Technical Review

Datto SaaS Defense for Advanced Threat Protection

Date: November 2021 **Author:** Tony Palmer, Senior Validation Analyst

Abstract

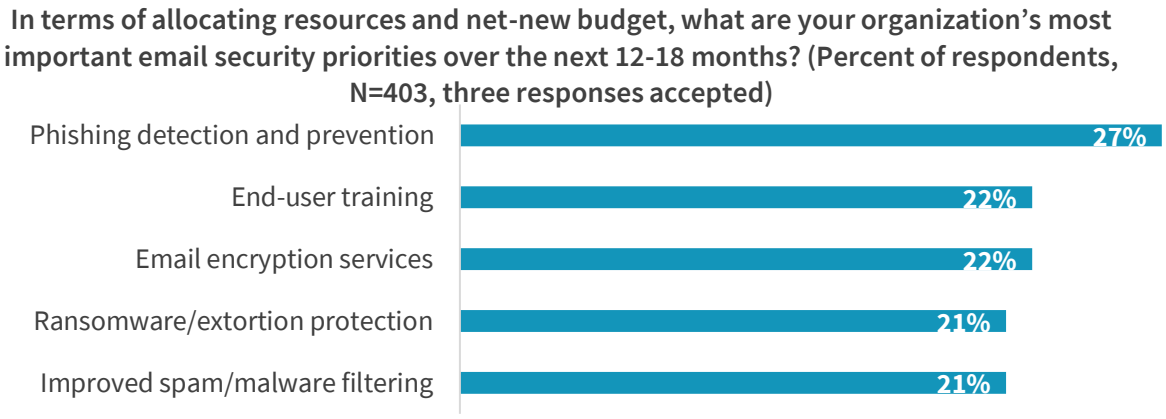
This ESG Technical Review documents the detailed evaluation of the Datto SaaS Defense Advanced Threat Protection (ATP) solution. ESG evaluated how the Datto SaaS Defense ATP solution provides detailed visibility and reporting while minimizing time to threat detection and remediation.

The Challenges

According to ESG research, most view email as a top five cyber-threat vector, with phishing considered the leading email security concern. More than two-thirds consider email to be one of their top five cybersecurity priorities relative to other security threat vectors. Further, nearly half experienced email-borne attacks on at least a monthly basis in the past year, and those experiencing daily attacks were significantly more likely to identify email security as their top overall cybersecurity priority. With phishing widely used to support the theft of credentials and other sensitive data, security professionals rank these types of controls at the top of their list when considering the purchase of new email security controls.[1] It's important to note that email is not the only vector to be concerned with. Attackers are also using other common communication and collaboration applications like OneDrive, SharePoint, and Teams to deliver malicious code.[2]

As organizations struggle to stop phishing-based attacks, increased investment in automated phishing controls (27%), end-user security awareness training (22%), encryption services (22%), ransomware/extortion protection (21%), and improved spam/malware filtering (21%) lead the list of email security priorities. Migration to cloud-delivered email security tools and the consolidation of email security controls show that organizations still want to simplify controls, while the focus on email spoofing and sender verification shows that slowing down impersonation attempts is a high priority (see Figure 1).

Figure 1. Top Five Email Security Priorities



Source: Enterprise Strategy Group

[1] Source: ESG Research Report: *Trends in Email Security*, August 2020. All ESG research references and charts in this technical review have been taken from this research report, unless otherwise noted.

[2] Source: ESG Master Survey Results, *The Maturation of Cloud-native Security: Securing Modern Apps and Infrastructure*, June 2021.

Datto SaaS Defense for Advanced Threat Protection

Datto SaaS Defense is an advanced threat protection (ATP) and spam filtering solution that detects unknown malware threats at first encounter across the Microsoft 365 suite. The solution provides data-independent technology, which was developed to stop zero-day threats and proactively defend against malware, phishing, and business email compromise (BEC) attacks that target Microsoft Exchange, OneDrive, SharePoint, and Teams.

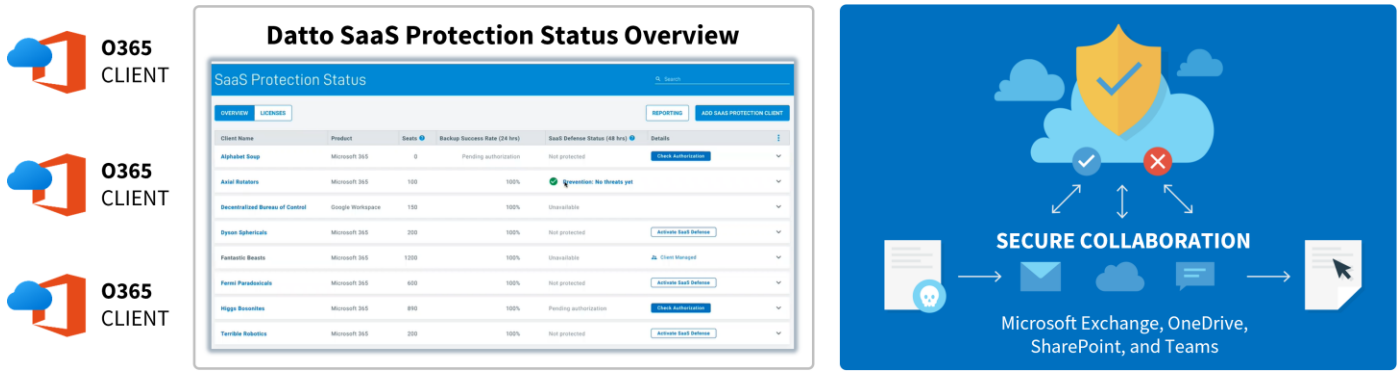
Datto SaaS Defense provides detailed monitoring and reporting with simple explanations as to what threats were identified and why. This includes silent detection that proactively monitors and eliminates cyber-threats as soon as they are encountered without manual interference or end-client disruption.

The security solution is designed for managed service providers (MSPs), providing seamless deployment and management to get new clients up and running in minutes with two-click onboarding and multi-tenant management from a single dashboard.

Datto SaaS Defense is fully integrated with Datto SaaS Protection to protect and defend critical cloud data against unknown cyber-threats and common data loss scenarios with comprehensive detection, protection, and recovery.

In addition, Datto offers a completely integrated solution built exclusively for MSPs that scans Microsoft 365 for malicious cyber-threats and ensures complete protection with daily backups and flexible recovery (see Figure 2).

Figure 2. Datto SaaS Defense Overview



Source: Enterprise Strategy Group

Datto SaaS Defense is designed to provide the following benefits:

- Proactivity – Proactive monitoring, detection, and elimination of unknown malware threats and phishing attempts.
- Minimized time to detection – Prevents zero-day threats as soon as they are encountered, without manual interference or end-client disruption.
- Seamless deployment and management – Ability to set up new clients in minutes.
- Complete integration – Integrated with Datto SaaS Protection, which provides a multi-layered security approach to protect against permanent cloud data loss.
- Streamlined protection – Reliable protection that saves MSPs time and resources previously spent on threat reporting, managing false positives, and updating blocklists.
- Robust reporting – Simple, detailed reporting that shows why a threat was identified as malicious, without a complex scoring matrix.

ESG Evaluated

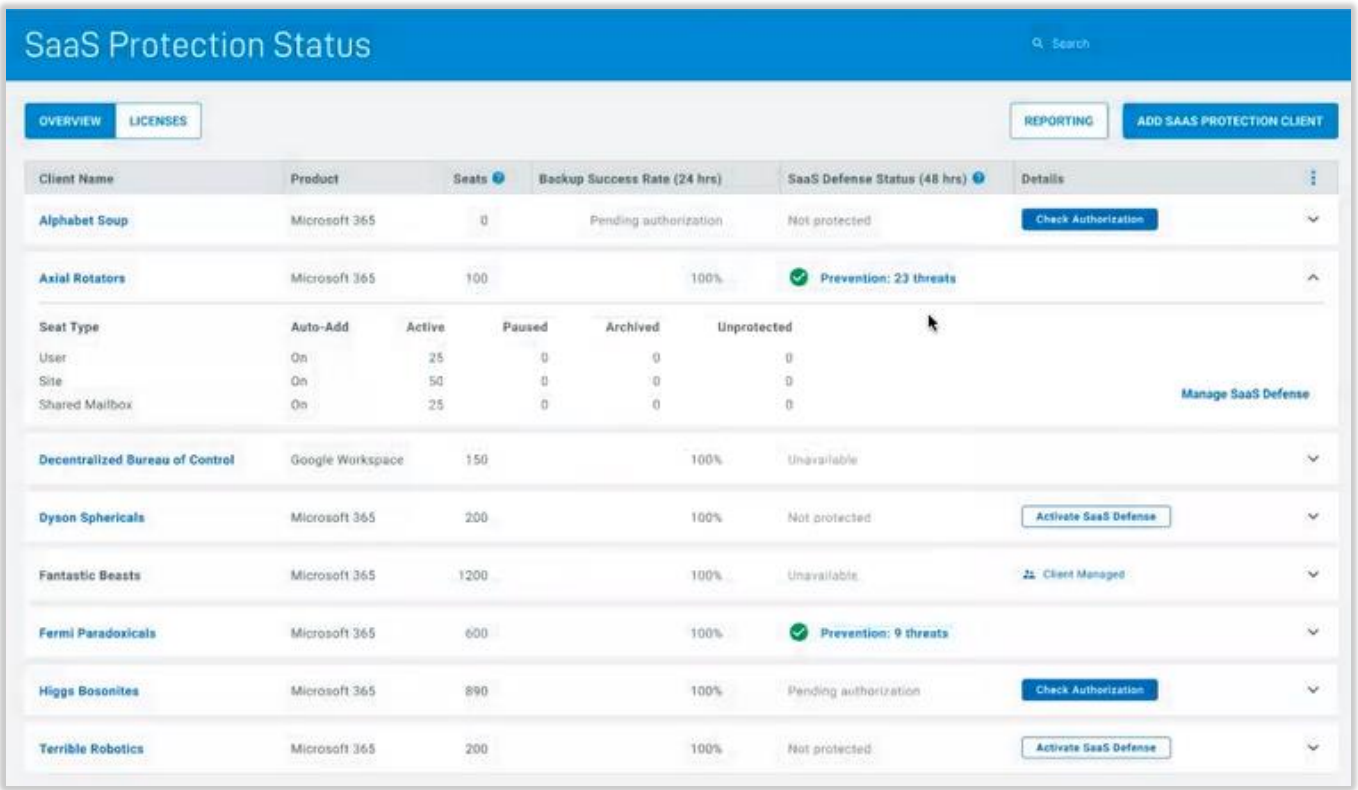
ESG completed a technical evaluation of the Datto SaaS Defense for ATP security solution with a focus on visibility and reporting, and time to threat detection and remediation.

Visibility and Reporting

The Datto SaaS Defense dashboard, which is designed specifically for MSPs, provides detailed visibility that allows admins to learn the details quickly and easily about each malicious object (e.g., email, file, or link) that Datto SaaS Defense has flagged. From this dashboard, admins can dive into why the threat was flagged as malicious, the penetration flow, and the evasion techniques used to attempt to bypass threat protection solutions (see Figure 3). There are different categories of information for each malicious item depending on the type of attack and the specific techniques used. Some examples include:

- Malicious files that require a password for accessing them (e.g., PDF or ZIP files).
- Malicious payloads that are found in email attachments and can sit harmlessly for some time until triggered.
- Macro malware that takes advantage of the VBA (Visual Basic for Applications) programming in Microsoft 365 macros to spread viruses, worms, and other forms of malware.
- WMI commands, which may be used to interact with local and remote systems to perform dangerous functions, such as gathering information for discovery and remote execution of files as part of lateral movement.

Figure 3. SaaS Protection Status Dashboard Overview



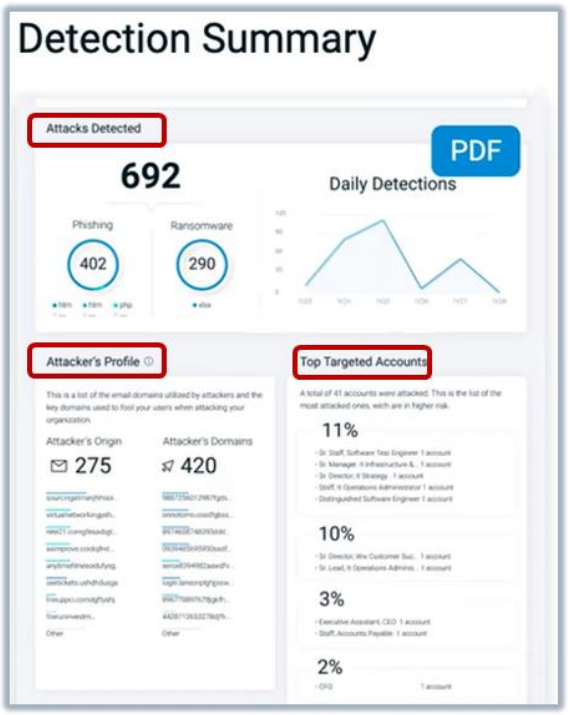
Source: Enterprise Strategy Group

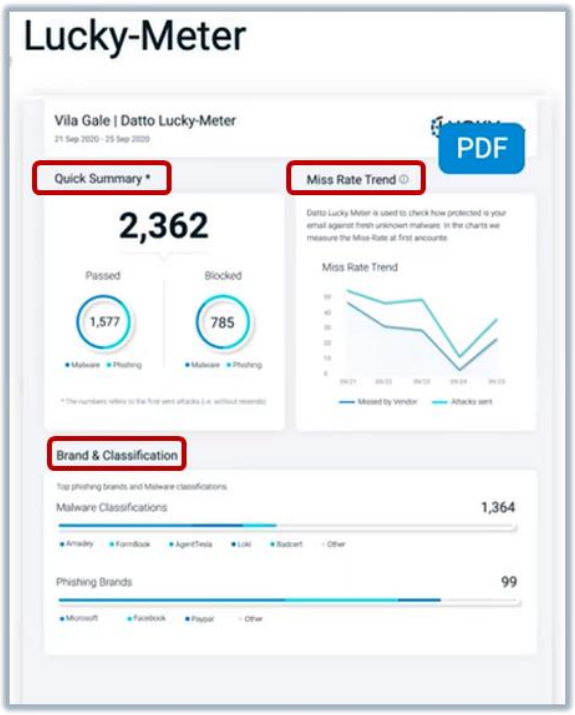
As shown in Figure 4, the Datto SaaS Defense solution also includes detailed reporting.

The Detection Summary report shows that 692 attacks have been detected, 402 were phishing attacks and 290 were ransomware attacks. The Attacker's Profile provides a list of the email domains utilized by attackers and the key domains used to fool users when attacking an organization. The Top Targeted Accounts section shows that a total of 41 accounts were attacked. In addition, it shows a list of the most attacked accounts, which are at a higher risk for continued attacks.

In this example, the *Lucky-Meter* report shows that, over a four-day period, there were 2,362 attacks. It also shows that 1,577 attacks passed through existing security solutions and that 785 attacks were blocked by existing security solutions. The Miss Rate Trend shows how protected email is against fresh unknown malware, including attacks missed by vendor versus attacks sent. This report also shows the malware classifications and phishing brands.

Figure 4. Datto SaaS Defense Reporting





Source: Enterprise Strategy Group

Both reports are easily downloaded as PDF files.

Why This Matters

According to ESG research, most organizations run cloud-delivered email and collaboration apps, with nine out of ten organizations surveyed by ESG reporting some usage of cloud platforms, and nearly three-quarters (73%) identifying cloud as their primary platform. Most of these organizations plan to use third-party controls to fill native security gaps.

ESG validated that Datto SaaS Defense security solution provided detailed visibility and reporting, which was achieved by providing an interactive dashboard overview, and detailed reports which can be downloaded as PDF files.

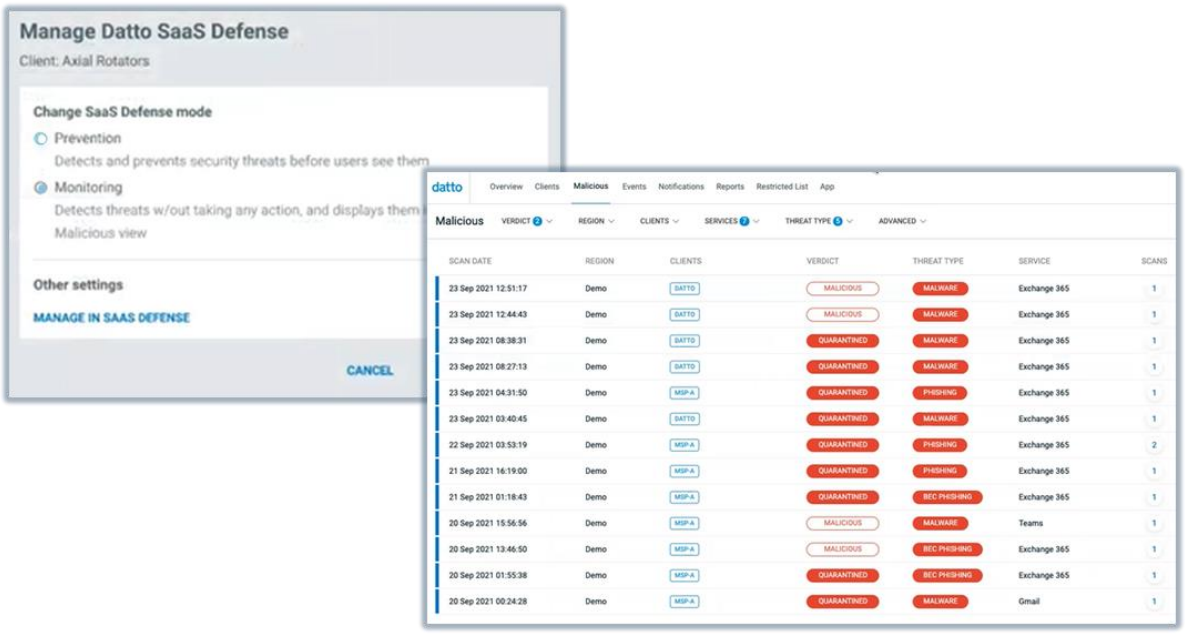
Threat Detection and Remediation

The Datto SaaS Defense solution has two modes of operation:

- **Monitoring Mode** – Detects threats without taking any action and displays the threats in the Datto SaaS Defense Malicious view.
- **Prevention Mode** – Detects and prevents security threats before users see them. This is the full version of the solution.

Monitoring Mode, as shown in Figure 5, shows the Malicious view, which will flag a threat as malicious but does not quarantine the threat. This is a great way to have the solution running to see what would have been detected and blocked, without taking action.

Figure 5. Datto SaaS Defense – Monitoring Mode



Source: Enterprise Strategy Group

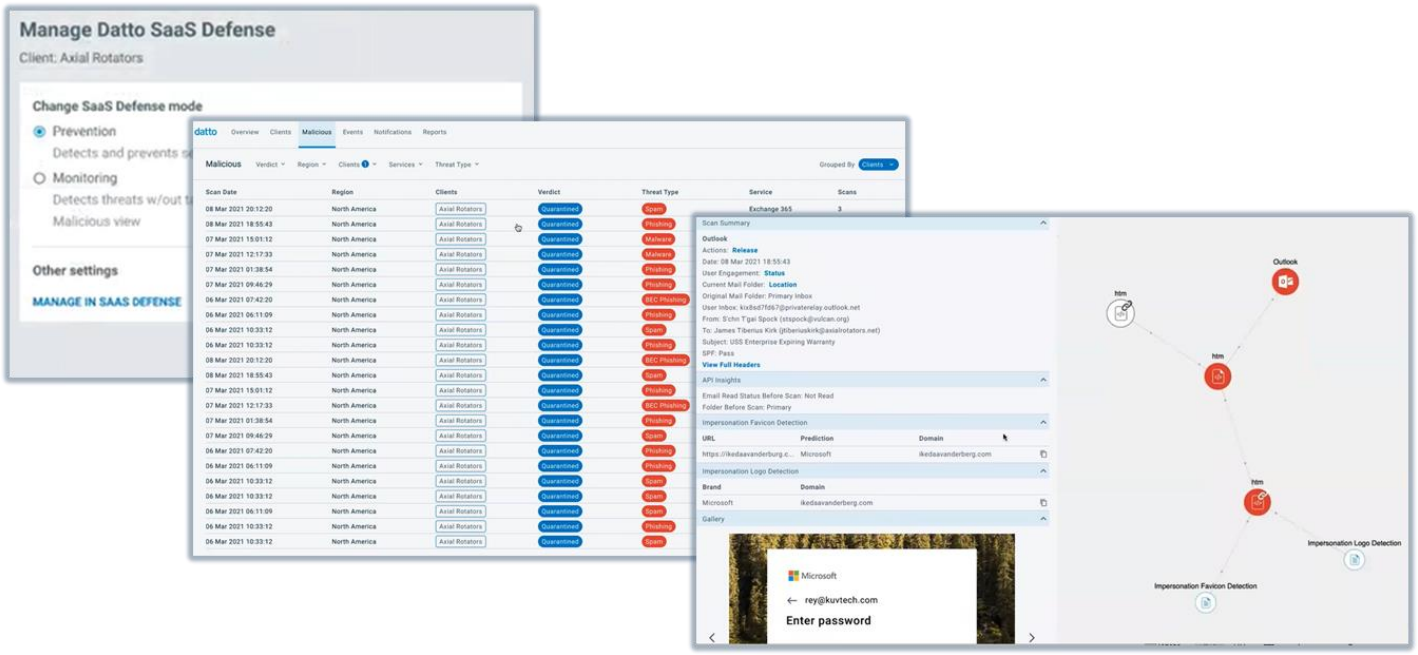
Prevention Mode, as shown in Figure 6, is the full version of the platform, which scans for malicious content coming into the environment. If it finds something malicious, the threat is quarantined by putting it into the junk folder so it's not directly visible to the user in their inbox. The solution will also neutralize the email itself. For example, if there was a phishing link or a malicious attachment, it will be replaced with a stub that says this is a malicious threat and advises end-users to contact their IT provider if they think this is a mistake. The solution does give end-users the ability to go into their junk folder to see that the email came in and that it got blocked by the system.

Datto SaaS Defense provides the ability to drill down and investigate threats. If the admin determines that this is a false positive and that the end-user should have received the email message, the admin can release the email. If the threat is positive, the admin can investigate the Scan Summary and drill down into the following information:

- **Actions** – Including releasing the email message.
- **Date –** Of the email message.
- **User Engagement –** Status of the message.
- **Current Mail Folder –** Folder location.

- **Original Mail Folder –** For example, the primary inbox.
- **User Inbox –** Inbox address.
- **From –** Email address.
- **To** – Email address.
- **Subject** – Of the email message.
- **SPF** – Pass or Fail.

Figure 6. Datto SaaS Defense – Prevention Mode



Source: Enterprise Strategy Group

In addition, the admin can view the full email headers to research a phishing attack or ransomware attack, including impersonation favicon detection and impersonation logo detection.

Why This Matters

According to ESG research, more than half (53%) of organizations believe that native email security controls are insufficient, though only 23% chose to incorporate additional, third-party controls before migrating to cloud-delivered email to compensate.

ESG validated that the Datto SaaS Defense security solution minimizes the time to threat detection and remediation by providing the ability to drill down and detect and prevent security threats before users see them.

The Bigger Truth

Since more than two-thirds of organizations consider email to be one of their top five cybersecurity priorities relative to other security threat vectors, organizations often look to ATP solutions for front line security. ATP solutions defend against sophisticated malware or hacking-based attacks. While specific features of ATP solutions vary, most include a combination of endpoint agents, network devices, email gateways, malware protection systems, and a centralized management console to correlate alerts and manage defenses for cloud-based email platforms. On the back end, organizations need a data protection solution that enables them to make fast, reliable restores after an attack.

Datto SaaS Defense is an advanced threat protection (ATP) and spam filtering solution that is fully integrated with the Datto SaaS Protection backup and recovery solution. Datto SaaS Defense detects unknown malware threats at first encounter across the Microsoft 365 suite. The solution provides data-independent technology, which was developed to stop zero-day threats and proactively defend against malware, phishing, and business email compromise (BEC) attacks that target Microsoft Exchange, OneDrive, SharePoint, and Teams.

MSPs that are not currently leveraging an ATP solution for Microsoft 365 open themselves and their clients to a host of potential risks, from basic threats like spam and viruses to more advanced threats, including advanced malware, ransomware, and zero-day attacks. MSPs without any type of threat protection or inadequate threat detection are placing their clients in a dangerous position, particularly considering the steady uptick in cybersecurity events.

ESG research shows most organizations and MSPs are using or are interested in ATP solutions. Of course, you should evaluate the needs of your environment before deciding on an ATP solution.

Datto SaaS Defense—with Datto SaaS Protection—provides a multi-layered cloud security solution that proactively prevents against malicious cyber-threats while providing powerful backup and flexible, fast recovery. This is all managed from a single portal, with a single management experience for an MSP. If you want to accelerate your time to threat detection and remediation, ESG recommends that you consider the Datto SaaS Defense security solution.