Endpoint Security: Securing the Extended Enterprise

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled "Endpoint Security: Securing the Extended Enterprise," on November 19, 2020.

With many employees working from home, the rise of the Internet of Things (IoT) and Operational Technology (OT) and exceptional network demands, CISOs asked the Forum to address a number of important questions surrounding this topic.

- How can we best manage risks and protect endpoints while still supporting the business and controlling costs?
- What added complexities must we consider?
- What leading practices are emerging in response to a more difficult threat landscape?

Accenture Security subject-matter experts and peer CISOs examined endpoint security challenges and leading practices for securing the enterprise. They concluded that managing risk and cost while enabling enterprise endpoint capabilities is a complex task. Many CISOs are reevaluating their strategy and approach to endpoint security.

The Forum was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

The complexity of endpoint expansion

As the Accenture 2020 Cyber Threatscape Report notes, "connectiveness has consequences." The shift to remote working due to the disruption caused by the COVID-19 pandemic has been forcing CISOs to put in place new monitoring and controls as threat actors continue to exploit vulnerabilities. The reliance on home routers and Virtual Private Networks (VPNs), coupled with unsatisfactory work-from-home practices, are putting enterprises at greater risk of cyber attacks. Increasingly, businesses are using unpatched and untested devices—which present a far more realistic and accessible target. The reliance on Operational Technology (OT) prompts threats that highlight the need for more effective security controls. Security testing can be expensive—and it is difficult to assess the risk posed by each device.

CISOs in capital-intensive industries, such as transportation and manufacturing, report the additional challenge of managing embedded endpoint technology that was not originally intended to be upgraded regularly. In addition to providing cybersecurity for knowledge workers, CISOs in these industries face the added challenge of isolating and protecting less agile assets.

The context of assets—the data, the environment, and how people are working—changes over time so it is important to monitor those changes. “Anyone who has gone down the road of user behavior analytics (UBA) knows that’s not the silver bullet we thought it would be,” said a cybersecurity expert. “Being creative about identifying those changes and feeding information back into the asset management process provides an important secondary level of control.”

Managing costs

CISOs agree that clearly understanding what endpoint security is intended to achieve for the good of the enterprise is critical in managing costs. First, determine the outcomes you are trying to achieve in protecting endpoints and solving real problems. Then, inform investment decisions with knowledge of the threat landscape. A sustainable threat intelligence program that collects and curates threat intelligence is invaluable.

It is also important to define what constitutes an enterprise’s endpoints and identify the risks that are worthy of focus. One CISO said: “The computing landscape has changed so much that it is easy to get distracted by less important, less risky concerns. We have to begin by agreeing what’s in scope. Then we can focus on decreasing risk, enabling the business and running the business.”

Cyber experts also stressed the importance the basics of cyber hygiene. These basics include:

- Identify and harden high-value assets.
- Establish which data is critical and make it difficult for adversaries to achieve their goals.
- Create environments to better monitor users and applications and block attackers.
- Adopt a continuous response model and use threat hunting teams to look for the next breach.
- Run adversary simulations and scenarios to validate that adversaries can be detected and practice your response.
- Scan applications for high-risk vulnerabilities and integrate security into development cycles. Introduce automatic notification when applications require a patch.
- Use two-factor authentication and role-based access to make automated decisions about who can see what data and systems.
- Monitor anomalous and suspicious activity.

Cyber experts discussed the phenomenon of “agent bloat”—the proliferation of devices and tools used to monitor and secure endpoints. Many CISOs acknowledged that security tools tend to accumulate unchecked, rather than being rationalized as updated versions become available. The result: greater complexity and higher total cost of endpoint ownership.

To address that problem, a CISO said his organization is doing a "total reset," assessing and rationalizing endpoint security tools on an enterprise-wide basis. "Trying to do this module by module just isn't cost-effective or efficient," he said.

How threat actors attack endpoints

Massive increases in bandwidth consumption puts most organizations at risk of distributed denial of service (DDoS) attacks. With most of the workforce telecommuting, DDoS attacks have strong potential to cause operational downtime issues.

The Accenture 2020 Cyber Threatscape Report notes that the most common ransomware attack vector continues to be poorly secured Remote Desktop Protocol (RDP) access points which has been intensified by the fact that there has been a marked increase in exposed RDP endpoints due to the surge in the need for remote working. What is more, ransomware threat actors are now targeting vulnerabilities in VPNs and other remote working tools and software.

CISOs expect that a combination of emboldened ransomware cybercriminals earning large sums of money and running their operations like a business, and a general weakening of organizational security, can only serve to make things worse for businesses in the short term. The ransomware threat is likely to fuel interest in managed detection and response services.

Furthermore, security experts said that threat actors are hitting a new low with attacks on pharmaceutical companies, hospitals and even high schools. "I'm not optimistic," said a CISO. "There are no societal norms in threat behavior." This is not a problem that can be solved by individual action. "We need an integrated response to threat actor behavior that includes intervention from governments and law enforcement," said a cybersecurity leader.

Leading practices

Here are some of the ways organizations can better manage security in disruptive times:

- **Focus endpoint security effort and investment** on decreasing risk, enabling the business and running the business so that end users can have a positive, productive experience. Focused endpoint security efforts will provide added value for the enterprise.
- **Develop an asset classification scheme or index.** Define what an endpoint is in your enterprise—it is unique to every enterprise. It will also help to create an inventory of all the assets on different networks. Focus controls on – protect – the highest value assets.
- **Assign shared accountability for vulnerability management.** Depending on the endpoint, responsibility for patching vulnerabilities might be best served by SecOps, the larger IT organization or within business operations.
- **Establish a security council** to define roles and responsibilities and transparently address and resolve issues such as tool rationalization and endpoint security maintenance.
- **Work collectively to drive vendor innovation.** CISOs said they need to engage vendors in difficult conversations to drive interoperability. "It's hard to do, but it's worked in biometrics," said a CISO.

- **Get as "skinny" as possible.** Decrease complexity and rationalize less valuable investments. Aim to cut the operational overhead associated with maintaining endpoint cybersecurity. Establish an endpoint security architecture rather than add one-off modules.
- **Don't forget about the end-user experience.** Be mindful of the impact of endpoint monitoring and security tools on user productivity. Try to find the right balance of security and productivity.
- **Maintain cyber hygiene best practices.** Innovation may be in order, but getting the basics right is essential to endpoint security. As one CISO said: "Don't start thinking about endpoint security by looking at vendor literature."

Conclusion

Endpoint security is increasing in value and importance as enterprises become digital businesses. To help drive transformation, CISOs will need greater visibility about threat actor behavior, endpoint vulnerabilities and business priorities. They will need to establish the appropriate behavioral, process and technology controls to manage compliance and telemetry, managing costs while enabling enterprise capabilities. They must be willing to uphold high compliance standards and consequences for risky end user behavior, balanced with a commitment to providing a level of training and security controls that support, not hinder, business performance.

CONTACT

Kris Burkhardt

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

LinkedIn profile – here

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 506,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

View the entire suite of ACF roundtable summaries on our webpage – here.