G2M RESEARCH

Endpoint Security Market Pulse Newsletter

May 2020

Even Joe Exotic's Data is Worth $250-$300

Whether you are gaming, in a zoom meeting, exchanging emails and text, or proclaiming Carol Baskin killed her husband, your data is worth money. Even the average Joe's data is worth $250-$300 according to cyber security expert Ryan Cloutier.

Hackers access that data by any means possible, from computer to phone to routers to gaming systems. COVID-19 has provided an opportunity for hackers to exploit fear and a desire for the latest medical and stay-in-home requirements. Scammers pose as professionals from charitable organizations, people selling COVID-19 protective gear, as high-ranking members of your employer, even as representatives from WHO.

Update all your devices and upgrade your router if it is over five years old. Set up two Wi-FI logins, with a guest network, putting your sensitive devices on one and less sensitive devices on the other. Don't click email links. Do not fall for the COVID19 tax refund email scam. Use passwords for video conferencing. Zoom is a big target, as we highlighted in our April newsletter. Find specific recommendations for securely using Zoom here.

> *"Having devices that are not up to date is equal to leaving the windows and doors of your home open and then leaving."* Ryan Cloutier, CISSP

Think about it this way- remote learning may be here for quite some time, so children are using many different platforms for learning, including those outside that provided or suggested by the school itself. A hacker with access to a child's data may not be discovered for years. Hackers steal W2 date to file false tax returns using that stolen identity from staff and students.

As Greg Stockstill, Cybersecurity State Lead for 12 State ESCs cautions "the younger a student is, the more their information is worth on the dark web" because "It could be 12 years of someone using that identity before anyone knows that it was stolen." Funny to consider Joe Exotic's personal data being sold; not so funny to consider your first grader's identity being stolen.

Is Endpoint Security Infrastructure Equipped to Withstand Cyber Attacks Directed at Exploiting COVID-19?

As first responders rushed to treat pandemic victims, amid concerns about adequate ventilators, masks, and even beds, cybercriminals acted relentlessly in exploiting this health care emergency to attack pandemic resource infrastructure, including hospitals. Hospitals, in particular, operate on thin margins, and don't invest the hefty resources necessarily to combat cybersecurity attacks. As Erik Decker, Chief Security and Privacy Officer at University of Chicago Medicine explains, "A dollar that goes to administration is a dollar that doesn't go to care"—adding that many smaller systems don't even have IT security personnel.

Cyberattacks in healthcare range from ransomware and email phishing to medical device attacks. Moving nonessential workers to working from home with remote access opens the door to more exploits.

Organizations need segmented networks with two-factor authentication using VPNs. VPN adoption has increased significantly- one step in the right direction. But, with resources stretched thin, suspect activity may not be monitored as closely as it would be otherwise. As Caleb Barlow, CEO of CynergisTek, explains, "You'd be astounded at how many people have no locks on the endpoint." Sometimes, the easiest, most readily available fixes, such as a Microsoft patch in the case of the 2017 WannaCry ransomware attack, are all that stand between security and disaster.

A fabulous result of the pandemic, for consumers, has been the opportunity for in-person, teleconference doctor's appointments. No commute, time in the waiting room, no exposure to sick people, no wait in the examination room… efficiency at its finest. However, the Department of Health and Human Services temporary enforcement discretion for telehealth creates a situation ripe for breaching every medical privacy protection. Zoom is not HIPAA compliant but is free. Zoom for Healthcare is HIPAA compliant but there is a charge. With thin margins, medical urgency, no time to put protocols in place, the situation is perfect for privacy breaches.

"Any new connected device expands IoT attack vectors; cyber-attackers are exploiting the global crisis, and hardening device security is critical. In the case of connected medical devices, security risks can be life impacting. The pandemic is changing the way we work today, but it will also shift the industry moving forward. Manufacturers must pivot their capabilities and the way they design, develop and test remotely; these new processes may mean more automation on factory floors and the introduction of smart control systems that reduce human interaction. This is the reality today, and companies will have to accept it as a long-term scenario." Ellen Boehm, Senior Director of IoT product management, Keyfactor.

Healthcare providers need every second available to save lives, not to worry about cybersecurity. Let's help healthcare providers and protect every electronic device they rely on.

70% of Successful Network Breaches Start on Endpoint Devices

… and, they are an effective entryway for taking down the entire network. The average time to detect a breach for an enterprise is about 8 months, plus over 2 months to contain it. EDR and EPR have provided some protection for endpoints but EDR is limited to endpoint traffic and cannot help once an attack moves beyond the perimeter. More complete centralization to address these issues can be partially accomplished by integrating EDR solutions with system information and event management solutions (SIEM) but requires management of two tools. Another option is XDR, extended detection and response, which expands on EDR by collection data from more sources providing information for more comprehensive analysis and allows tracking of attacks no matter where the attack is happening in the system.

Also, many organizations simply do not have adequate personnel to respond to alerts. MDR, managed detection and response, cloud-based approach can provide alert prioritization for those entities.

It's time to get smart. To move beyond intelligence,
because the way it's always been shouldn't always last.
It's time to ask, can we act in time to change the future?
Steven Grobman, Sr VP & CTO, McAfee

In Steven Grobman's keynote at RSA he emphasizes the need for companies to consider how long data will need to be protected. "Nation-states will use quantum computing to break our public key encryption systems," he said. "Our adversaries are getting the data today and counting on quantum to unlock in tomorrow."

His urgency and warning were reminiscent of a blog two years earlier, highlighting the AI threats and opportunities he presented to that year's RSA crowd:

"The key to successfully unlocking the potential of AI in cybersecurity requires that we in the cybersecurity industry answer the question of how we can nurture the sparks of AI innovation while recognizing its limitations and how it can be used against us.

We should look to the history of key technological advances to better understand how technology can bring both benefits and challenges. Consider flight in the 20th century. The technology has changed every aspect of our lives, allowing us to move between continents in hours, instead of weeks. Businesses, supply chains, and economies operate globally, and our ability to explore the world and the universe has been forever changed.

But this exact same technology also fundamentally changed warfare. In World War II alone, the strategic bombing campaigns of the Allied and Axis powers killed more than two million people, many of them civilians.

The underlying technology of flight is Bernoulli's Principle, which explains why an airplane wing creates lift. Of course, the technology in play has no knowledge of whether the airplane wing is connected to a 'life-flight' rescue mission, or to a plane carrying bombs to be dropped on civilian targets.

When Orville Wright was asked in 1948 after the devastation of air power during World War II whether he regretted inventing the airplane he answered:

"No, I don't have any regrets about my part in the invention of the airplane, though no one could deplore more than I do the destruction it has caused. We dared to hope we had invented something that would bring lasting peace to the earth. But we were wrong. I feel about the airplane much the same as I do in regard to fire. That is, I regret all the terrible damage caused by fire, but I think it is good for the human race that someone discovered how to start fires, and that we have learned how to put fire to thousands of important uses."

Orville's insight that technology does not comprehend morality—and that any advances in technology can be used for both beneficial and troubling purposes. This dual use of technology is something our industry has struggled with for years."

History Hit, May 27, 1937 - In San Francisco, 200,000 people celebrated the grand opening of the Golden Gate Bridge by strolling across it.

Not allowed in 2020 unless spaced 6 feet apart.

Upcoming 2020 Security Events

National Cyber Summit- June 2-4

Keynote Speakers- Jon "Mad Dog" Hall- Board Chair, Linux Professional Institute
Major General Thomas Murphy, Director of DoD's Protecting Critical Technology Task Force, Air force
Robert Powell, Senior Advisor for Cybersecurity, NASA

SANSFIRE 2020- June 13-20 (Virtual Event)

SANS provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats- the ones being actively exploited.

If you missed our May 19 webinar “Utilizing HPC-Scale Storage and AI for Business Intelligence” with sponsors WekaIO, Samsung, Datyra, and NVIDIA/Mellanox Technologies, you can see it here. Interested in Sponsoring a webinar? Contact **us** for a prospectus. Interested in attending our webinars? Register by clicking below on the dates of interest.

G2M RESEARCH

- **July 21**: AV, Self-Driving Cars, and Advanced Storage
- **September 15**: Edge Computing/Storage – Get (and Keep) Your Data Off Of My Cloud
- **October 20**: AI and Storage Use Cases in Healthcare
- **November 17**: NVMe-oF™ - Using Telemetry to Improve Network Latency

G2M
COMMUNICATIONS
Effective Marketing & Communications with Quantifiable Results

Endpoint Security Newsfeed

Endpoint Security Market Worth $18.6 billion by 2027- Pre & Post COVID-19 Market Estimates by Meticulous Research(R)
London, May 19, 2020 (GLOBE NEWSWIRE) -- According to a new market research report titled, "Endpoint Security Market by Component, Enforcement Point (Workstation, Mobile Devices, Server, Point of Sale ...

MarketWatch6d

Best endpoint protection software of 2020: internet security for business

Endpoint security software aims to bring together all cyber security and privacy controls for business PCs into a single management dashboard. This means everything from a standard firewall to ...

TechRadar4d

FireEye enables orgs to respond to security incidents faster with flexible and customizable modules

FireEye, the intelligence-led security company, introduced a new Innovation Architecture behind FireEye Endpoint Security.

Help Net Security4d

Better Endpoint Security Improved Security and Lowers Operational Costs

Computerworld covers a range of technology topics, with a focus on these core areas of IT: Windows, Mobile, Apple/enterprise, ...

Computerworld3d

Endpoint Security Market Size, Industry Share and Total Revenue Growth Rate Till 2026 | Fortune Business Insights

As per a recent report, organizations have reported more than 15% of endpoint attacks as compared to the last year.

MarketWatch10d

Real Time Matters in Endpoint Protection

The new generation of endpoint detection and response (EDR) solutions is not only able to detect threats, but also immediately defuse them to stop attackers from achieving their goals in real-time.

CSOonline4d

FireEye Endpoint Security: Introducing Innovation Architecture for Rapid Deployment of Advanced Capabilities

And traditionally, the time that the industry took to respond with the creation, testing and deployment of new features has been too long," said Michelle Salvado, Vice President of Engineering and ...

Dark Reading4d

VMware Security- One Of The Best Kept IT Secrets

Patrick Moorhead dives in as he recently got the chance to attend an analyst briefing held by VMware senior executives to ...

Forbes5d

Jamf Protect adds new macOS malware prevention capabilities to its endpoint security solution

Jamf Protect is launching a handful of new features aimed to continue simplifying the endpoint security on macOS for IT ...

9to5Mac4d

With latest acquisition and alliance, VMware seeks differentiation from endpoint security players

With latest acquisition and alliance, VMware seeks differentiation from endpoint security players - SiliconANGLE ...

SiliconANGLE11d

CrowdStrike Falcon Expands Linux Protection with Enhanced Prevention Capabilities

CrowdStrike® Inc. (Nasdaq: CRWD), a leader in cloud-delivered endpoint protection, today announced the CrowdStrike Falcon® ...

Business Wire4d

Endpoint Security Market Worth $18.6 billion by 2027- Pre & Post COVID-19 Market Estimates by Meticulous Research®

According to a new market research report titled, "Endpoint Security Market by Component, Enforcement Point (Workstation, ...

Benzinga.com6d

Aruba and Microsoft provide security solutions to improve security and IT team collaboration

Aruba ClearPass Policy Manager integrates with Microsoft endpoint protection platforms to deliver significant advances in ...

Help Net Security13d

Aruba Collaborates with Microsoft to Advance Enterprise Cyberattack Protection

Technology Integration Provides Advanced Security Solutions to Improve Security and IT Team Collaboration Sydney, Australia – Aruba, a Hewlett Packard Enterprise company (NYSE: HPE) announced the ...

cmo.com.au23h

Endpoint security insights highlighted by coronavirus outbreak

Absolute's insights reveal sustained gaps in endpoint health and security, and a high number of Windows 10 devices not being patched.

ITWeb5d

CrowdStrike Falcon bolsters Linux protection with ML prevention, custom and dynamic IoAs

CrowdStrike Falcon platform is bolstering its Linux protection capabilities with additional features, including ML prevention ...

Help Net Security4d

Security Analytics Market In Depth Analysis By Total Revenue And Industry Growth Rate Forecast Till 2026

The global security analytics market size is projected to reach USD 28.55 billion by 2027, exhibiting a CAGR of ...

MarketWatch6d

Bitglass Integrates CrowdStrike’s Machine-Learning Technology to Provide Zero-Day Advanced Threat Protection in the Cloud

Gen Cloud Security Company, announced today that it has partnered with CrowdStrike®, a leader in cloud-delivered endpoint ...

Business Wire13d

Octarine Acquisition to Boost VMware’s Kubernetes Security Play

VMware’s acquisition of the Kubernetes security startup Octarine reflects a shift in cybersecurity, driven by ...

Data Center Knowledge5d

Changing workplaces: Telecommuters need security too

As users stuck at home try to solve productivity challenges, the amount of shadow IT gaps increases. Hackers are already ...

Digital Journal13d

Cyber Security Market Global Analysis, Opportunities and Forecast To 2025

The cyber security market is segmented on the lines of its type, solution, service and vertical analysis. The cyber security market is segmented on the lines of its type like network security, ...

MarketWatch7d

SafeBreach Enhances Microsoft Defender Advanced Threat Protection Evaluation Lab With Advanced Attack Simulations

Today SafeBreach announces integration of its attack technique simulations into the Microsoft Defender Advanced Threat Protection (ATP) evaluation lab, offering friction-free access to SafeBreach's ...

Business Insider5d

Cyber Security Market 2019 - Challenges, Drivers, Outlook, Growth Opportunities - Analysis to 2025

The scope of the report includes a detailed study of global and regional markets for various types of cyber security with the reasons given for variations in the growth of the industry in certain ...

MarketWatch11d

How To Build A Business Case For Endpoint Security

Think of building a business case for endpoint security as the checkup every company needs to examine and identify how every ...

Forbes15d

Smart Grid Security Industry 2020 to 2026 by Manufactures Types, Applications, Market Size, Regions and Forecast to 2026

Final Reports will add the analysis of the impact of COVID-19 on this industry” Global “Smart Grid Security ...

MarketWatch4d

COVID-19 Impact and Recovery Analysis | Endpoint Security Market 2020-2024 | Increasing Incidence of Cyberattacks to Boost Growth | Technavio

Technavio has been monitoring the endpoint security market and it is poised to grow by USD 8.90 billion during 2020-2024, ...

Business Wire18d

Endpoint Security Market to See Major Growth by 2025: Carbon Black Inc., McAfee LLC, Symantec Corporation, Sophos Group PLC, Bitdefender LLC

Endpoint Security Market is valued at USD 11,723.84 Million in 2018 and expected to reach USD 29,156.53 Million ...

MarketWatch21d

Marketopia: 3 Steps for MSPs to Sell DNS Protection

Threats are everywhere, and endpoint security simply isn’t enough to keep your clients safe. Pairing domain name system (DNS) ...

CRN13d

Endpoint Protection Market in depth Research about Market Trends & Competitive Landscape with key players McAfee, ManageEngine, AVG

Advance Market Analyticsreleased the research report of Global Endpoint Protection Market, offers a detailed overview of the factors influencing the global business scope.Global Endpoint Protection ...

MarketWatch14d

CrowdStrike Has Highest Rating Among Vendors Named in May 2020 Gartner Peer Insights ‘Voice of the Customer’ for Endpoint Detection and Response Solutions Re…

CrowdStrike® Inc. (Nasdaq: CRWD), a leader in cloud-delivered endpoint protection, announced it has the highest overall ...

Business Wire18d

Endpoint Security Market Growing at a CAGR 7.6% | Key Player Microsoft, CrowdStrike, Symantec, TrendMicro, McAfee

May 01, 2020 (AB Digital via COMTEX) -- The global Endpoint Security Market size is expected to grow from USD 12.8 billion in 2019 to USD 18.4 billion by 2024, at a Compound Annual Growth Rate ...

MarketWatch24d