LITE-ON Storage is now Solid State Storage Technology Corporation

Security at Speed:

Leveraging SSDs with UTM for Lightning Response

Introduction

In an increasingly digitalized age, more and more valuable data is finding itself online, often stored in distributed networks within the “cloud.” This potentially offers greater flexibility and reduced costs but also moves security to the forefront of concerns. It seems like every week a new website is breached, a credit card database is harvested, passwords are getting leaked, and data is being stolen or locked behind encryption for a hefty ransom. This happens to businesses both big and small but ultimately they have to answer to their customers and shareholders. Threat management has therefore become a top priority as the volume and value of online data continues to increase.

Traditionally the status quo has been to solve security problems with specialized rather than universal paradigms. However, over time threats have grown more complex and security needs have in turn become that much greater. Novel schemes nevertheless do not exist in a vacuum and require the hardware to back them up, with one primary component being storage. Threats must be analyzed and contained which requires both capacity and performance. Therefore, the transition to complete digital security requires the correct solid state solution.

What Is Unified Threat Management?

Novel threats have become multi-varied and blended – this means they can attack from multiple vectors at once or evolve past their point of entry. The old approach of specialized security functions, such as having a firewall separate from real-time analysis, has become outdated. This is where Unified Threat Management (UTM) comes into its own. It’s possible to have an all-in-one security paradigm that mixes multiple elements together into a singular, manageable protocol. The evolution of threats has been met by a progression of protection with the so-called “next generation firewall.”

This type of security architecture has many advantages as the unification of security functions reduces monitoring time, draws back costs through the avoidance of many individual components, and also lessens the burden on personnel. Everything can be managed from a single portal and the facets are able to work together without complex interaction of different standards. Of course, this opens the door to a single point of failure and the traditional concept of “defense in depth” is not as well-realized. However, the potential to respond to existing and unique threats, and especially complex ones, generally outweighs these risks. Furthermore, this type of solution allows a business to tailor protection to their needs on-the-fly, focusing on the areas that are important at any given time.

Features of UTM

UTM offers some minimum features with the possibility of more, offering flexibility to information technology (IT) departments. These can be broken down into a few discrete categories with the advantage that a security solution can be as comprehensive as required. While any basic network protection will include a firewall – which primarily detects and prevents intrusions – it can be further expanded to protect applications, including email and web browsers. Anti-virus can also be present and expanded to protect against malware, spyware, and even ransomware in order to prevent the loss or theft of data.

Real-time analysis with the logging of events can help pinpoint weaknesses or breaches before and as they occur. Networks can be hardened against denial-of-service (DoS) attacks, distributed (DDoS) or otherwise, including with the use of a “tarpit” and port mirroring. The former makes a network a less-desirable target as the increased latency discourages probing while the latter allows contemporaneous analysis of data in transit. The ability to track events more generally helps prevent leaks, especially at traditional endpoints. Full control can be exerted on data-in-motion, data-at-rest, and with data-in-use with identification and detection of data type in real time.

Network access by legitimate users can be filtered with a proxy with simultaneous fine-grained network access control for permissions. Virtual Private Networks (VPNs) can be set up also to facilitate remote work and communication. With regularly updated heuristics it is even possible to protect against so-called 0-day attacks. Data is further defended through deep packet inspection (DPI), on top of all of the above security mechanisms as a part of full meta-analysis approach. A complete protection paradigm can be built from these independent elements utilizing a single maintenance apparatus, reducing the demands to a business that would rather focus on products and clients.

- Firewall
    - Intrusion Detection Service (IDS) and Prevention Service (IPS)
    - Application Layer (7) Firewall
    - Filtering and Proxy
- Protection
    - Anti-Virus, Anti-Malware, Anti-Spyware, Anti-Ransomware
    - Email Protection
    - Anti-DoS, Anti-DDOS
    - 0-Day
- Analysis
    - Deep Packet Inspection
    - Real-time Event Logging and Analysis
    - Tarpit
- Network
    - VPN
    - Network Access Control
- Data
    - Data Loss Prevention (DLP)
    - Data-in-Motion, Data-at-Rest, Data-in-Use
    - Leak Prevention

SSDs and UTM

One often-overlooked element of UTM is the absolute need for fast and capacious storage. The logging of events requires storage, as do the applications themselves, the quarantine and analysis of threats, definitions, and much more. Especially when analyzing lots of data in parallel there is a need for rapid storage so that reaction times are consistent and timely. Memory and compute time are expensive and given the raw amount of data transfers within the cloud, there simply must be a non-volatile (NVM) solution that allows for a comprehensive history of threats. This is where solid state drives (SSDs) come into play.

SSDs can provide local storage for threat quarantine but also instant access to reports and logs. Because modern threats are multi-varied and many solutions, like tarpits, are time-dependent, having low latency and consistent response times is paramount to successfully mitigating these threats. HDDs are not capable of achieving the number of operations per second (IOPS) required by any UTM solution that is actively defending a complex network. In the interest of data protection especially, the ability for SSDs to have power loss protection (PLP) is particularly critical for minimizing downtime when responding to threats – a response that can include disconnecting or cycling devices. Additionally, the capabilities of NVMe drives especially are attuned to the philosophy of a unified security design, thanks to features offered by the specification.

Recent historical developments, including the lockdown from COVID-19 but also significant ransomware attacks on important infrastructure, have reinforced the importance of a strong security protocol. With the compute power available today it is possible to analysis threats in real-time but also by looking at past data; there is an immense need for databases and logging in order to track these threats. This means capacity, but to keep up with the real-time demands there must also be consistent latency at high IOPS. SSDs have the potential to offer both while also having flexibility with, for example, form factor. SSDs are also reliable for minimum downtime and a low total cost of ownership (TCO) when deployed correctly.

Summary

New problems require novel solutions. The amount of digital data is expanding daily, and with it the value of that data – which is why hackers are regularly breaching networks to retrieve and ransom that data. Conglomerations of independent security devices, each specialized for just one function, have become unwieldy, unresponsive, and expensive. The future is in a unified threat management system that can offer flexibility based on the needs and size of a business’s network. Intellectual property and client data alike are far too valuable to be ignored or relegated to a secondary concern; there is an immediate and growing need for information security at all levels.

Regardless of implementation, storage is the backbone of any UTM system. Threats must be analyzed, logged, quarantined, and reverse-engineered, all without interruption of network functionality. SSDs, and particularly NVMe SSDs, offer the reliability and performance required for real-time analysis where a fast and consistent response time could mean all the difference. SSTC realizes this and provides a wide range of products that can meet your needs in a convenient, scalable fashion. Don’t leave your data security up to chance – institute a UTM backed by solid storage.

*All product and company names may be trademarks or registered trademarks of their respective holders.

Our SSD Solutions

PCIe™ - Our ED1 Series is a powerful, high performance SSD made for edge storage applications. It comes in M.2 and U.2 form factors.

SATA - Our ER2 SSD Series delivers affordability and performance with superior random read/write speeds of up to 90,000/45,000 IOPS. It comes in M.2 and 2.5" form factors.

Please contact our Solid State Storage Technology Corp. expert for more information.

*Specifications and features are subject to change without prior notice. Images are samples only, not actual products.

Request Full Specs Sheets

ABOUT US

A subsidiary of KIOXIA Corporation, **Solid State Storage Technology Corporation** is a global leader in the design, development, and manufacturing of digital storage solutions. We offer a comprehensive lineup of high-performance customizable SSDs for the Enterprise, Industrial, and Business Client markets. With various form factors and interfaces, our SSD solutions help businesses simplify their storage infrastructures accelerating variable workloads, improving efficiency, and reducing total cost of ownership.

Learn more at www.ssstc.com