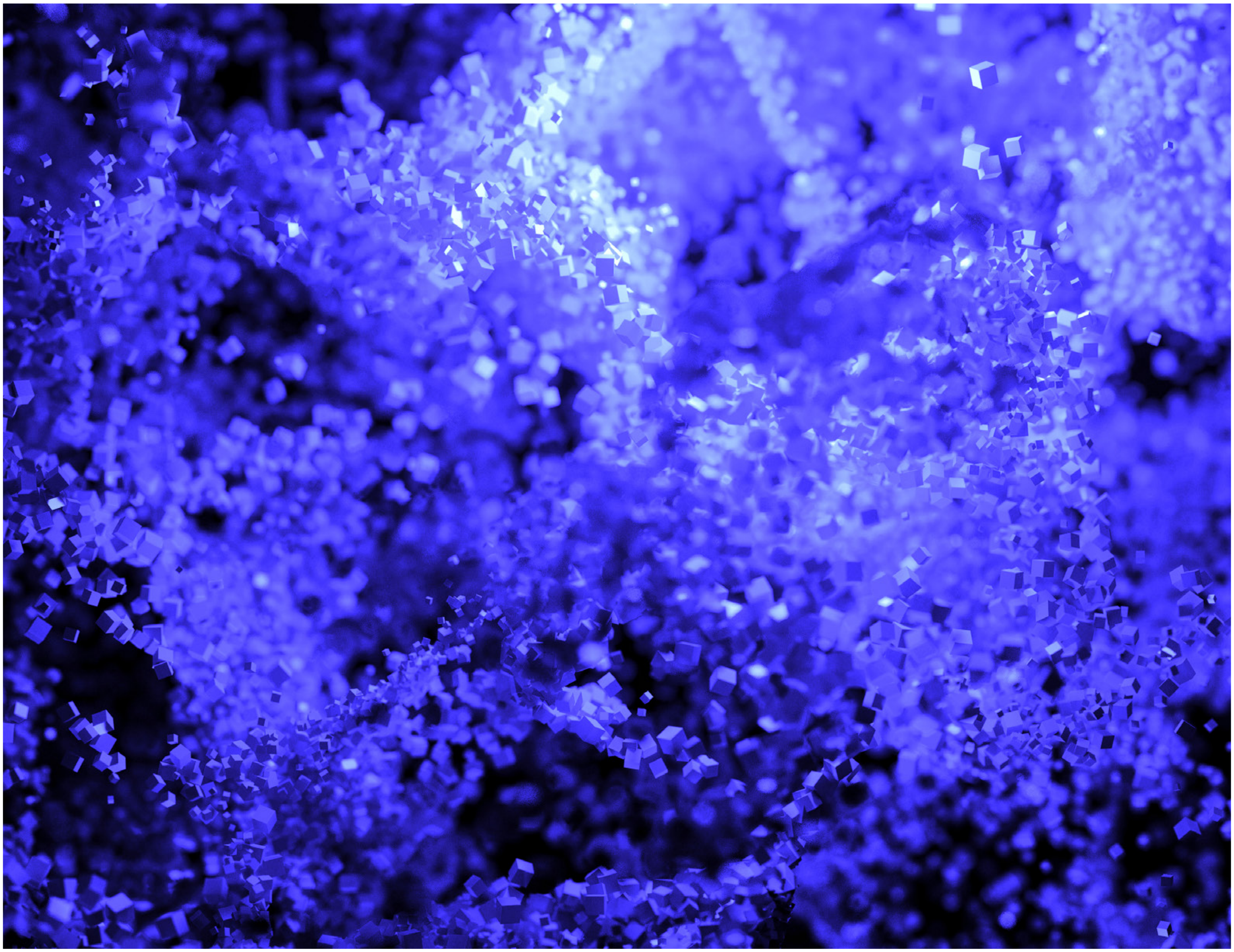
Secureworks®

WHITE PAPER

Advancing Endpoint Security

The importance of threat intelligence, visibility and disrupting the kill chain.



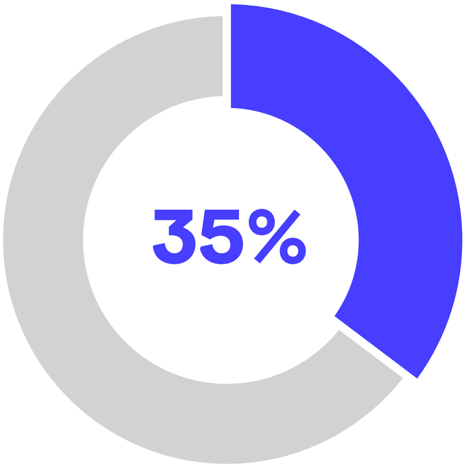
Sixty-nine percent of enterprises polled in Ponemon Institute's 2017 State of Endpoint Security Risk report said their endpoint security risk has significantly increased over the past few years.

To make matters worse, only 31 percent of respondents say traditional solutions, such as antivirus programs that rely on file scanning and signature matching, provides the protection needed to stop serious attacks against their systems, including new and unknown threats. However, IT and IT Security staff must address the tremendous risk posed by inadequate protections on endpoints.[1]

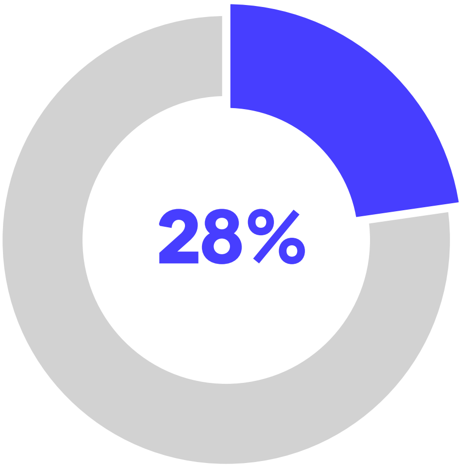
Managing and securing endpoints effectively against today's threats requires companies to mix anti-malware capabilities with a high-level of visibility and behavioral- based detection. By arming itself with these weapons, an organization has a chance to not only detect threat actors and their tradecraft, especially when they employ evasive tactics, but to also slash the amount of time it takes to respond to attacks and minimize the damage they cause.

Perhaps now more than ever, endpoint security requires a comprehensive approach. In this paper, we will discuss how businesses big and small can effectively fight back

2017 Endpoint Risk Entry Point Breaches[2]



Estimated number of file-less attacks against organizations in 2018 - up from 29% in 2017



of companies have kept their current antivirus software and invested in further endpoint protection security solutions

The Problem

There is a famous – if possibly apocryphal – quote from bank robber Willie Sutton, where he supposedly said he robbed banks because "that's where the money is." Whether he actually said that or not, the underlying logic of the quote goes a long way to explaining why attackers are interested in endpoints. They're easy to exploit. Compromising endpoints is how attackers go after corporate data. By targeting endpoints, they can get at the data stored on the machine as well as move through the network and steal information. With the traditional concept of a network perimeter essentially extinct, the importance of a sound endpoint security strategy has never been clearer.

The problem is that protecting the endpoint hasn't been easy. Traditional anti-virus is signature based, which requires that security researchers see something before a signature or countermeasure can be developed. In a sense, there has to be a victim or victims of a given exploit before a protection can be created and applied to a broader population. Of course, this doesn't address the increasing use of evasive tactics such as modifying malware to bypass these traditional controls or the threat actor who leverages tools native to the target's environment.

The Path of Least Resistance

Like any other intruder, a hacker will look for the easiest way into the network first and foremost. After all, why use a zero-day when a two-year-old vulnerability exploit will do? There is nothing new about an attacker going after low-hanging fruit. What is interesting is some threat groups are not using malware very extensively or at all. Hackers increasingly "live off the land" – they use legitimate tools in the environments they compromise to move laterally throughout the network, exfiltrate data, and even get back into the network should the attack be discovered and their access terminated. This is not a challenge easily addressed without understanding how attackers do what they do once they are on a system. Without that level of intelligence on threat actor activity and behavioral-detection capabilities on the endpoint, businesses cost themselves time and money by increasing the amount of time it takes to detect and respond to an attack.

Threats Are Growing More Sophisticated

While not all attackers rely heavily on malware, malware writers remain prolific, and their creations continue to pound endpoints relentlessly. The avalanche of attacks also has been bolstered by an increasing amount of more sophisticated threat activity. These attacks tend to be targeted, and often will use specialized or modified tradecraft to bypass normal security controls such as firewalls and antivirus. In fact, it is common for malware authors to test their creations against popular security software to see if it is detected.

The Solution

Catching Bad Behavior

As tactics, techniques and procedures used by threat actors have become more sophisticated, stopping attackers has become less about signature-based detection and more about identifying malicious behavior. By focusing on attacker activity and not just known threats, organizations can identify attackers living off the land as well as zero-day threats.

Certain actions can serve as red flags. For example, network connection data that indicates a host may be sending or receiving unusual communications can be a sign of data theft or command and control activity. By detecting system changes and looking for behavior such as DNS lookups, companies can begin to get ahead of adversaries who already managed to penetrate their networks.

Continuous Visibility

Protecting endpoints requires 24x7 visibility into the activities taking place on those endpoints. This is not only a requirement for detecting potentially malicious activity, but it also helps forensic investigators piece together how an attack unfolded once a breach has been detected. When a company is attacked, there are a number of questions that enterprises need to be able to answer:

- How and where in the environment did the attack start?
- How many systems have been impacted?
- Has data been successfully exfiltrated from the environment?
- How can the same type of attack be prevented at this company in the future?

Answering these questions will speed incident response and, ultimately, remediation. With high levels of visibility, investigators can pinpoint the entry point of the attackers and close the hole or holes they were able to walk through. Understanding what the attackers did once they entered the network is critical for a company to improve its security posture after a breach.

The Importance of Threat Intelligence

The more that is known about potential attackers, their motivations and their methods, the more organizations can focus on telltale signs of malicious activity that may otherwise slip under the radar. For example, it is not uncommon for threat actors to use unique malware that is unknown to antivirus vendors. Knowing how attackers move throughout a network – for example, targeting certain services – can allow organizations to keep an eye on seemingly innocent behavior that is actually masking malicious intent.

The key word is context. Threat intelligence links the activity businesses see to the larger picture. Without that, closing the door on attackers once they have been evicted can be tricky. For example, Secureworks Counter Threat Unit™ (CTU™) researchers have monitored one particular threat group that will typically attempt to re-enter a network when they were evicted by brute forcing remote access services. Being unaware of this tactic could easily result in one of the group's victims thinking they had closed the door on the hackers by cleaning malware when, in fact, they had not – a potentially deadly mistake against a group linked to attacks against dozens of organizations.

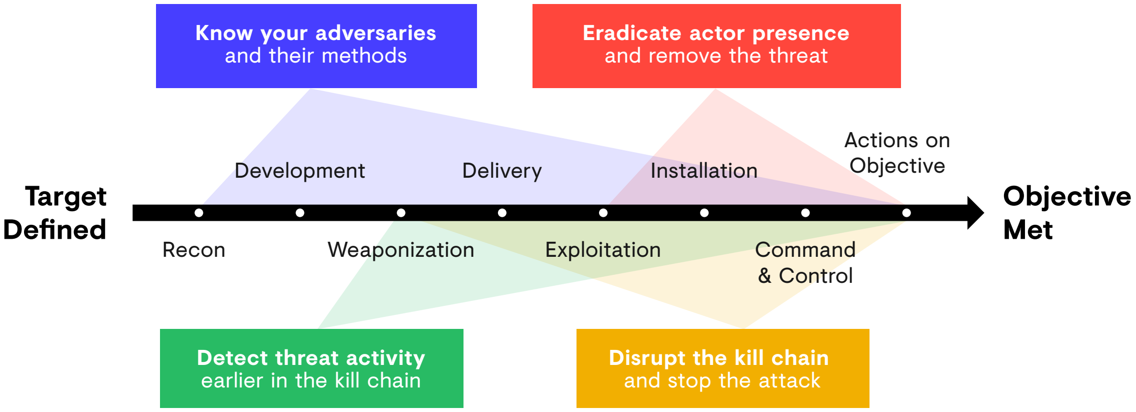
Continuous monitoring of threat groups is just as important as monitoring the devices themselves. By combining threat intelligence with other security capabilities such as IPS/IDS, log analysis and advanced malware detection capabilities, organizations can begin to answer a number of additional questions that complement an analyst's understanding of a threat detected at the endpoint-level:

- Who the attackers may be and how do they operate, including what tradecraft they prefer to use?
- What are some other tradecraft (tactics, techniques and tools including other malware) security staff may want to look for in the environment?
- What is the threat actor's ultimate objective or goal?
- If they still have access to the network, how do you get them out?
- How do you prevent the attackers and others like them from entering your network again?

The key word is context. Threat intelligence links the activity businesses see to the larger picture. Without that, closing the door on attackers once they have been evicted can be tricky.

Disrupt the Kill Chain Sooner

Bringing all this information together to protect the endpoint underscores one basic reality: getting into the network is only one part of the battle for the attacker. In reality, security defenders have multiple opportunities to stop hackers from succeeding in their goals, even after malware has managed to bypass security systems and get on an endpoint. These opportunities present themselves in what is known as the Cyber Kill Chain, the multi-phase process of how adversaries launch successful attacks. Originally conceived of by Lockheed Martin, Secureworks employs its own version of the Kill Chain based on its extensive visibility, experience and intelligence. This iteration includes eight steps: reconnaissance, development, weaponization, delivery, exploitation, installation, command and control and actions on objectives. To win the battle against an intruder, organizations need only to disrupt one of these steps. The earlier in the Kill Chain this can happen, the better.

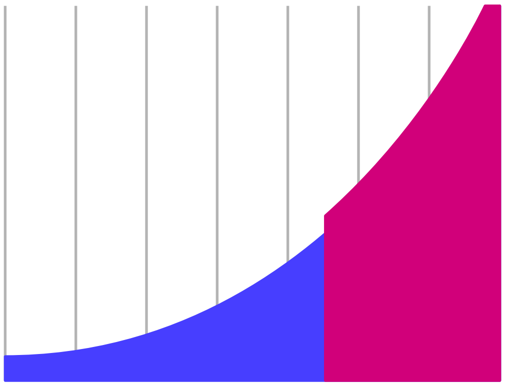


This is one of the reasons why threat intelligence is so important. By applying contextual information about the attack – the malware being used, the way the attackers went about stealing credentials and data, etc. – organizations will be able to get a leg up on hackers even if they have already gotten inside.

Lowering the Cost to Correct the Problems

While all of these capabilities sound nice, the reality is that security risk management also involves executives considering how much they are willing to spend. A CIO or CISO needs to be able to make a case for a budget. The good news is that these capabilities can actually save businesses money, first and foremost, by helping organizations detect an attack and limit its impact. Depending on the intensity of the attack and how much damage was done, it can take IT security professionals months to remediate and patch the environment to close the holes that let the attacker in in the first place. By using the correct methods to detect, deal with and prevent these problems, the cost of addressing these issues can be greatly reduced.

Cost to Resist



Lateral Movement

Costs begin to rise at a more pronounced rate as soon as the actor expands beyond the endpoint into the environment.

Remedial Razor

Costs to remediate experience a step function and subsequent steeper cost curve once exfiltration occurs.

Three Things You Want Your Endpoint Security Solution to Do

1. Detect malware and other tradecraft a threat actor may use, as well as detect behaviors that suggest the presence of a threat actor in your environment when they effectively live off the land.
2. Reduce the response and detection time for attacks, and lower the effort and cost in fixing them.
3. Greater context into the motives and identities of the attackers so that new threats by them and others like them can be more easily addressed — and even prevented — in the future.

Conclusion

Organizations now have compelling options for addressing the substantial risk posed by threats that target their employees and endpoint devices. By using a mix of threat intelligence, endpoint device monitoring and behavioral threat detection, organizations can position themselves to keep digital intruders at the gate and kick them out of the castle if they manage to get in.

Sources:

[1-2] https://cdn2.hubspot.net/hubfs/468115/Campaigns/2017-Ponemon-Report/barkly-2017-state-of-endpoint-security-risk-ponemon-institute-final.pdf?t=1536584055324

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

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
www.secureworks.fr

Germany

Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom

UK House, 180 Oxford St
London W1D 1NN
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

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
www.secureworks.com.au

Japan

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