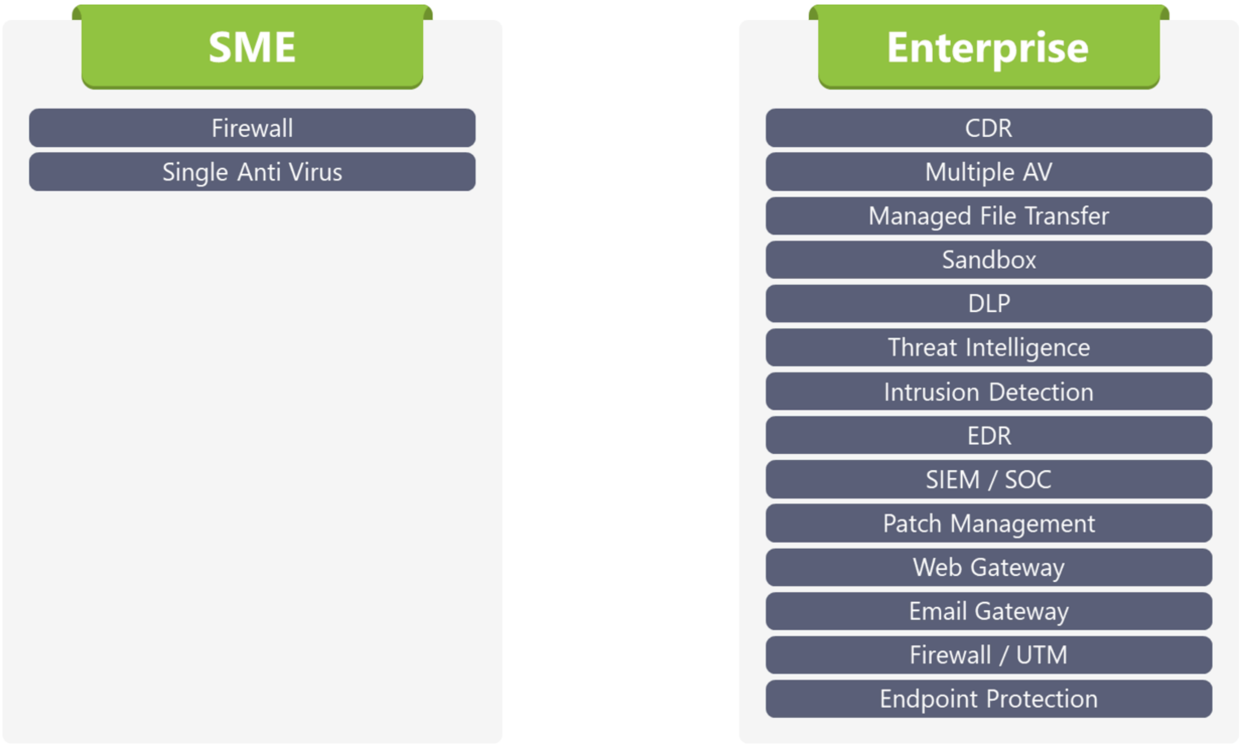
Only one in three SMEs has any IT employees, and 75% only have one or two, reported Baseline. Lack of awareness and limited budgets play a big part here, but cybersecurity team development is a challenge for large companies too.

A 2017 survey by Trustwave and Osterman Research, revealed that 57% of security decision makers "say finding and recruiting IT talent are their biggest challenges," and 36% "say turnover is higher among IT security professionals than in other parts of the organization." In addition, a 2017 Cybersecurity Ventures report predicted that "nearly 3.5 million cybersecurity jobs will be left vacant by 2021," according to Women2.

Investment in Cybersecurity Tools

Large companies already use many cybersecurity tools to secure each component of their network, endpoints and servers, and Clutch added that more than 70% planned to increase their investment in cybersecurity.

On the other hand, as we see in the image, many SMEs can't afford robust tools – and are often unaware of these tools' necessity – so they usually purchase only one or two basic tools.



SME

- Firewall
- Single Anti Virus

Enterprise

- CDR
- Multiple AV
- Managed File Transfer
- Sandbox
- DLP
- Threat Intelligence
- Intrusion Detection
- EDR
- SIEM / SOC
- Patch Management
- Web Gateway
- Email Gateway
- Firewall / UTM
- Endpoint Protection

How is Your Company Handling Cybersecurity?

Companies that want to ensure their longevity can no longer sit back and hope for the best. There are just too many vulnerabilities in most companies [link to the vulnerabilities article when it gets published]. It's important to analyze what your specific vulnerabilities are, and start taking proactive actions toward security. Look for the actions that can make the biggest impact in the shortest amount of time, and move up the list from there.