Securing Endpoints Is the Future Of Cybersecurity

IMPACT SUMMARY:

- 86% of all breaches are financially motivated, where threat actors are after company financial data, intellectual property, health records, and customer identities that can be sold fast on the Dark Web
- 70% of breaches are perpetrated by external actors, making endpoint security a high priority in any cybersecurity strategy
- 55% of breaches originate from organized crime groups
- Attacks on Web apps accessed from endpoints were part of 43% of breaches, more than double the results from last year

---

Why Securing Endpoints Is The Future Of Cybersecurity

Louis Columbus, Senior Contributor
Enterprise & Cloud

Additional Research by: Karl Norris
DUOLARK

The following is a summary of the Verizon Data Breach Investigation Report 2020 (DBIR). It is one of the most read and referenced data breach reports in cybersecurity. Verizon's DBIR, is considered the definitive source of annual cybercrime statistics. Verizon expanded the scope of the report to include 16 industries this year, also providing break-outs for Asia-Pacific (APAC); Europe, Middle East and Africa (EMEA); Latin America and the Caribbean (LAC); and North America, Canada, and Bermuda, which Verizon says is experiencing more breaches (NA).

The study's methodology is based on an analysis of a record total of 157,525 incidents. Of those, 32,002 met Verizon's quality standards, and 3,950 were confirmed data breaches. The report is based on an analysis of those findings. Please see Appendix A for the methodology.

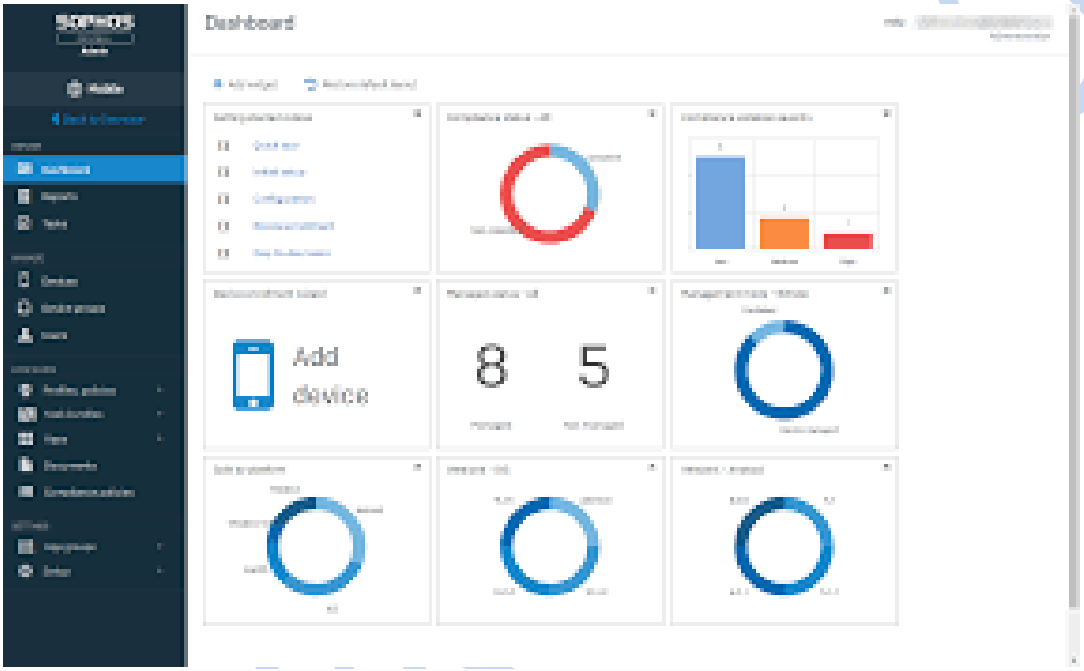
Key insights include the following:

- **RISK OF WORKING REMOTELY FROM HOME** = Verizon's DBIR reflects the stark reality that organized crime-funded cybercriminals are relentless in searching out unprotected endpoints and exploiting them for financial gain, which is why autonomous endpoints are a must-have today. After reading the 2020 Verizon DBIR, it's clear that if organizations had more autonomous endpoints, many of the costliest breaches could be averted. Autonomous endpoints that can enforce compliance, control, automatically regenerating, and patching cybersecurity software while providing control and visibility is the cornerstone of cybersecurity's future. For endpoint security to scale across every threat surface, the new hybrid remote workplace is creating an undeletable tether to every device as a must-have for achieving enterprise scale.

Securing Endpoints Is the Future Of Cybersecurity

- **<u>CONTINUOUS MONITORING NETWORK ASSETS, ACTIVITIES AND ALERTS</u> =** The lack of diligence around Asset Management is creating new threat surfaces as organizations often don't know the current health, configurations, or locations of their systems and devices. Asset Management is a black hole in many organizations leading to partial at best efforts to protect every threat surface they have. What's needed is more insightful data on the health of every device. There are several dashboards available, and one of the most insightful is from SOPHOS called the Sophos Management Console.

,



- **<u>FOCUS – FOCUS – FOCUS</u> =** 85% of victims and subjects were in the same country, 56% were in the same state, and 35% were even in the same city based on FBI Internet Crime Complaint Center (IC3) data. Cybercriminals are very opportunistic when it comes to attacking high-profile targets in their regions of the world. Concerted efforts of cybercriminals funded by organized crime look for the weakest threat surfaces to launch an attack on, and unprotected endpoints are their favorite target. What's needed is more of a true endpoint resilience approach that is based on a real-time, unbreakable digital tether that ensures the security of every device and the apps and data it contains.

- **<u>LOOK FOR THIS TO CHANGE IN THE 2021 REPORT</u> (*Protect Endpoints Now*)** = Cloud assets were involved in about 24% of breaches this year, while on-premises assets are still 70%. Ask any CISO what the most valuable lesson they learned from the pandemic has been so far, and chances are they'll say they didn't move to the cloud quickly enough. Cloud platforms enable CIOs and CISOs to provide a greater scale of applications for their workforces who are entirely remote and a higher security level. Digging deeper into this, cloud-based Security Information and Event Management (SIEM) provides invaluable real-time analysis, alerts, and deterrence of potential breaches. Today it's the exceptional rather than the rule that CISOs prefer on-premise over cloud-based SIEM and endpoint security applications. Cloud-based endpoint platforms and the apps they support are the future of

Research by: Karl Norris | DUOLARK Founder & CEO
For more information please contact us (954) 324-3478 | info@duolark.com | www.duolark.com
June 18, 2020

cybersecurity as all organizations now are either considering or adopting cloud-based cybersecurity strategies.

- **IT IS NOT THE HACKERS, IT IS THE HACKERS ACTING LIKE THEY ARE YOU.** Over 80% of breaches within hacking involve brute force or the use of lost or stolen credentials. One of the most valuable insights from the Verizon DBIR is how high of a priority cybercriminals are placing on stealing personal and privileged access credentials. Shutting down potential breach attempts from stolen passwords involves keeping every endpoint completely up to date on software updates, monitoring aberrant activity, and knowing if anyone is attempting to change the configuration of a system as an administrator. By having an unbreakable digital tether to every device, greater control and real-time response to breach attempts are possible.

Summary Conclusion

Self-defending endpoints that can self-heal and regenerate operating systems and configurations are the future of cybersecurity, a point that can be inferred from Verizon's DBIR this year. While CIOs are more budget-focused than ever, CISOs are focused on how to anticipate and protect their enterprises from new, emerging threats. Closing the asset management gaps while securing every endpoint is a must-have to secure any business today. There are several cybersecurity companies offering endpoint security today DUOLARK is one of them.

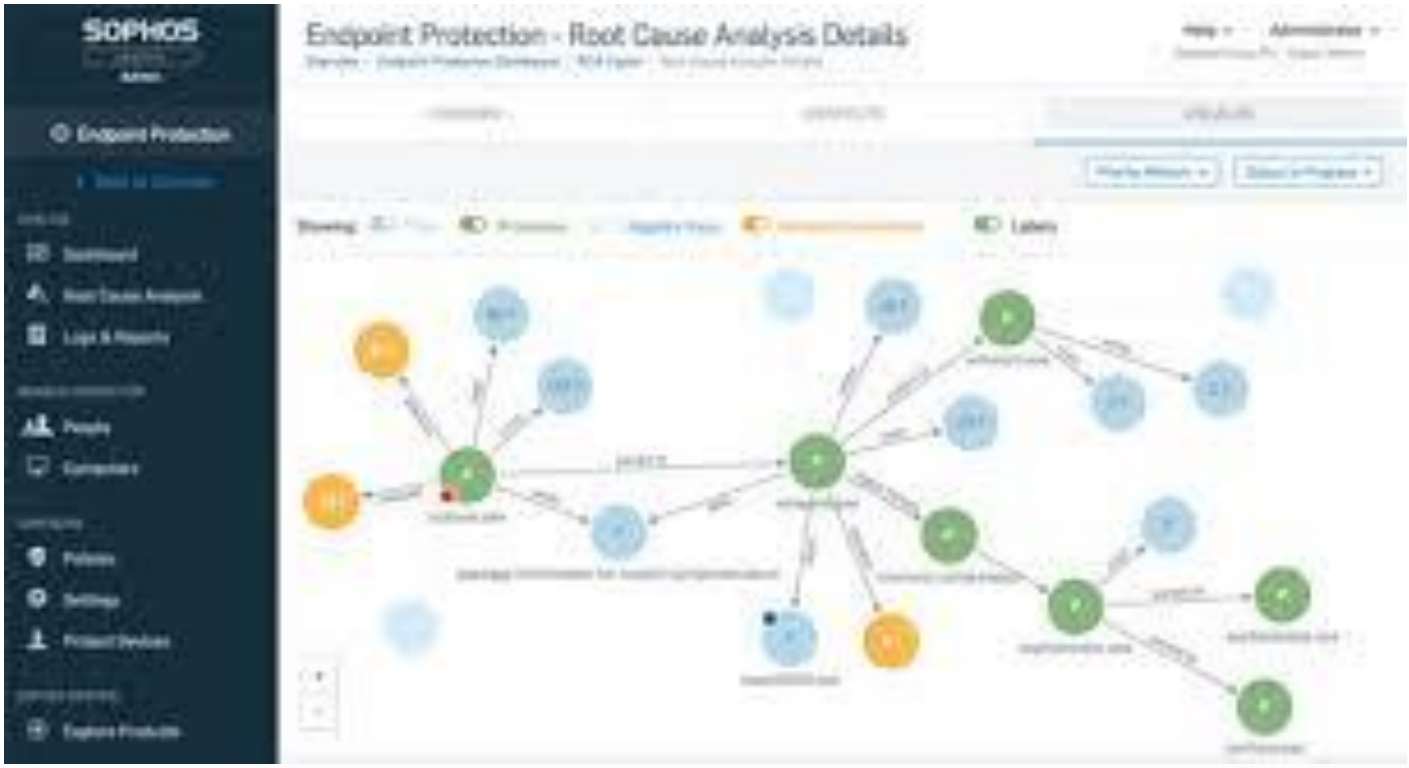
How To Turn Your Network Into A Self Defending Network Protect All Your DATA And Your EMPLOYEES

DUOLARK's SOLUTION: SELF HEALING / SELF DEFENDING NETWORKS = Using AI Neural network technologies we blend a solution together that is synchronized smart. It can tell if there is someone trying to attack the network. Before the attacker is successful the endpoint defends itself by disconnecting from the network. It still is capturing information on what the intruder is attempting to do to it. The network is alerted, the network engineers are alerted. They can then simply address the issue that has been isolated. This is really smart. It gets better. We can then run a "Root Cause Analysis" on the entire system and find out if there are other similar vulnerabilities. We can also look at what led up to the attack being initiated. In some cases, we can find out exactly who the attacker was and deal with it accordingly. With the number of remote workers being deployed, and the lax security we can help stop data leakage. It is normally not the employee. It is the environment.

IF THERE IS AN ISSUE, WE CAN FIND OUT WHAT HAPPENED?

We can find out what the Root Cause of the problem was. By using neural network AI we can recreate what happened. Below is an example of how DUOLARK and SOPHOS Team up together to do Root Cause Analysis. We can show weak points based on the exploit. Strengths where endpoints are safest. Then where did the exploit occur, what did it take to remediate it, and in some cases evidence to present to law enforcement.

Securing Endpoints Is the Future Of Cybersecurity



Who's Watching The Watcher?

We offer a free assessment of your network. We want to provide you with a unique concept.

For more information contact us today and we can set up a conversation, a Zoom / Team Meeting, or practicing proper Covid-19 precautions. We will even set an appointment to visit you on your site.

SOMETHING NEW FOR HELPING TO STOP THE SPREAD OF COVIS-19

RISK MANAGERS! COVID-19 DUAL RAPID ANTIBODY TESTS AVAILABLE:

We also can work with you to test your employees at work, at home, and at a physician's office to find out if they have Covid-19 antibodies. These tests take only 15 minutes to know if your employee may have Covid-19 antibodies already. That opens up many possibilities. Test – Test – Test and together we can slow the spread of Covid-19 until there's a vaccination or until there's enough people with anti-bodies that we can work normally again. Get ahead of the curve while supplies are available.
www.duolark.com/business-returns-to-work

Research by: Karl Norris | DUOLARK Founder & CEO
For more information please contact us (954) 324-3478 | info@duolark.com | www.duolark.com

Links to more about Covid-19 antibody testing:

DUOLARK – Home – look for more information on your specific industry and COVID-19 solutions
https://duolark.com

DUOLARK – Back To Business Safely
https://duolark.com/business-returns-to-work

What's Being Said By Others About DUOLARK's Covid-19 Rapid Tests

https://southfloridahospitalnews.com/page/DUOLARK_Covid19_Rapid_Dual_Tests_10_minutes_for_results_Approved_for_Laboratory_and_Healthcare_Professionals_Businesses_and_/16236/25/

For more information please contact us at:

DUOLARK

www.DUOLARK.com

(954) 324-3478

info@duolark.com