Redmond INTELLIGENCE

EXPERT RESEARCH ON MICROSOFT TECH

SOLUTION SPOTLIGHT

# Sherweb Office Protect

BY SCOTT BEKKER

SPONSORED BY SherWeb
Simplifying the Cloud

## INTRODUCTION—THE OFFICE 365 SECURITY BALANCE

Securing Office 365 for business customers presents a difficult balancing act for Microsoft partners. Office 365 is in extremely high demand among business users. When Microsoft last publicly discussed usage figures last fall, the commercial version of the cloud productivity platform had 155 million monthly active users worldwide. Microsoft also boasts 33 million consumer subscribers. The cloud productivity platform occupies a sweet spot with its combination of price and utility. Businesses are attracted to the suite's operational expense (versus capital expense) purchase model. Making that even more appealing is the relatively low per-user/per-month cost. With full packages starting in the range of $12.50 per user per month, the suite includes business email and other key collaboration services in the cloud and subscription access to the core Office productivity applications, such as Word, Excel and PowerPoint, which remain the industry standard.

Beyond the cost, a key selling point is the way subscribing to Office 365 offloads the maintenance of hardware and software of the server-side applications to Microsoft's efficient global datacenters, rather than having each customer be responsible for that upkeep and expense locally. At the same time, even the smallest, lowest-budget organizations find themselves in the novel situation of constantly getting access to the most up-to-date features and capabilities through the subscription model.

Having Microsoft manage the hardware, the operating system maintenance and the software updates also removes a huge source of security vulnerabilities, especially for smaller organizations. Many of the most significant security vulnerabilities that smaller organizations face arise from misconfiguring their systems and from falling behind on security patches.

**Microsoft's Security Offerings**

While Microsoft's world-class administrative staff, datacenter operations processes, datacenter automation and security research resources make Office 365 extremely well managed from a security standpoint, the product's market success represents a different kind of security risk. It is a situation that is almost unique to Microsoft and has played out across several of its most successful products over the decades. From Windows clients to SQL Server to Windows Server, Microsoft's repeated success in building a global installed base of business customers makes its products an incredibly attractive target for attackers. Because the products are used by businesses, they wind up being an attacker's route to valuable corporate assets. Attackers invest the time and effort to understand Microsoft's products, find vulnerabilities in them and develop exploits against them because they can reuse that effort against tens or hundreds of thousands of organizations. Given an Office 365 monthly active user base that is approaching 200 million users, the pattern is repeating itself with the cloud productivity suite.

Cover: Den Rise / Shutterstock.com

> **Microsoft's repeated success in building a global installed base of business customers makes its products an incredibly attractive target for attackers.**

Attackers prefer to go after the easiest targets, so much of their effort is going into the areas of Office 365 that are still under the control of individual organizations. That includes areas such as insecure use of the administrative settings and options within Office 365 and end users' continued willingness to click on URLs or attachments in phishing, spearphishing and ransomware-seeding emails.

Microsoft has anticipated these developments and invested substantial effort in countering them. Office 365 comes with powerful security capabilities built in. Even the most basic Office 365 plans include significant security capabilities. For example, Office 365 Business Essentials is the $5/user/month plan that includes Exchange Online and many other capabilities, but does not include the desktop versions of the Office applications. Within that bare bones plan, Microsoft includes Exchange Online Protection for anti-spam and anti-malware, more than 1,000 security and privacy controls, the ability to set security groups and permissions, and password policy capabilities.

**The Price Factor**

Other Office 365 and Microsoft 365 plans take those base-level security capabilities and package higher-level functionality around them. The mid-range Office 365 E3 plan adds in compliance capabilities such as legal hold and data loss prevention. Security is one of the major selling points of the top-tier Office 365 E5 plan. Security features of that plan include Advanced Threat Protection, for protection against phishing and zero-day malware; a security intelligence-related feature set called Office 365 Cloud App Security; a Customer Lockbox, which controls how Microsoft support personnel can access your mailbox; and more advanced compliance capabilities.

Earlier this year, Microsoft also introduced some security and compliance-specific packages for organizations that might not need the full voice capabilities that are another major component of the E5 suite. Those are the Identity & Threat Protection package for Office 365, Windows 10 and Enterprise Mobility + Security (EMS), and Information Protection & Compliance.

Yet price remains a significant barrier, especially for smaller customers, and the partners who serve them. Given that the affordable cost of Office 365 is such a sales driver, it can be difficult for organizations to see the value in nearly doubling their budget to get many of the more advanced security features.

Let's walk through a couple of examples at a small business on a per-seat cost basis. Say a customer needs the basic capabilities. On the services side, that's Exchange Online, SharePoint Online, Microsoft Teams and OneDrive. By Office applications, that includes desktop downloads for Outlook, Word, Excel, PowerPoint and Access. The Office 365 Business Premium plan would cost $12.50 per user per month, and includes anti-spam, anti-malware, and all of the security and privacy controls. Yet to go up to the more advanced tier of security and compliance tools of the $20/user/month E3 suite is an additional $7.50—a 60 percent price increase. The best security features, though, are in the E5 suite, but that's $35/user/month—a whopping 180 percent price increase.

The reality is that the market is really priced for two audiences. One audience is the companies that operate in regulated industries who must meet compliance requirements, and therefore have compliance budgets—often substantial—set aside. Most of the security products are priced for those customers. The other audience is companies without compliance requirements, who are much more motivated by price and are much less interested in advanced security capabilities. Those companies are much more likely to try to make do with the base security capabilities of the product.

> **"It can be difficult for organizations to see the value in nearly doubling their budget to get many of the more advanced security features of Office 365."**

**A Complicated Situation**

There's another significant factor when it comes to the substantial base-level security capabilities. While Microsoft has gone to impressive lengths to give organizations fine-grained control over security settings, less effort has gone into making the settings easy to use, especially for partners and customers who aren't focused exclusively on security.

The flip side of having more than 1,000 security settings is the challenge of finding them all, monitoring them and knowing what to do with them. This is a challenge for both partners and customers. Office 365 includes security settings in nearly a dozen dashboards. The online service also has half a dozen audit logs. Data in those logs also can be quite noisy, requiring a sophisticated user to make sense of the flood of events. Getting

that data is often a stumbling block in the first place. Logging has historically been turned off by default in Office 365, meaning the first time many organizations suspect they have an incident to investigate, they discover they have no data to examine.

Another aspect of the security complexity is ease of use. An attraction of Office 365 is that the suite generally works the way users want and expect it to. Some security changes, such as requiring multi-factor authentication, may be an unexpected annoyance for users who are in lower risk use environments, such as inside the company headquarters and sitting at their desk.

Taken together, all these factors mean that partners find themselves engaged in a complex balancing act, especially for customers without major compliance requirements. For each customer, the partner needs to weigh the level of security against ease of use, price and client expectations that the partner is helping to secure their environment. Within their own service organizations, meanwhile, partners must balance their own ease of administration for Office 365, often across multiple client accounts, with how much security expertise and training they must invest in for their own staff.

## SOLUTION

One company focused on providing a solution for partners trying to strike that balance between security, price and complexity in Office 365 is SherWeb. A Canadian company based in Sherbrooke, Quebec, with customers in more than 100 countries, SherWeb is a longtime hosting provider that has expanded into helping customers with their requirements involving cloud services, especially Office 365. SherWeb works primarily through a large network of partners and is an Indirect Provider in the Microsoft Cloud Solution Provider (CSP) program. Microsoft authorizes a limited number of Indirect Providers in each country or region to provide Office 365 and other cloud and subscription services to the much larger group of Indirect Reseller partners, who resell those subscriptions to end customers.

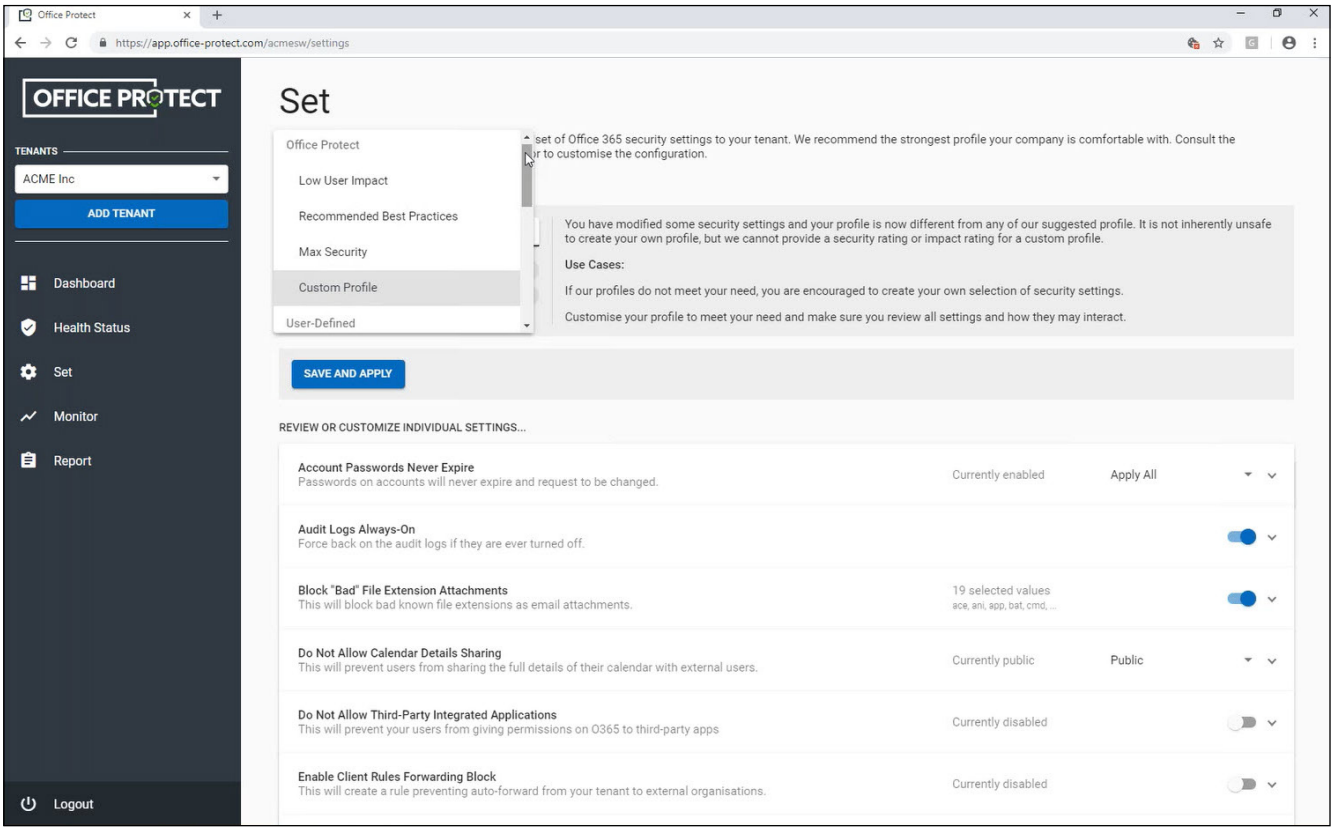
SherWeb's solution for partners serving smaller customers is a product called Office Protect. The primary design goal was to provide a tool for managed services providers (MSP) to simplify the process of securing basic Office 365 environments in a way that raises the security baseline significantly at a low price point. In addition to improving the security posture of small businesses running Office 365, other objectives included helping MSPs improve their internal efficiencies by making secure Office 365 setup easier, both for individual customers and across dozens or hundreds of customers, and providing additional business opportunities around basic security services for MSPs.

## PRODUCT DETAILS—OFFICE PROTECT

SherWeb officially launched Office Protect in October 2018 after a five-month soft launch with select partners. At its core, Office Protect is a Software-as-a-Service (SaaS) solution that works through Microsoft APIs to allow partners to set, manage and monitor their customers' Office 365 security.

Partners log in to an Office Protect portal that looks very much like the Office 365 interface and features simple choices from dropdown lists and on-off slider buttons, along with ample high-level explanations of what each choice entails. Top-level menu items include Dashboard, Health Status, Set, Monitor and Report.

To get started with a single customer, a partner goes into the "Set" section. At that page, SherWeb has collected from among all the Office 365 administrative dashboards a straightforward list of about 10 settings. The partner selects the customer from a dropdown list or clicks an "Add a Tenant" button for a new customer. Next, the partner can select one of SherWeb's pre-made templates for that customer.



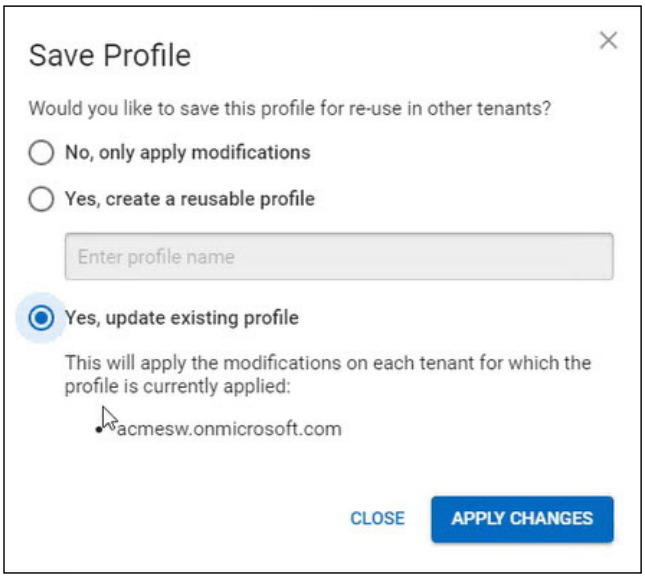

*The Office Protect Set menu allows the selection of a basic template that quickly configures security controls to ensure strong security. Options include Low User Impact, Recommended Best Practices and Max Security. MSPs can also configure individual settings for a custom profile.*

Those pre-built templates include:

- **Low User Impact:** A bare-bones security setting that does not rise to the level of best practices, but does not impact users' Office 365 experience at all. SherWeb recommends the setting for pilot programs.
- **Recommended Best Practices:** A more standard set of good security practices that balances strong security with end-user productivity needs.
- **Max Security:** A setting that favors strong security over user productivity preferences in cases where they conflict.

Lower on the page, a partner can see the full list of about 10 security settings that are being controlled by the template. Most notable among them are Audit Logs Always-On and Mailbox Audit Logs Always-On, which ensure that these critical logs are collecting data. The setting also means that if the logs are turned off for some reason, Office Protect will force them back on. Some of the other settings are Account Passwords Never Expire, Block "Bad" File Extension Attachments, Do Not Allow Calendar Details Sharing, Do Not Allow Third-Party Integrated Applications, Enable Client Rules Forwarding Block, Enable Multi-Factor Authentication and Set Outbound Spam Notifications. Because Office Protect has a fairly fast release cadence with new features being added on a monthly basis, several security settings have been added since Redmond Intelligence first viewed the menus. Those include Exchange Scripting (PowerShell) Access, Flag Phishing Emails using Tenant Domain or Staff Name, Block Top Spamming Countries and Only Allow Emails in Specific Languages.

Partners who wish to change a setting from the template are presented with an option to save the new profile. If yes is selected, the partner is prompted to name the profile, and it can be re-used for other customers. A truly partner- friendly feature is that when an existing profile is modified, a partner has the option to apply that modification on every tenant that has the profile applied. So, for example, if a partner has applied a profile to 100 tenants, and wants to change one of the settings, the partner has the option to apply the change to all 100 customers at a click. Contrast that with having to go in and reapply a new policy name one by one to each of the tenants. At the prompt, the tool also shows a list of all the customers covered by the policy.



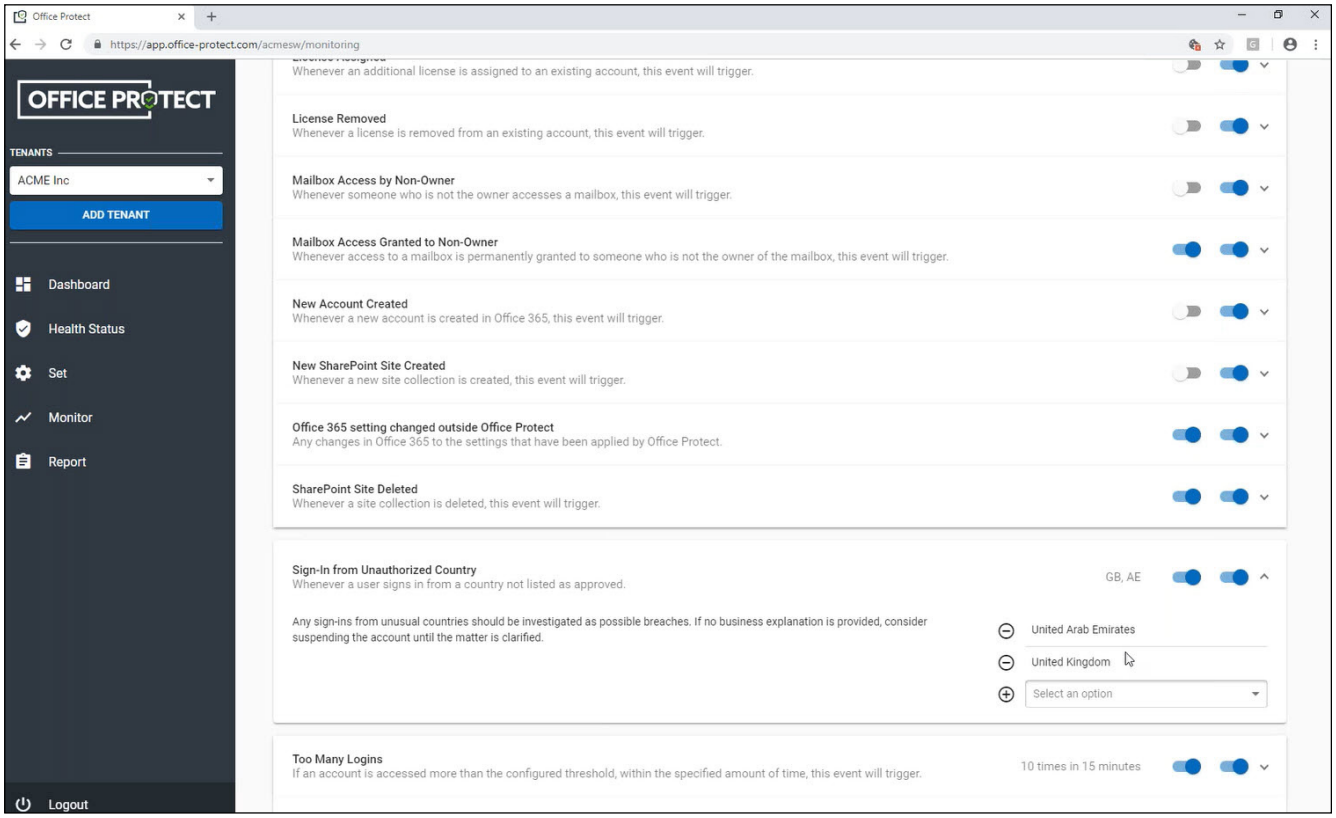

*One MSP-friendly feature of SherWeb Office Protect is the option to save a customized profile for multiple tenants at once.*

In the same way that SherWeb has worked to consolidate and simplify security settings, the company simplified Office 365's chatty logs for partners who are not daily or even weekly users. Under its Monitor tab, SherWeb set up monitoring

profiles that a partner can choose from, such as No Alerts, Focused, Recommended, Active or Everything On. Beyond that, SherWeb broke out Office 365 log output into events that might require action on the part of a security administrator. A headline example is Sign-In from Unauthorized Country, which like the other actions can either be chosen as an alert or something included in a weekly digest. Administrators can add authorized countries from a dropdown list. Being able to alert a customer that they have noticed a potentially suspicious logon from an unauthorized country can be a good conversation starter for an MSP with a customer and can demonstrate that the MSP is on top of the customer's Office 365 environment.

Other actions that can be monitored in the same way include account deletions, administrative role changes, email impersonation, user access with a previously unknown device and IP, the creation of a rule to transport email to an external domain, mailbox access by a non-owner, Office 365 settings changes not initiated from within Office Protect and excessive logins.

With the Report tab, Office Protect uses the data from the monitoring function to allow MSPs to create reports for their clients. An MSP can select a date range to bring up a report showing the date and user involved in events that are each explained in a details section.

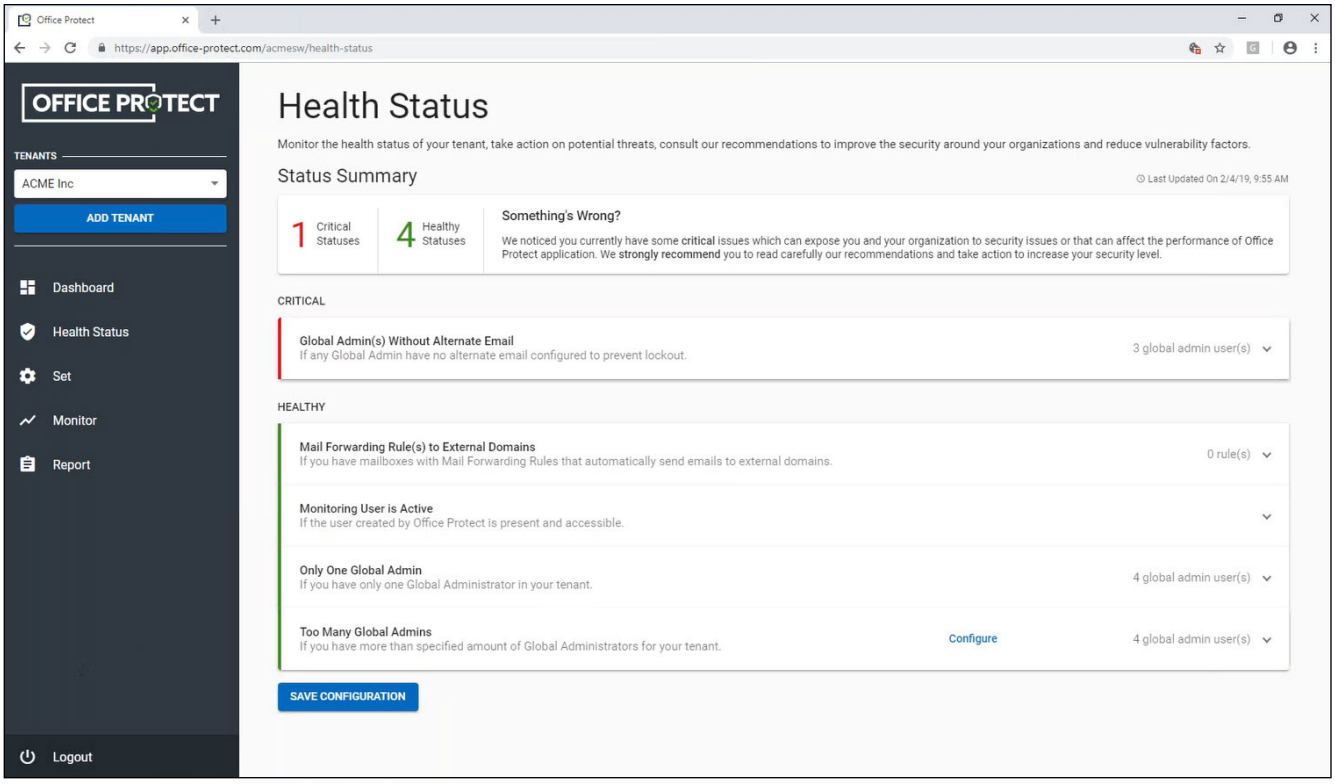



*A powerful feature is an alert when there is a sign-in from an unauthorized country. It gives MSPs a reason to pick up the phone and call a customer with a valuable piece of intelligence that also demonstrates how closely the MSP is watching the customer's environment.*

SherWeb has also created a Health Status tab in the Office Protect portal that collects some important security data points that are not necessarily security settings or security events. Those color several categories in green for safe or red for dangerous for a few key security questions. Examples include best practices around global admins, showing whether an organization has any global admins without alternate email addresses, whether an organization has only one global admin and whether an organization has too many global admins. Health Status also shows whether user monitoring is active and whether there are any rules forwarding mail to external domains. While similar data is available from the Monitor tab, the Health Status information notes if any such rules were set up, potentially by attackers, before Office Protect was installed.

The Health Status entry about having too many global admins illustrates a larger design principle in Office Protect. SherWeb automatically suggests a figure, based on the number of seats in the organization, but it can be configured. In general SherWeb aims for all the settings to be useful for improving security in their default configurations, but better if tuned by the MSP.

Making Office 365 security simpler to set up, manage and monitor is one major advantage of SherWeb Office Protect. The other is a price point low enough to appeal to customers without substantial compliance budgets. SherWeb charges $1 per user per month for the service. Compared to other security add-ons from Microsoft and third parties, the cost is




*There are a few vital elements of Office 365 security that aren't exactly settings or logged events. The Health Status view gives MSPs a way to track them.*

extremely low. It represents about an 8 percent increase per user per month for an organization already subscribing to Office 365 Business Premium. That cost for improving baseline security compares very favorably to the 60 percent to 180 percent price premiums discussed earlier for Microsoft's security-focused suites and packages.

Partners can use Office Protect even if they do not use SherWeb as their Indirect Provider within the Microsoft CSP program. Setting up the solution requires a few more authorizations than it does for SherWeb Indirect Resellers, but the functionality is the same for all partners using the product. For its own reseller partners, SherWeb offers Office Protect in a free bundle alongside an Office 365 or Microsoft 365 plan. That bundle allows resellers to use Office Protect for security setup at a customer within the first 30 days of purchase, SherWeb's Online Backup to provide 1GB per user pooled across the organization and 45 days of access to an app for client onboarding and training.

## PARTNER BUSINESS MODELS

Office Protect presents several business model opportunities for Microsoft partners.

### Upsell Security

Partners with existing clients can upsell security as an add-on for a price of their choosing, bundling in Office Protect, with its increased baseline security and ongoing monitoring. SherWeb's early-adopter partners are also adding in security assessments and on-site or remote training with this option.

## SECURITY COSTS FOR OFFICE 365

Advanced security functionality exists in all of Microsoft's Office 365 plans, including the most basic SKUs. This table uses Office 365 Business Premium as a baseline plan, and then shows the additional features and increase in price of various add-ons and higher-level plans. While less-expensive plans than Business Premium exist, the table uses only plans that include desktop Office applications to ensure a meaningful comparison with E3 and E5.

| Plan | Security Highlights | Price/user/month | Price increase over Business Premium |
|---|---|---|---|
| Office 365 Business Premium | Anti-spam, anti-malware, security & privacy controls, security groups, password policies | $12.50 | N/A |
| Office 365 E3 | Above + legal hold, data loss prevention | $20 | 60% |
| Office 365 E5 | Above + Advanced Threat Protection, Cloud App Security, Customer Lockbox, additional compliance capabilities | $35 | 180% |
| SherWeb | Baseline security setting templates, simplified security event management, reporting, health status, multi-tenant support | $13.50 ($12.50+$1) | 8% |

*Source: Microsoft, SherWeb, Redmond Intelligence*

### Managed Security Service

One of the strongest partner business opportunities with Office Protect is to offer an overall managed security service for new customers. This service bundle can include initial assessments, Office 365 licenses, Office Protect, ongoing monitoring and reporting for the customer, and end-user training. This option gives MSPs strong pricing control over the security service.

### General Managed Service

Another way to use Office Protect is to include its capabilities as part of the partners' in-house toolset for offering a general-purpose productivity managed service that is differentiated by the overall quality of the service.

## CONCLUSION

Microsoft offers incredibly powerful security tools for Office 365. Higher-level plans offer extremely strong security capabilities, but are priced mainly for enterprises and organizations with significant compliance budgets. Even the basic Office 365 plans include most of the security tools and capabilities that a small to midrange organization needs to thoroughly lock down the environment. Yet the ways that the security controls and logs are scattered throughout the Office 365 administrative interfaces can make it difficult for smaller customers and their partners to properly use them.

SherWeb's approach with Office Protect offers a cost-effective and straightforward way for partners—even those without significant security expertise—to raise the baseline security level for all of their customers' Office 365 environments.

---

***Scott Bekker*** *is a senior analyst with Redmond Intelligence and editorial director of Converge360. He has been reviewing, analyzing and covering Microsoft-related technologies for more than 20 years.*

## ABOUT REDMOND INTELLIGENCE

Redmond Intelligence provides independent and objective research and advisory services to technology buyers and vendors in the Microsoft ecosystem. Written by technical subject matter experts, Redmond Intelligence reports dive into the details of the Microsoft stack to provide actionable insights and concrete guidance. Projects range in scope from Solution Spotlights covering products in the Microsoft ecosystem to survey-based research reports to custom papers. For more information, visit *redmondintelligence.com*.

REDMOND INTELLIGENCE COPYRIGHT STATEMENT
© 2019, Redmond Intelligence and/or its affiliates. All rights reserved. Unauthorized reproduction is forbidden. Information is based on resources available during the time of preparation of the report and believed to be reliable. Opinions in this report are subject to change without notice. Redmond Intelligence Solution Spotlight, Redmond Intelligence Best Practice Report and Redmond Intelligence Research Report are trademarks of Redmond Intelligence. All other trademarks are the property of their respective companies. For additional information, go to redmondintelligence.com.