insight.tech

Closing the Door on Cyberthreats

Published Date MARCH 26, 2021
Author TERESA MEEK

As organizations push deeper into the cloud and the IoT edge, the cybersecurity landscape is changing. To keep up, companies must change the way they protect their most valuable assets and infrastructure. The past year has driven that lesson home, as IT teams find themselves managing a myriad of computers outside their protected network to accommodate remote work.

And the proliferation of IoT devices—many of which lack the most basic security protections—vastly broadens the attack surface, creating new risks for organizations. "If a device is compromised, attackers can go from there to the corporate network," says Alex Ting, senior cybersecurity advisor at MasterSAM, a cybersecurity company, specializing in Privileged Access Management.

Traditional methods such as VPNs and firewalls do not comprehensively address the threats of this scale and magnitude. But new technologies in automation and advanced analytics offer stronger, broader protections, while simplifying management for IT personnel.

The IoT Security Problem

While IoT connectivity is growing by the minute, security has lagged. Devices are programmed with default passwords that often go unchanged. Automated security updates—a standard feature of modern cloud-based software—typically don't exist, leaving dangerous gaps for hackers to exploit.

To make matters worse, the same default credentials are commonly used for all devices of a particular ilk, and some can be found by searching public databases.

By infecting a large group of devices with malware, an attacker can also direct them to overwhelm a company's servers, disrupting websites and ecommerce in a botnet attack. That happened with the infamous Mirai botnet in 2016, which corralled hundreds of thousands of internet-connected cameras and routers to shut down sites including GitHub, Twitter, Netflix, and Airbnb.

To guard against these threats, MasterSAM and Intel® jointly developed the Universal Secure Access Management (USAM) X series hardware appliance, making it easier for clients to manage privileged accounts. USAM delivers its cybersecurity products, services, support, and maintenance in a single package. "Now they don't have to look for hardware or software—they just plug in the box," Ting says.

The solution automatically creates and securely stores all device passwords, changing them at set durations. It also provides fine-grained access controls.

"Organizations decide who can access a device and require human approval when necessary," Ting says. "In addition, we can monitor and record user activity to detect suspicious events, such as inappropriate commands or large-scale downloads of sensitive information."

The @SMasterSam solution enables privileged account management, providing several ways to defend against cybersecurity threats. via @insightdottech

---

IoT Threats Extend Their Range

As organizations and cities connect more systems to the IoT, attacks could threaten everything from factories to water systems and power grids. "We are seeing an increased convergence of the IT and OT spaces, making it easier for attacks to spread," says Ting.

For example, at aluminum manufacturer Norsk Hydro, a ransomware attack spread to production lines after an office employee clicked a phishing link. Some operations shut down, and the entire workforce had to do their jobs with pen and paper.

Ransomware, botnets, and other attacks often propagate through software vulnerabilities or outdated operating systems. To help clients keep up with thousands of users and devices, Silverlake uses Intel® Active Management Technology, which allows IT to install security updates and fix device problems remotely. It runs even when a device's operating system shuts down, allowing technicians to resolve problems without physical intervention or lengthy wait times.

Protecting Privileged Accounts

Attackers don't have to search for vulnerabilities if they can hack into privileged accounts, which belong to IT administrators and others with access to critical systems and data. Because privileged users have access to many devices and systems, they give hackers an ideal way to spread attacks.

The USAM solution enables privileged account management, providing several ways to defend against these threats, illustrated by the launch experience at a major ASEAN commercial bank.

The bank had 1,500 company resources to manage, including user devices, servers, and network equipment. Providing secure access was an enormous challenge for the small IT and security staff, which managed equipment and device passwords manually. In some cases, a technician had to walk over to users' computers and log in, without ensuring log-offs or recording sessions. Some passwords were kept in envelopes locked in a safe, causing mass confusion when users made errors or forgot to update them.

The bank implemented USAM to store passwords in a secure online vault and manage them with automated controls to avoid human error and free up staff. Access to sensitive systems is now tied to user and device identity and further controlled with multifactor authentication. Managers can approve or deny access requests with a click, and privileged sessions are remotely monitored and recorded. The bank also added analytics to gather data about privileged activities, such as accessing critical systems.

Adding Controls and Convenience

To further guard clients' sensitive information, USAM is embedded with Intel® Software Guard Extensions (Intel® SGX), which protects data when it's being processed in memory – for example, when a person or an IoT device is using a server. It prevents memory dumps and verifies that applications have not been compromised and contain the latest security updates.

MasterSAM continues to seek ways to improve security for its clients, who are increasingly turning to deep-learning technologies to spot evolving threats and improve anomaly detection. "As more organizations adopt cloud infrastructure, they will require more access controls and better analytics," Ting says. "In the cloud, you need to change constantly to keep up."

About the Author

Teresa Meek is an independent writer and editor with a background in journalism (Miami Herald, Newsday) who now specializes in content marketing. She writes blog posts, case studies, white papers, video scripts, and ghosted thought leadership pieces for major brands. Her clients have included Dell, Hewlett-Packard, Microsoft, Coca-Cola, Delta, Humana, JPMorgan Chase, and many other Fortune 500 companies. She is the author of the Amazon ebook Say It With Feeling: Business Writing in the Internet Age. She would be delighted to connect with you on LinkedIn or Twitter.