UNISYS | Securing Your Tomorrow®

WSJ. CUSTOM STUDIOS

The Cloaked Approach to Business Data Security

Capturing and storing data—and making that data available to employees, customers and partners—is essential to many businesses' success today. But it also creates new security risks: As more data is shared and stored, companies are far more vulnerable to cyber threats.

"How enterprises run their operations and manage data is changing both swiftly and significantly," says Tom Patterson, chief trust officer for Unisys. Many companies today allow their employees to work remotely using public Wi-Fi and personal mobile devices, give their independent contractors access to their networks and systems, and rely on public cloud services to store important data. Without modern security planning, all of these trends greatly increase risks that cyber thieves and criminals—who have grown even more sophisticated—can break in, steal information and wreak havoc.

Moreover, technologies that store highly sensitive business information, including medical devices, energy grids and automatic teller machines (ATMs), are vulnerable to cyberattack because they're now linked to the internet.

"These assets that used to be held within four walls required someone to physically be at a company location to access them," Patterson says. "Now, it has become routine that they're able to steal them directly over the internet, so it's time to change their security approach."

These heightened cyber risks mean companies must think differently about securing their systems and devices. Rather than erect broad firewalls—as has been traditionally done—they should be protecting data in a more refined, segmented way. A growing number of companies are using microsegmentation, a new security approach that isolates critical data and systems, allowing them to communicate securely within trusted communities. It allows an enterprise to break the traditional, monolithic data security umbrella into carefully designed subgroups of employees and systems, providing each one with tailored, highly secure access. It then "cloaks" data, systems and users by concealing them from outside attackers while still allowing them to collaborate through encrypted channels within their trusted community.

Software that provides microsegmentation needs to operate based on the identity of the user as opposed to the device to be efficient. Unisys developed this software, Unisys Stealth®, in 2007 by leveraging advanced user authentication and strong data encryption technologies so that the identity of trusted users is irrefutable, and their communication in trusted communities is secure. And because the state of trust is always changing, Unisys microsegments of trusted users can be quickly adapted to drop or add users when their trust levels change.

Many enterprises can benefit from cloaking using microsegmentation, but Patterson points to four pressing reasons why they should be using it:

1. **Thwarting ransomware attacks.** Within their arsenal of weaponry, cyber attackers have increasingly turned to ransomware, which lock up systems until a ransom—usually a large sum of money—is paid. Healthcare systems, city governments, school districts and businesses of all sizes, from multinational corporations to small businesses, have fallen prey to these attacks.

   "If just one employee is tricked into downloading the ransomware software, it can bring down the whole network," Patterson says. "That can happen by clicking the wrong link, opening the wrong email attachment or connecting the wrong thumb drive to a laptop."

   Cloaking through microsegmentation prevents ransomware's wrath by containing it to only the group of employees who let it in. "You're not able to stop ransomware from getting in completely, but you're stopping it from spreading and being effective," Patterson says. "And that's really the number one goal of countering ransomware today."

2. **Meeting growing data security compliance hurdles.** The European Union's recently enacted General Data Protection Regulation (GDPR) places new, rigorous data privacy measures on companies and organizations around the world that serve EU residents. Data security regulations in payment security and health care have also increased in recent years—and penalties for breaching those regulations have climbed considerably. "In the past, a company might just have paid any fine it incurred," Patterson says. "Now these penalties are really significant, and companies are being proactive in trying to reduce their risk. By putting restricted data into a protected microsegment, you're able to greatly reduce the 'audit surface' and simplify compliance."

3. **Protecting internet-connected devices.** From ATMs to industrial control systems, companies are hooking up all sorts of devices that process and store sensitive data on the internet. For example, the systems that control natural gas flow below cities are often now internet-connected. "These things are life-and-death critical for us," Patterson says. "And because they are able to hurt people if they're misused, they've become a new target for bad guys around the world."

   Stealth™ allows companies to essentially hide these highly vulnerable technologies from anyone not pre-authorized to access them. "So if someone does break into the sales or HR portal of a company, their malware cannot get to or even see cloaked devices that are also connected to that same network," Patterson adds. "By hiding devices from the malware and from prying eyes, we not only protect data but also protect lives."

   The risks faced by life sciences and health care organizations are also significant. Many health care providers, for example, have connected legacy and mission-critical medical devices that were not designed to be internet-accessible. The explosion of ransomware and other more sophisticated cyberattacks have put both providers and patients at risk. Microsegmentation can thus be a valuable way for these companies to segment and restrict network and device data to pre-authorized groups of users and devices.

4. **Preventing insider security risks.** Employee espionage—whether small-scale or large-scale—has become a bigger concern for companies as they collect and store more data in more places. A firewall doesn't prevent an employee from stealing information since it's only meant to thwart outsiders. But using microsegmentation and cloaking to limit employees' access to only the information they need greatly reduces an employee's or contractor's ability to commit fraud, Patterson says.

   Companies need to be proactive and strategic about managing their cybersecurity risks as their operations and data storage and usage evolve—and their risks grow. Cloaking data using Stealth microsegmentation software provides a strong barrier to prevent thieves from accessing sensitive systems and data, while embracing the modern technologies that employees use, from data centers to mobile to public cloud.

*By **WSJ. Custom Studios***

Find out more about microsegmentation at
www.unisys.com/stealth

Printed in the United States of America 06/18 18-0334