WHITE PAPER

BEFORE THE FIREWALL

INTELLIGENT DEFENSE AGAINST THE OPEN WEB

OASIS TECHNOLOGY

TITAN

TITAN UP YOUR SECURITY INTRUSION PREVENTION SYSTEM

Protective equipment on the edge of a company's network is often the only witness to just how chaotic and lawless raw Internet traffic can be. As malicious traffic increases in volume and sophistication, the risk of costly and disruptive intrusions is increasing, with a serious attack occurring on every business, on average, 46 times per day.

Bombardment and Defenses

To get a perspective on potential dangers of the open Internet, people need only look up at the sky. As peaceful as the sky appears, Earth is actually under constant bombardment by objects from space. Most are dealt with by the atmosphere, which destroys them or rejects them before they become visible.

Over longer periods of time, a pattern of increasingly large hazards can be expected. In September of 2016, NASA made a presentation at the White House about hazards which could require human intervention. They won't be automatically deflected or absorbed, and will need a more powerful technology to protect Earth from damage or disaster.

> "Firewalls provide a basic filter and a secure way to hop over a wall into the local network, but admitted data can carry all sorts of malicious software."

The Open Internet is a Nasty Place

So it is with Internet hazards -- the peaceful corporate network is only a firewall away from chaotic, intense, and often malicious patterns of data traffic. Firewalls provide a basic filter and a secure way to hop over a wall into the local network, but admitted data can carry all sorts of malicious software. Firewall manufacturers are starting to include more advanced features, and cloud-based services offer help watching incoming data. As a uniquely targeted, on-premises, dynamic solution, the **Oasis Titan** works with existing firewalls and stays ahead of other security offerings.

Software hitchhikers are ingenious in finding beachheads in servers, PCs, mobile devices, even HVAC controllers. They arrive by the network or carried in the front door by computer users on USB memory sticks or other media. These rogue operatives can take advantage of the lightweight protections covering incoming firewall traffic, and the virtually nonexistent protections within most trusted corporate networks.

Numbers and Costs -- Eye Opening

For businesses, the incoming threats from the Internet are every bit as diverse and dangerous as those impinging on the planet. For the corporate network, the firewall system has been traditionally trusted to keep those dangers out. As long as it does, a sense of safety persists. When the first clever exploit penetrates and becomes known, eyes are opened and the company will usually start to take action. Why not **before**?

Even IT May Not Know the Big Picture

A combination of "it won't happen here" and a lack of awareness of potential threats keeps heads in the sand. There is plenty of other work to be done, and except for "small" threats such as email viruses, not much of the outside dangers are seen. Incidentally, as of 2016, the demand for IT specialists in the security area is enormous. Companies are catching up on their IT security protection, and recognizing that it is usually a bigger job than their current staff can manage, especially for small- and medium-sized businesses (SMBs). The **Oasis Titan** solution eliminates the need for constant staff research and technology updates to meet evolving threats.

The Threat Landscape from a Government Perspective

Congressman Ed Perlmutter, working in Congress on a bill (H.R. 6032) to help mitigate the threat to businesses, notes an average cost of $3.8 million per data breach. Some of the household names in the news, like Target and several other retailers, carry even higher price tags

for their intrusions – and they theoretically could have the resources to prevent them. But how? IBM estimates that businesses are attacked 16,856 times per year.

Those aren't just brute-force door knocking attacks, but attempts by sophisticated computer experts who often have very little to fear. The result of these attacks? 50% of SMBs had at least one data breach. Congressman Perlmutter's work aims at providing a tax credit for related insurance coverage, connected to a requirement to follow NIST standards-based security practices. In some industries, breaches trigger specific standards violation penalties from regulations such as Sarbanes-Oxley and HIPAA.

The number of records exposed, such as customer credit card numbers, provides a starting point for a loss of customer confidence and company reputation. Perlmutter's website notes that 783 reported breaches in 2014 exposed 85.6 million customer records.

Attack Technology -- Often Organized, Trained, Powerful

The openness of the Internet allows attackers to work from almost anywhere. This helps them avoid legal repercussions and often makes them difficult to locate, even for Internet experts. When criminals attack, they can even multiply their effect by thousands or millions using computer viruses and other tricks to hijack personal computers throughout the world in a "botnet" attack.

The primitive but effective DDOS (distributed denial of service) attack, which simply keeps a target network or system busy enough that it can't function properly, is an effective use of botnets, forming an attacking army of hijacked computers.

Black Hat, Dark Web

Advanced training and self-education places some cyber criminals at the forefront of the computer science field, although perhaps a darkened part of it. "Black Hat" conventions, information sharing on the hidden "dark web," and other connections keep hacker information flowing and techniques advancing.

CASE IN POINT:

Lightbulbs and Thermostats Attack

A leading security blogger, Brian Krebs, who exposes those profiting (sometimes by hundreds of thousands of dollars per year) from Internet attacks was shut down by a massive DDOS attack reported in late September, 2016. Experts are estimating that as many as one million "Internet of Things" devices including lightbulbs, security cameras and home automation devices such as thermostats were formed into a botnet which brought a 665Gbps (yes, gigabits!) stream to bear on his content delivery provider, major player Akamai.

After three days, the cost of mitigating the incoming harassment proved too much for Akamai, and they canceled Krebs' service account. This "weapon" could be aimed at any Internet target, and researchers have demonstrated that even FitBit wrist devices could be used in the botnet. Firewalls alone don't provide adequate protection, but the Oasis Titan can deflect incoming attack traffic, gather data on it, and engage strategies to reduce the effect of DDOS.

Old Scams and New Tricks

Assaults used are inspired by physical attacks and traditional criminal activity such as burglary, blackmail, and holding valuables for ransom. In the virtual (but very real) world, these equate to firewall attacks, vulnerable information theft, and ransomware which encrypts information until a "fee" is paid.

Modern assaults also include computer viruses and trojan horses distributed within the company in a variety of ways such as email, free USB keys, screensaver software, and malicious websites. System flaws can provide "open doors" to exploit until they are patched – several decades ago, a flaw was exploited by the simple "ping of death" to allow crashing of most of existing networked systems. Hackers constantly seek such flaws, and the **Oasis Titan** naturally rejects these kinds of exploits.

The Why of It

Hacker motivations can be financial, political, ego-based or purely malicious displays of their abilities. Potential payoffs include:

- Financial, as in ransomware or the value of illicitly acquired information
- Corporate espionage, especially international
- Damage and disruption
- Destruction of confidence in a company or government

Payoffs can range from small ransoms to millions of dollars, and consequences for international hacking can be limited in some cases.

Response capabilities

For known threats, corporate network operations departments have response teams that deploy to handle data breaches, network disruptions, and service outages. On an industry-wide basis, threat assessment and information dissemination is provided by CERT at Carnegie-Mellon University and other specialized organizations.

For small and medium-sized businesses, in-house response capabilities are usually limited. Contracted managed service providers may provide more extensive action to mitigate attacks. As a sign of the times, the FBI places computer and network intrusions first on their website under Key Priorities.

Unknown Threat Types

Since many threats are variations on previous methods, intelligent software found in **Oasis Titan** can look for patterns which are similar in function, or partially similar to known attack technologies. In addition to detecting static software such as simple trojans, intelligent approaches can detect behaviors which give away attack patterns. By keeping watch over system resources, software hiding places, and data assets known to be used or exploited by existing attack software, attacks can be identified.

Worst Case: Be Prepared for a Faster Recovery

As with natural disasters, protection against exploits and attacks is not the only way to avoid loss. Being prepared for disaster recovery (DR) is a company-wide need, and computer systems must be included. In the event of business interruption, data loss, or other significant events, a tested plan can be followed to keep the business viable.

New Technologies Require Updated Protection

As new and exciting technologies solve business problems and provide new opportunities, they can also challenge companies to implement further security measures. Virtualization, new web technologies, container technologies and software-based storage, networking, and even computerized HVAC systems all potentially carry vulnerabilities, both within the software and in the way that the software interacts with other systems.

IoT Will Be In Everything

The Internet of Things puts common software modules in many unexpected places such as refrigerators and home automation systems, offering more network entry points, especially if the network is shared with non-IoT devices. These systems can theoretically be infected and then serve as launching points, even as a version of the "botnet" army mentioned earlier, amplifying attack efforts. Imagine a collective botnet army consisting of hijacked home refrigerator systems!

Financial Platform Evolution

As interconnected financial platforms grow, especially in electronic data interchange and other B2B technologies, the potential for transfer of attack software and messages grows. Payment processing systems operate on many websites, and those websites are required to meet security standards to be connected to payment networks.Financial systems are an obvious

target for hackers, and will continue to be as they become ever more complex and interconnected.

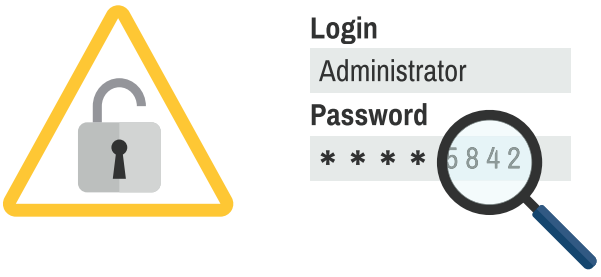
Protection Technology is Evolving Quickly

Static protections such as traditional firewall devices and software are becoming obsolete long before they can be depreciated on the books. They are being replaced by equipment which includes at least some "stateful" protections to identify attacks in progress, rather than just rebuff and filter network packets. Ideally, firewall devices will be complemented by the advanced hardware in the **Oasis Titan** which can keep pace with attack technologies without further hardware replacement, and when needed can scale to handle higher volumes of corporate network traffic.

Shared information, managed by a device manufacturer like **Oasis** or other centralized and secure source, helps users of advanced devices to keep as up to date as possible. They can be both informed and prepared for current attack methods, wherever they first appear. A collective defense enables even smaller companies to keep up with exploit activity in real time.

SMBs Need to be Empowered to Stay Secure

Security procedures, training, audits and planning may become increasingly costly as more sophisticated attacks are developed. A cost-effective and powerful solution, scalable to meet the needs of small business and companies with larger Internet data flows, the **Oasis Titan** works alongside the firewall with a managed solution or in cooperation with company IT personnel.



INTRUSION PREVENTION SYSTEM
SECURITY BEFORE THE FIREWALL

TITAN
TITAN UP YOUR SECURITY INTRUSION PREVENTION SYSTEM

The Power of Titan™

Oasis Technology's Titan system is an advanced network security solution to safeguard corporations, financial groups, government, and military agencies from the growing specter of international cyber intrusions and terrorism activities.

- Fast network Deep Packet Inspection (DPI) inspects all incoming and outgoing packets
- Improved network performance
- Self adjusting logic adjusts as hackers change their methods
- Fast HIPAA, PCI, SOX, and Gramm-Leach-Bliley compliance audits
- Fast installation - no changes to your existing network
- Stops ransomware and malware attacks
- Stops DDOS attacks
- 24x7 monitoring, data warehousing, and backups
- Automatic regular reports
- Security consulting
- Data warehouse of all data breach attempts

For more information on Titan, visit:
http://www.oasistechnology.com/titan/

Oasis Technology, Inc. 601 Daily Drive, Suite 226, Camarillo, CA 93010-5839 | (805) 445-4833

OASIS TECHNOLOGY

Oasis Technology, Inc.
601 Daily Drive, Suite 226,
Camarillo, CA 93010-5839
(805) 445-4833

www.oasistechnology.com/titan