SIM2K
Adapting Technology to Your Business Needs

9•22
Information you can use

SIMformation

ThreatLocker Provides Added Security

In this month's issue we're excited to showcase one of our security partners, ThreatLocker. A real-world correlation between the new threat environment is that organizations are increasingly getting pressure from their cyber insurance providers to have more rigorous controls in place. Ransomware, by way of exploiting legitimate software, is still a very real risk. And it's not just the ransomware – organizations are also experiencing the exfiltration of their confidential data which is also held hostage to being released to the news or public dumps.

New threats demand new tools and new approaches to problems. Most tech companies claim to have differentiated offerings, of course. But which vendors actually deliver on their promise of innovation? And deliver in a way that creates major opportunities for partners?

Recently, industry trade magazine CRN published its "Top 25 Innovators of 2022" list where they selected executives that have been bringing true channel-friendly innovation to the market – accelerating digital transformation, enabling new growth opportunities for partners and producing one customer success story after another.

SIM2K is excited to see that the list is topped by Danny Jenkins, Co-Founder, CEO of ThreatLocker. CRN noted:

> *One of the security industry's most innovative visionaries and a true cybersecurity maverick, Jenkins is turning the tide on the barrage of attacks battering MSPs with ThreatLocker's deny by default whitelisting and ringfencing technology.*
>
> *The indefatigable Jenkins stared down the skeptics who scoffed at that technology, which is now being embraced by MSPs and even large enterprises at a breakneck pace.*
>
> *In April alone, ThreatLocker added 700 new MSPs to its community and is on pace to add a total of 3,000 MSPs in 2022.*
>
> *"Ransomware is the biggest threat to any individual MSP, but it is also the biggest threat to the industry as a whole because when one of your peers gets hit by ransomware and it makes the headlines, it makes it harder for MSPs to sell their services to businesses," he told CRN in May. "Once MSPs start treating security with a sense of urgency, the world will be a better place," he said.*

Ben Finegan, president of SIM2K, noted, "In 2020 COVID changed the work-at-home model for most SMB's and remote work exploded. The traditional perimeter vanished. Legitimate software has been weaponized. Organizations need to re-think how they protect at the endpoint (and human) outwards. In this new era, our partnership with visionaries like ThreatLocker enables us to bring that to our clients."

Danny Jenkins told SIMformation, "Small businesses are fighting the same cyber criminals as large corporations without the tools. Through MSPs, ThreatLocker enables small businesses the same levels of security as large corporations without investing hundreds of thousands of dollars into solutions. Zero trust means allowing what is needed in your organization and blocking everything else... including ransomware and putting granular controls over your environment."

SIM2K offers ThreatLocker ZeroTrust protection to our SIM2K Vault and Pinnacle-22 customers as part of their package, and can provide this service to other clients as an added service. The concept behind ThreatLocker's protection covers fivebasic provisions:

Ringfencing™: Controlling what software can run should be the first line of defense when it comes to better protecting against malicious software. Ringfencing adds a second line of defense for applications that are permitted. First, by defining how applications can interact with each other, and secondly, by controlling what resources applications can access, such as networks, files, and registries. Ringfencing is an invaluable tool in the fight against fileless malware and software exploits.

Allowlisting: Allowlisting has long been considered the gold standard in protecting businesses from known and unknown executables. Unlike antivirus, Allowlisting controls what software, scripts, executables, and libraries can run on your endpoints and servers. This approach not only stops malicious software, but it also stops other unpermitted applications from running. This approach greatly minimizes cyber threats by stopping rogue applications from running on your network.

Storage Control: ThreatLocker® Storage Control is an advanced storage control solution that protects information with tools to control the flow and access of data. You can choose what data can be accessed, or copied, and the applications, users, and computers that can access said data. By

continued on page 2

ThreatLocker *(con't)*

using ThreatLocker, you are in control of your file servers, USB drives, and your data. Most data protection programs on the market are butcher knife solutions to a problem that requires a scalpel. Blocking USB drives and encrypting data-storage servers can help secure your organization's private data, but these tools don't take into account that this data still needs to be utilized and quickly. Waiting for approval or trying to find a device that's allowed to access needed files can drain hours of productivity.

Elevation control: When it comes to adding extra layers of security to your cyber security stack, it is important to always add a human layer. Users with admin access are often the weakest link across your network, so their movements must be monitored and tracked. ThreatLockers Elevation Control provides an additional layer of security by giving IT administrators the power to remove local admin privileges from their users, while allowing them to run individual applications as an administrator.

Network Access Control: Network Access Control allows for total control of inbound traffic to your protected devices. Using custom-built policies, you can allow granular access based on IP address or even specific keywords. Unlike a VPN that needs to connect through a central point, the ThreatLocker NAC is a simple connection between server and client. ThreatLocker NAC is built in a way that creates a seamless experience, enabling users to work as normal while eliminating the need for a solution, such as a VPN.

How does this work for you? Here's an example. Ransomware and other malicious software can copy or encrypt your files in a few minutes. ThreatLocker uses a more logical approach to stop viruses and malware from affecting your business. ThreatLocker Application Control uses a combination of Default Deny and Ringfencing to protect your business from known and unknown malware threats such as:

- **Zero-Day Attacks:** ThreatLocker® protects against vulnerabilities that haven't even been discovered yet;
- **Macro Viruses:** Malware embedded in trusted programs like Office can't overcome ThreatLocker's Ringfencing;
- **Fileless Malware:** Even malware that hides in memory can't sneak in; if its code isn't on the trusted list, it isn't getting access; and
- **Ransomware:** Ringfencing lets you dictate how apps interact with data; if a program, ANY program, tries to encrypt data it isn't authorized to, it will be blocked

Application Whitelisting and Ringfencing are considered the gold standards when it comes to stopping ransomware, viruses, and other malicious software. Typically these enterprise-class tools often come with a significant management overhead, long deployment times, and red tape that makes business operations difficult.

SIM2K is a Platinum Partner for ThreatLocker so can bring the full suite of solutions to bear for your company. Contact us for more information on how to incorporate ThreatLocker into your security program.

Hackers Target Healthcare

Last month we discussed how Indiana healthcare companies were being targeted for cybercrimes. Now, a recent study shows that Indiana leads the nation in medical data breaches, with more than 80 million records affected since 2009, followed by New York, Florida, California and Texas..

Much of that was due to one massive incident involving insurance company Anthem Inc. (now called Elevance Health Inc.) in 2015, when hackers obtained data on 78.8 million members and employees. Anthem later agreed to pay $170 million in settlements to federal and state officials and civil plaintiffs for failing to safeguard its data. But more than a dozen other Indiana companies over the years – including Indiana University Health, Hancock Health, Eskenazi Health, Schneck Medical Center and Goodman Campbell Brain and Spine – also suffered large data breaches amounting to tens of thousands of patient records.

Indiana accounted for nearly 25% of all breached records during the 13-year period between 2009 and June 2022, due largely to the Anthem breach, according to a report by Comparitech, a consumer website focusing on cyber security. The report is based on data from the U.S. Department of Health and Human Services breach portal, which stores thousands of hacking reports.

All companies holding medical records are required to report data breaches to the federal government if more than 500 records are affected. Since 2009, medical organizations in the U.S. have suffered nearly 5,000 data breaches, affecting over 342 million medical records.

Cybersecurity experts say health care is a soft target because the sector is a relative latecomer to the digital revolution, and many hospitals and other players have been slow to invest in new software that can stop or slow hackers. By gaining access to sensitive health data, hackers can profit by selling the information on the dark web. Much of the hacked medical data includes Social Security numbers, birthdates and addresses, which hackers can use to steal identities and credit information.

According to the Comparitech report, 2020 was the biggest year for medical data breaches, with 803 incidents reported. Hacking was the most popular method of breaching medical data, accounting for 41% of breaches last year. The next largest category was ransomware, where cyber pirates install malicious software into a database or computer system to block access until a sum of money is paid. Phishing attacks are suspected to be the root cause of many of the ransomware attacks, as medical personnel are not as attuned to watching out for suspect attachments or links as private company employees.

In 2021 and 2022 (so far), specialist medical clinics accounted for the most data breaches in the U.S. (15%), but hospital systems accounted for the most breached records, with 8.8 million affected, or 16% of total records affected.

Certainly not a category to be "Number One" – so more diligent training and awareness should be paramount in the medical field.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Avoiding MFA Fatigue

MFA fatigue cyberattacks exploit the human element of cybersecurity via social engineering. MFA is still a relatively new form of security, especially with authenticator apps – users aren't familiar enough with MFA technology to recognize that an attack is even happening. It's easy to chalk this type of attack up to a bug and keep going about your day.

To initiate an MFA fatigue attack, the hacker needs to have obtained your login credentials already. Cracking passwords is easier than you might think, especially if they're weak. Learn more about creating stronger passwords.

Once the hacker has entered in your login credentials, the system will prompt them to approve the login via MFA. At this point, you'll receive a notification on your mobile device asking you to approve the login. The hacker is counting on your distracted brain or habit of automatically approving logins to gain access to your account. Once you approve the login, they're in.

In more advanced scenarios, a hacker may use an MFA auto-retry script, where the MFA sign-in is sent repeatedly until you inevitably give up and approve the login. In many cases, users think the multiple approvals are just a bug in the system and approve the login to end the nuisance.

Now there is a solution – Verified Duo Push assures that the person requesting a push really is who they say they are and helps stop two of the biggest threats to MFA access control: push harassment and push fatigue:

Push harassment: After a bad actor has compromised the first factor by obtaining a username and password, they persistently initiate push requests until the end-user gives in, approving an unintended push request and compromising the second factor.

Push fatigue: With the growing volume of mobile notifications on a daily basis, users are more likely to blindly approve a push request that only requires a tap to grant 2FA.

Verified Duo Push is being rolled out for SIM2K clients.

How does Verified Duo Push work?

By requiring the manual entry of a verification code, Verified Duo Push helps end-users immediately recognize push requests that they didn't initiate and provide accurate fraud reporting. When an end-user logs into a protected application, Verified Duo Push generates a six-digit verification code in the Duo Universal Prompt:

Duo Mobile prompts the user for the verification code and displays contextual information about the authentication request to help end-users quickly identify a problem. More information will be coming as this new service comes on-line.

"Random Tid-Bytes"

Apple Issues Warning

This news has been out since the end of August, but we wanted to be sure any iPhone users were aware of serious security vulnerabilities for iPhones, iPads and Macs that could potentially allow attackers to take complete control of these devices. Apple released two security reports about the issue at the end of August, although they didn't receive wide attention outside of tech publications. Apple's explanation of the vulnerability means a hacker could get "full admin access" to the device. That would allow intruders to impersonate the device's owner and subsequently run any software in their name. Security experts have advised users to update affected devices — the iPhone6S and later models; several models of the iPad, including the 5th generation and later, all iPad Pro models and the iPad Air 2; and Mac computers running MacOS Monterey. The flaw also affects some iPod models. If you are an Apple user, please go to your **Settings** icon, and look for **Software Update** to see if you have the patch pending. Please proceed with installation if not yet installed.

Apple to Permit Self Service on MacBooks

Apple announced Self Service Repair will be available tomorrow for MacBook Air and MacBook Pro notebooks with the M1 family of chips, providing repair manuals and genuine Apple parts and tools through the Apple Self Service Repair Store. Self Service Repair for iPhone launched earlier this year and the program will expand to additional countries – beginning in Europe – as well as additional Mac models later this year. Self Service Repair for MacBook Air and MacBook Pro offers more than a dozen different repair types for each model, including the display, top case with battery, and trackpad, with more to come. Customers who are experienced with the complexities of repairing electronic devices will be able to complete repairs on these Mac notebooks, with access to many of the same parts and tools available to Apple Store locations and Apple Authorized Service Providers. To start the Self Service Repair process, a customer will first review the repair manual for the product they want to repair by visiting **support.apple.com/self-service-repair**. Then, they can visit the Apple Self Service Repair Store and order the necessary parts and tools. Every genuine Apple part is designed and engineered for each product, and goes through extensive testing to ensure the highest quality, safety, and reliability. Customers can send replaced parts back to Apple for refurbishment and recycling, and in many cases receive credit of their purchase by doing so.

Telehealth Decline

After reaching historically high adoption rates during the height of the COVID-19 pandemic, the use of telehealth services has plummeted since the beginning of the year. Experts say that places the healthcare industry at a fork in the road, where providers and payors choose whether to embrace this healthcare medium or abandon it. Before the COVID-19 pandemic, the adoption rate in the US was just 0.9% of outpatient visits. In first few weeks of the pandemic, this jumped to 52%, according Gartner. Now, as Covid has eased, usage has fallen to about a steady 12%. So questions remain if this is viable or people really just want in-person visits.

Huntress #1 for Endpoint Protection

Endpoint detection and response (EDR) tools are the newest members of the endpoint security family. They combine elements of both endpoint antivirus and endpoint management solutions to detect, investigate, and remove any malicious software that penetrates a network's devices. These tools give greater visibility of a system's overall health including each specific device's state. Companies use these tools to mitigate endpoint penetrations quickly and prevent data loss, theft, or system failures. They are typically used as a complement to larger security systems such as security information and event management (SIEM), vulnerability management, and incident response tools.

Huntress is part of SIM2K's Managed Security platform – this platform offers simplified EPP, managed EDR and more. We will begin aggressively replacing our other EPP and EDR systems to bring management under a "single pane of glass". Huntress is classified as a "managed EDR" – which is great news for SIM2K as it allows us to bring management of EPP (traditional AV) and EDR with 24x7x365 response.

Huntress finds and stops the spread of hidden threats that sneak past most security tools. Using a combination of automation and human ThreatOps experts, Huntress focuses on a specific set of attack surfaces, vulnerabilities and exploits. This enable Huntress to protect your infrastructure from persistent footholds, ransomware and other attacks. In an ever-evolving threat landscape, it is critical to stay ahead of hackers and bad agents. With the Huntress Security Platform, you're prepared no matter what tries to break through your defenses. As Huntress' slogan says, *"As long as hackers keep hacking, we keep hunting."*

G2, an on-line clearinghouse for information about software products with customer reviews and rankings, has released a list of the top Endpoint Detection & Response (EDR) Software products based on user satisfaction. A product's satisfaction score is calculated by a proprietary algorithm that factors in real-user satisfaction ratings from review data. Software buyers can compare products according to their satisfaction scores to streamline the buying process and quickly identify the best products based on the experiences of their peers.

As shown in the chart, Huntress is rated number one for Endpoint protection out of 20 products that include Symantec, Microsoft Defender and N-Able (falling below the graphic's display.) It shows that Huntress has a overall satisfaction score of 97% from all users participating in survey, as well as 90%+ rankings for Ease of Use, Meeting Requirements and Ease of Setup and Administration. Huntress also ranked highly for Ease of Doing Business and Quality of Support, which is important for SIM2K, our relationship with Huntress and our ability to then support your protection.

These capabilities are part of a new managed feature from Huntress called Process Insights, which continuously monitors activity from the thousands of applications that run on laptops and servers every day. It's also backed by the company's ThreatOps experts, which review all suspicious activity to validate threats, remove false positives and determine what remediation steps are needed – making it easy for even non-security teams to swiftly respond to cyber incidents.

"The first iterations of the Huntress platform focused on eliminating threats that had slipped past preventive tools, like persistent malware or ransomware," said the company's CEO.

"Over the last 18 months, we've extended [our protection] with external port monitoring, a robust managed antivirus offering, host isolation functionality and much more. These EDR capabilities are the next step forward in delivering an end-to-end platform that helps protect businesses at every stage of the modern attack lifecycle."

After several months in a public beta program, Process Insights has already been put to the test and seen multiple high-profile successes – including the discovery of North Korean actors targeting a Nuclear Think Tank. It was also tested during Huntress' rapid response efforts to combat a surge of Cobalt Strike payloads delivered to vulnerable VMware Horizon servers.

"In today's threat landscape, EDR is a must-have for protecting our clients," said a security expert. "Process Insights gives users increased visibility into endpoints and networks in a way that easily integrates into their technology stack."

"The past year or two have really validated what we've known since day one at Huntress – that SMBs need more cybersecurity help now than ever before," said a Huntress spokesman. "Process Insights is an exciting step in our continued journey to provide increased visibility to our ThreatOps team and drive improved outcomes for businesses."

Additionally, Huntress is looking to Process Insights to help businesses navigate another difficult challenge: cyber insurance and liability conversations. The company has designed Process Insights around the core set of EDR capabilities insurance carriers are looking for – helping ensure businesses can appropriately mitigate risk while getting the financial support they need during a security incident.

SIM2K believes our clients need to use this modern toolset to stay ahead of today's threats. As mentioned above, it allows you to check the "right" boxes on a cybersecurity audit and improve your profile when applying for cyberinsurance protection.

SIM2K is constantly looking to add the best solutions to our security suite, and thus offer our clients the security tools they need. Our partnership with Huntress is one more way we bring "best of breed" solutions to you. Contact us for more information on Huntress and how we put is to work for you.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com