REPORT REPRINT

GDPR drives compliance to top of security project list for 2018

DANIEL KENNEDY

4 OCT 2018

Compliance requirements vary from one industry to the next. The May Voice of the Enterprise, Information Security survey of 552 security professionals looks at the trends and factors affecting security teams and project prioritization.

451 Research®

Compliance requirements vary from one industry to the next. In an ideal world, it would be nice if compliance were simply the byproduct of a good security program, but things rarely work that perfectly; compliance and security each represent their own set of diverging requirements. The 2018 Voice of the Enterprise: Information Security, Workloads and Key Projects survey of 552 security professionals looks at the trends and factors affecting security teams and project prioritization.

THE 451 TAKE

The attention around the General Data Protection Regulation (GDPR), with its timelines for notification, new requirements for identity and privacy, and significant potential fines, has added to substantial industry requirements already present and pushed compliance requirements to the top of the list of pain points and security projects.

REPORT HIGHLIGHTS

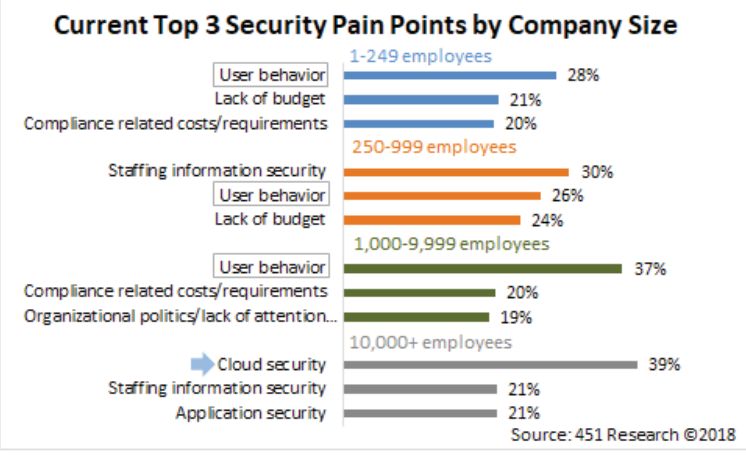
- Top pain points – While end-user behavior continues to be a top pain point for companies with fewer than 10,000 employees, respondents from very large organizations are struggling with cloud security.
- Compliance jumps the queue – The EU enactment of the GDPR in May has pushed compliance to the forefront of security project priorities for the coming year.
- Endpoint security – Endpoint security remains relevant. It is still the most widely adopted (91%) security technology across organizations of all sizes.
- Compromised endpoints – On average, companies with fewer than 1,000 employees spend 5.2 hours a week cleaning up compromised endpoints. Larger organizations with many more endpoints to manage are spending 8.5 and 13.5 hours a week.

TOP SECURITY PAIN POINTS

User behavior continues to be a top pain point for companies with fewer than 10,000 employees. A closer look at the top three security pain points by company size shows that for 39% of very large organizations, cloud security is their top paint point.

FIGURE 1: TOP SECURITY PAIN POINTS BY COMPANY SIZE

Source: Voice of the Enterprise: Information Security, Workloads and Key Projects 2018



COMPLIANCE JUMPS THE QUEUE

What constitutes compliance is very industry-specific (e.g., Gramm-Leach-Bliley Act, HIPAA, HITECH, etc.), but the breach notification timelines and fines associated with the European Union GDPR enacted on May 25 has gotten the attention of many security managers. The GDPR not only applies to organizations located within the EU, but it will also apply to all companies processing and holding the personal data of data subjects residing in the EU, regardless of the company's location. Companies out of compliance can face steep fines.

Although compliance has been an ongoing concern, GDPR is causing a reprioritization of security project plans, and in some cases, has derailed them – especially in Europe. Instead, companies are focusing on inventorying systems against new concepts of identity and remediating identified gaps. Consequently, regulatory compliance (PCI compliance, GDRP, PSD2, NIST) is the top security project for 35% of respondents over the next 12 months, and this is true for organizations of all sizes. That number jumps to 40% for very large organizations with more than 10,000 employees.

FIGURE 2: TOP SECURITY PROJECTS

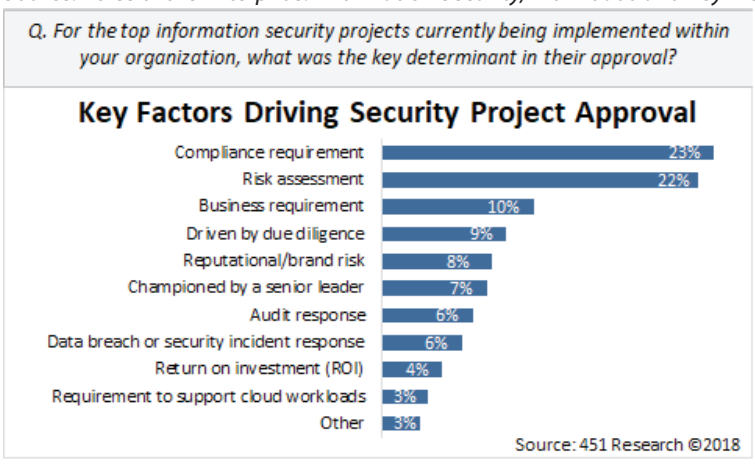
Source: Voice of the Enterprise: Information Security, Workloads and Key Projects 2018

PROJECT APPROVAL DRIVERS

For the last three years, some manner of risk assessment has been the most common driver moving security projects forward. In 2018, compliance requirements (23%) are edging out risk assessment (22%) as the top factor in security projects being approved and prioritized.

FIGURE 3: DRIVERS FOR SECURITY PROJECT APPROVAL

Source: Voice of the Enterprise: Information Security, Workloads and Key Projects 2018

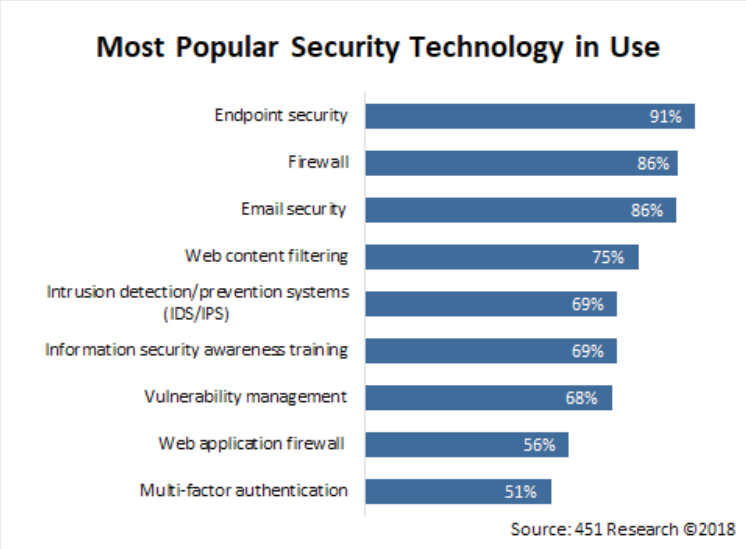


ENDPOINT SECURITY

Endpoint security remains relevant; even as new architectures come further into play, protecting users' endpoints remains a concern. Endpoint security (91%) is still the most widely adopted security technology across organizations of all sizes. This is followed closely by firewall (86%) and email security (86%).

FIGURE 4: SECURITY TECHNOLOGY IN USE

Source: Voice of the Enterprise: Information Security, Workloads and Key Projects 2018

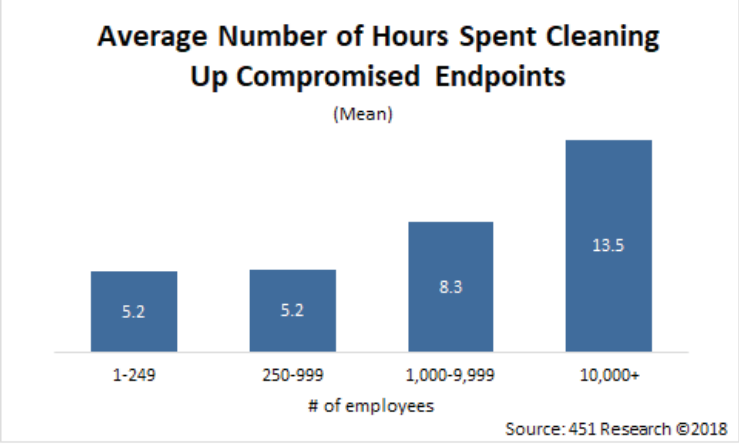


COMPROMISED ENDPOINTS

Endpoints are critical points of vulnerability. When endpoints are compromised, that device transforms from a secure endpoint on the corporate network to an exploitable access point vulnerable to external cyber attacks. This exposes not just the device, but the entire corporate network to the threat. On average, companies with fewer than 1,000 employees spend 5.2 hours a week cleaning up compromised endpoints. Larger organizations with many more endpoints to manage are spending 8.5 and 13.5 hours a week, on average.

FIGURE 5: TIME SPENT CLEANING UP COMPROMISED ENDPOINTS

Source: Voice of the Enterprise: Information Security, Workloads and Key Projects 2018

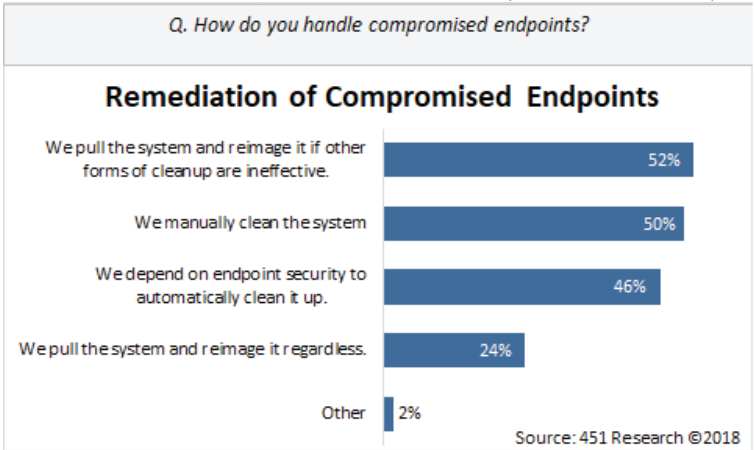


DEALING WITH COMPROMISED ENDPOINTS

The remediation process is time-consuming because it is highly manual – 52% of respondents are forced to re-image the system if other forms fail, and another 50% manually clean the compromised system.

FIGURE 6: REMEDIATION OF ENDPOINTS

Source: Voice of the Enterprise: Information Security, Workloads and Key Projects 2018

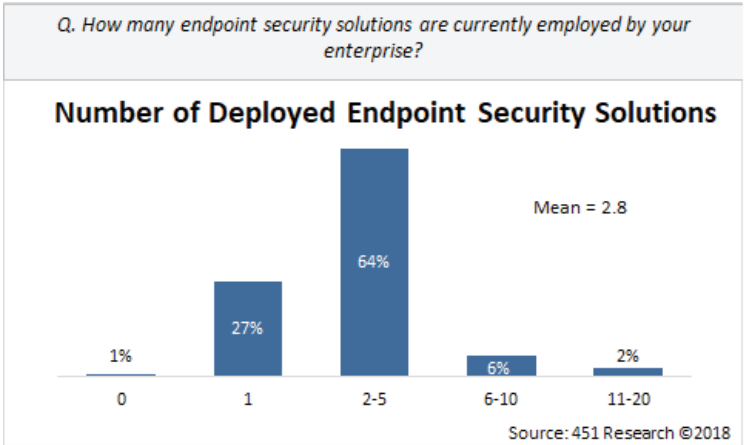


PUSH TO DECREASE ENDPOINT TOOLS

Organizations are pushing back against the number of tools they're running on each endpoint. On average, organizations have three (2.8) endpoint security solutions running. Larger enterprises (10,000-plus employees) have closer to four.

FIGURE 7: DEPLOYED ENDPOINT SECURITY OFFERINGS

Source: Voice of the Enterprise: Information Security, Workloads and Key Projects 2018



PRIMARY USERS OF ENDPOINT SECURITY TOOLS

The primary user of endpoint security tools varies by company size. For half of very large organizations with more than 10,000 employees, the security operations team is the primary user. However, for smaller enterprise with fewer than 1,000 employees, the desktop/IT team is the primary user.

FIGURE 8: PRIMARY ENDPOINT SECURITY USERS

Source: Voice of the Enterprise: Information Security, Workloads and Key Projects 2018