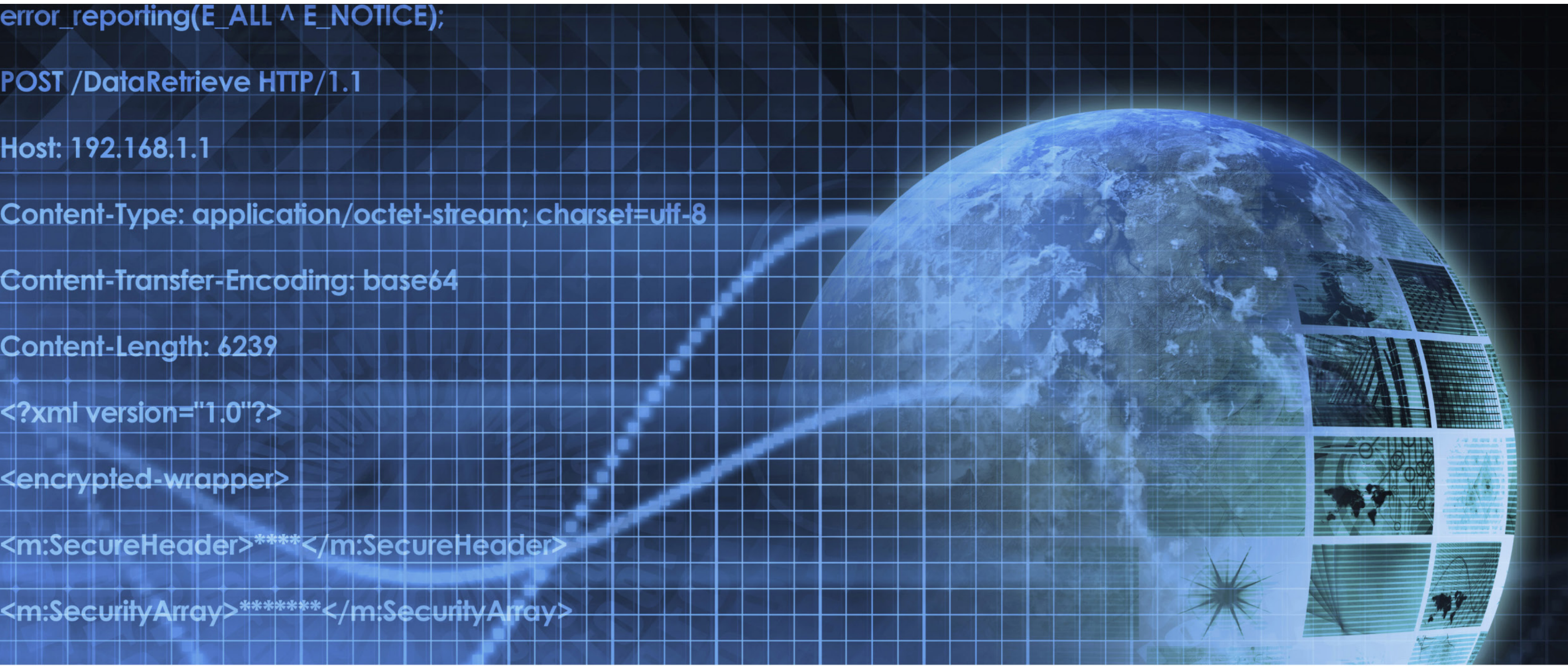

```
error_reporting(E_ALL ^ E_NOTICE);
POST /DataRetrieve HTTP/1.1
Host: 192.168.1.1
Content-Type: application/octet-stream; charset=utf-8
Content-Transfer-Encoding: base64
Content-Length: 6239
<?xml version="1.0"?>
<encrypted-wrapper>
<m:SecureHeader>****</m:SecureHeader>
<m:SecurityArray>*******</m:SecurityArray>
```

Online Security

Beyond Malware and Antivirus

Brought to You By:

AVG Business

Abstract

Security has always encompassed physical and logical components. But in the face of Bring Your Own Device (BYOD), an increasingly mobile and remote workforce, highlydistributed assets and sophisticated online threats, security has become too complex and multifaceted for many organizations to manage alone. At the same time, managed service providers (MSPs) are looking to explore new revenue streams in a changing market. Security, in all its forms, is a key area in which MSPs can become indispensible partners to their clients and with the right partner, online security has low barriers of entry and solid payoffs.

Read this white paper to learn ways that MSPs can leverage online security solutions to add substantial value for their customers and expand their service portfolios to grow their businesses.

Introduction

Security concerns, privacy invasions, data breaches, and new threats to computers and networks are making headlines every day. As the lines between our professional and personal lives blur and employees increasingly access corporate networks and resources with personal devices, the variety and complexity of security concerns can be overwhelming for even the savviest of organizations. SMBs, which often lack dedicated IT resources or experienced staff to address these challenges, are even more vulnerable to potential security threats.

It should come as no surprise, then, that businesses of all sizes are eager for new tools, new services, and strategic partners that can help them operate securely in IT environments dominated by cloud computing, BYOD, consumerization and highly distributed workforces. Markets and Markets projects that the global cybersecurity market will reach $155.74 billion by 2019 driven by "the rapid adoption of cloud-based services, wireless communication along with strict government mandates and increasingcyber crimes," according to its 2014 report.

Even taking a narrower view than the all-encompassing market described in this report, it's clear that service providers have extraordinary opportunities to address unmet needs for comprehensive security solutions in SMBs and large enterprises alike. Looking exclusively at "online security," the point at which all organizations become vulnerable to a growing range of malware and automated threats, managed service providers are uniquely positioned to help clients protect their networks, endpoints and users. Without making the investments or business model shifts required to sell and support security hardware, service providers can quickly introduce new revenue streams from online security services and further expand their portfolios of mission-critical services they can deliver to clients.

> “The cybersecurity market is estimated to grow from $95.60 billion in 2014 to $155.74 billion by 2019.”
>
> – Markets and Markets

Be the Expert

MSPs make their living delivering Software-, Platforms- and Infrastructure-as-a-service (SaaS, PaaS and IaaS, respectively). Yet an often overlooked differentiator for MSPs is their ability to provide "Consulting as a Service." Smaller and midsize businesses, in particular, need expert guidance in creating and executing robust security strategies. As IT service providers face increased pressure from commodity cloud providers, taking a personal, hands-on approach with clients around online security can provide several immediate benefits to MSPs:

- Generate demand for new online security services
- Nurture client relationships and establish a leadership position around the hot-button issue of security
- Create opportunities to bundle, integrate and upsell a variety of services with online security as the entry point

Capitalizing on these opportunities, however, requires both internal security expertise and strong partners with powerful security solutions that allow customers to execute on the security strategies you help them develop.

Secure BYOD and Mobility

Bring Your Own Device (BYOD) is one of the most-watched trends in business technology, and for good reason. The global market for devices, services, etc., related to BYOD is expected to top $181 billion by 2017. Despite this rapid growth and widespread attention, security and privacy remain the biggest barriers to BYOD adoption. A recent Ovum survey of more than 5,000 employees found a genuine lack of trust that employers could manage end-user privacy and security effectively. Conversely, IT departments are understandably concerned about leaky and malicious apps, lost and stolen devices and new vectors for malware resulting from BYOD.

> “The global BYOD market will grow to over $181 billion by 2017.”
>
> – Markets and Markets

Again, though, MSPs can play an important role mitigating these concerns with the right software and services. In particular, IT service providers can include mobile device management (MDM) in their service portfolios, provisioning, monitoring and securing employee-owned devices. This not only offloads responsibility from client IT departments but ensures that a trusted third party with MDM expertise can address end-user concerns about privacy.

In addition, MSPs can take on a consulting role, providing training and education for both employers and employees on best practices around mobile devices and BYOD. Secure BYOD requires a combination of vigilant and informed users, savvy administrators and solid MDM. This is hardly a pipe dream—solutions exist right now that the channel can leverage to ensure that their customers’ BYOD initiatives are successes rather than the stuff of headlines.

Protecting Users From Themselves

The average end user is far more focused on doing his or her job than the latest bit of malware found in the wild or the potential warning signs of sophisticated spear-phishing attacks. Instead, organizations must take aggressive steps to protect users and their networks from end users themselves.

Until recently, endpoint protection (and the overall improvement of network security that resulted) fell squarely on the shoulders of IT departments. MSPs and other IT service providers simply didn’t have the tools or resources to take this on for their clients. Now, however, secure remote management tools allow service providers to address two key areas of endpoint security:

- Antimalware installation and updates
- Patch management

Patch management, in particular, is labor-intensive for many IT departments and yet represents a major source of security vulnerabilities. In fact, as many as three-quarters of the attacks reported every year could be addressed simply by patching commercial operating systems and application software, according to a 2013 study by the Center for Strategic and International Studies.

> “75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching.”
>
> – CSIS

Ubiquitous installation and regular updates of endpoint antimalware software is also critical, especially when so many devices are used outside of corporate networks where gateway appliances and firewalls can at least partially mitigate malware risks. As with OS and application patches, IT service providers can now manage anti-malware installations for their clients along with improved email security measures, and even content filtering, to prevent users from accessing compromised or potentially risky domains.

Perhaps more importantly, modern remote management software can transparently and immediately provide insight to service providers about emerging threats at both the network and endpoint levels. The faster threats are identified, the faster they can be remediated, ensuring the highest levels of client security.

Disaster Recovery is the Ultimate Security

Although we often think of security in terms of online protection, defenses at the edge of our networks, logical measures to prevent unauthorized access or physical measures to thwart intrusions, business continuity also should be a critical IT service providers for robust backup and recovery solutions that leverage off-site backup, and intelligent tools for dealing with hardware failure, human error and disasters.

Backups traditionally took place in-house, with critical data copied in batches to tapes or other removable media. Service providers can help businesses overcome the limitations of this approach by introducing cloud-based backup, more frequent snapshots of data and regular off-site backup of all endpoints instead of just servers.

But backup is only the first step to true data security. Service providers can deliver substantial value to their clients by ensuring that they also are able to recover quickly from a disaster. In fact, by again acting as consultants, service providers can guide organizations in the development of robust disaster-recovery plans and then provide the software and services to implement them. Combined with the remote monitoring tools described earlier, service providers can immediately and proactively respond to problems, helping their clients recover from failures and errors quickly.

Security Anywhere, Anytime

We have touched on remote management solutions in each of the areas above, but these tools have important applications for service providers on their own. MSPs need to be able to discover endpoints, software and services, and ensure that they are properly controlled and maintained.

One of the barriers for service providers delivering this level of support to their clients, however, has been the need for rapid response and deep insight. Both of these were more easily delivered by on-site staff. Now, however, MSPs can make use of cloud-based services and small-footprint management agents to receive reports and alerts in realtime from anywhere. At the same time, they can remediate many problems remotely, often before clients are even aware a problem exists. Indeed, many of these monitoring and remediation tasks can now be automated, dramatically reducing burdens for both clients and service providers.

> “The survival rate for companies without a disaster recovery plan is less than 10%.”
>
> – Touche Ross

Conclusion

IT service providers have a unique opportunity to provide powerful security solutions and expertise to their clients. Security in the form of end-point management, antimalware services, patch management and disaster recovery all represent new potential revenue streams and important value-adds for clients. MSPs don’t need to break into this market alone, though. Finding the right strategic partners with established, respected services will ensure that barriers to entry are low, returns are high and clients are confident. ■

About AVG

AVG is the online security company providing leading software and services to secure devices, data and people. AVG has over 200 million active users, as of March 4, 2015, using AVG´s products and services including Internet security, performance optimization, and personal privacy and identity protection. By choosing AVG´s products, users become part of a trusted global community that engages directly with AVG to provide feedback and offer mutual support to other customers.

AVG Partners, Authorized Distributors and Authorized Resellers comprise a distribution network in over 150 countries and are a major contributor to the awareness of AVG Anti-Virus around the world. We also provide other ways for business cooperation such as Affiliate and OEM programs. The growing success of AVG and our business partners is a testament to our strategic business partner programs.